

UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Aécio de Lima Oliveira

**PROCESSADOR INTELIGENTE DE ALARMES E MODELOS DE
PROGRAMAÇÃO MATEMÁTICA PARA DIAGNÓSTICO DE FALTAS
EM SISTEMAS ELÉTRICOS DE POTÊNCIA**

Santa Maria, RS
2016

Aécio de Lima Oliveira

**PROCESSADOR INTELIGENTE DE ALARMES E MODELOS DE
PROGRAMAÇÃO MATEMÁTICA PARA DIAGNÓSTICO DE FALTAS EM
SISTEMAS ELÉTRICOS DE POTÊNCIA**

Tese apresentada ao Curso de Doutorado do Programa de Pós-Graduação em Engenharia Elétrica, Área de Concentração em Processamento de Energia, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Doutor em Engenharia Elétrica.**

Orientador: Ghendy Cardoso Jr., Dr. Eng.
Coorientador: Olinto César Bassi de Araújo, Dr.

Santa Maria, RS
2016

Ficha catalográfica elaborada através do Programa de Geração Automática da Biblioteca Central da UFSM, com os dados fornecidos pelo(a) autor(a).

Oliveira, Aécio de Lima
Processador inteligente de alarmes e modelos de programação matemática para diagnóstico de faltas em sistemas elétricos de potência / Aécio de Lima Oliveira.- 2016.
203 p.; 30 cm

Orientador: Ghendy Cardoso Jr.
Coorientador: Olinto César Bassi de Araújo
Tese (doutorado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia Elétrica, RS, 2016

1. Diagnóstico de Faltas 2. Estimação da Seção em Falta
3. Processamento Inteligente de Alarmes 4. Proteção de Sistemas Elétricos I. Cardoso Jr., Ghendy II. Araújo, Olinto César Bassi de III. Título.

© 2016

Todos os direitos autorais reservados a Aécio de Lima Oliveira. A reprodução de partes ou do todo deste trabalho só poderá ser feita mediante a citação da fonte.

Endereço: Rua Bento Gonçalves, n. 3174, Centro, Santiago, RS. CEP: 97700-000

Fone (0xx) 55 96443702; E-mail: aecio.eng@gmail.com

**Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Engenharia Elétrica**

A Comissão Examinadora, abaixo assinada,
aprova a Tese de Doutorado

**PROCESSADOR INTELIGENTE DE ALARMES E MODELOS DE
PROGRAMAÇÃO MATEMÁTICA PARA DIAGNÓSTICO DE FALTAS
EM SISTEMAS ELÉTRICOS DE POTÊNCIA**

elaborada por
Aécio de Lima Oliveira

como requisito parcial para obtenção do título de
Doutor em Engenharia Elétrica

COMISSÃO EXAMINADORA:


Ghendy Cardoso Jr., Dr. (UFSM)
(Presidente/Orientador)


Olinto César Bassi de Araújo, Dr. (UFSM)
(Coorientador)


Adriano Peres de Moraes, Dr. (UFSM)


Flávio Antônio Becon Lemos, Dr. (UFRGS)


Gustavo Dorneles Ferreira, Dr. (UFRGS)


Maurício Sperandio, Dr. (UFSM)

Santa Maria, 24 de junho de 2016.

AGRADECIMENTOS

Este trabalho é uma conquista que divido com cada uma das pessoas que me auxiliaram, contribuíram e apoiaram. Agradeço a todos que fizeram parte dessa caminhada e que de alguma forma colaboraram para este resultado. Agradeço:

- à minha noiva Elisa por estar sempre ao meu lado e pelo amor compartilhado;
- aos meus pais, Rubem e Idalina, por nunca medirem esforços para me amar, educar e dar todo o apoio necessário;
- aos meus orientadores, Ghendy e Olinto, pela oportunidade dada e pelos ensinamentos, confiança e amizade;
- aos professores membros da banca examinadora: Adriano, Mauricio, Flávio, Gustavo, Tiago e Viviane, pela disponibilidade em participar e pelas pertinentes contribuições que engrandeceram esse trabalho;
- aos professores e servidores do PPGEE pelo empenho com que sempre trabalharam;
- às minhas irmãs, Ariane e Aline, e ao meu sobrinho, Fabricio, pelas palavras de conforto e de encorajamento;
- à minha vó, tios, primos, cunhados e familiares da Elisa, pelas mensagens positivas e de apoio;
- aos amigos Mauren, Olinto, Cacilda, José, João Marcos, Patrick, Aldêbar e Guilherme por todo suporte que me deram nesses últimos meses;
- aos amigos brasileiros e colombianos do CEESP pela parceria de sempre;
- aos demais amigos que fizeram parte dessa jornada pelas palavras de incentivo.

Teria Hércules sido quem foi se não houvesse um leão, uma hidra, um cervo, um javali, e homens desonestos e cruéis, a quem ele expulsou e venceu? E o que faria se nada disso tivesse acontecido? Não é evidente que se envolveria num cobertor e dormiria?

(Epicteto)

RESUMO

PROCESSADOR INTELIGENTE DE ALARMES E MODELOS DE PROGRAMAÇÃO MATEMÁTICA PARA DIAGNÓSTICO DE FALTAS EM SISTEMAS ELÉTRICOS DE POTÊNCIA

AUTOR: AÉCIO DE LIMA OLIVEIRA
ORIENTADOR: GHENDY CARDOSO JÚNIOR
COORIENTADOR: OLINTO CÉSAR BASSI DE ARAÚJO

Esta tese propõe um Processador Inteligente de Alarmes para diagnóstico de faltas em sistemas elétricos de potência. O objetivo é desenvolver uma metodologia para a análise automática de faltas a partir dos alarmes reportados no sistema de supervisão e aquisição de dados (SCADA) que possibilite o uso de métodos de diagnóstico em sistemas de potência de grande porte. Essa proposta pode ser empregada em sistemas de apoio à decisão em tempo real, que auxiliem operadores de centros de controle do sistema (COS) na tomada de decisão após desligamentos não programados, com informações pertinentes para o restabelecimento do sistema. O trabalho espera contribuir com o desenvolvimento de lógicas avançadas de gerenciamento de alarmes que possibilitem a reordenação cronológica dos alarmes reportados, o mapeamento dos eventos e a geração de padrões de funcionamento de sistemas de proteção de acordo à topologia da rede. Além disso, os modelos de programação matemática foram formulados como um problema de recobrimento de conjuntos parcimonioso, para estimação da seção em falta e identificação dos dispositivos de proteção com atuação indevida. Dentre esses modelos, destaca-se o modelo que analisa, de forma integrada, os alarmes reportados e determina os eventos e diagnósticos que melhor explicam os alarmes. A abordagem proposta foi testada em diferentes porções do sistema sul do sistema interligado nacional (SIN). Os resultados mostram que as rotinas desenvolvidas para o processamento de alarmes permite a implantação prática de métodos inteligentes de diagnóstico em sistemas supervisórios existentes. Os métodos propostos para diagnóstico de faltas mostraram desempenhos e precisão nos resultados superiores a outros métodos presentes na literatura.

Palavras-chave: Diagnóstico de Faltas. Estimação da Seção em Falta. Processamento Inteligente de Alarmes. Proteção de Sistemas Elétricos.

ABSTRACT

INTELLIGENT ALARM PROCESSOR AND MATHEMATICAL PROGRAMMING MODELS FOR FAULT DIAGNOSIS IN ELECTRICAL POWER SYSTEMS

AUTHOR: AÉCIO DE LIMA OLIVEIRA
ADVISOR: GHENDY CARDOSO JÚNIOR
CO-ADVISOR: OLINTO CÉSAR BASSI DE ARAÚJO

This thesis proposes an Intelligent Alarm Processor for fault diagnosis in electrical power systems. The objective is to develop a methodology for automatic fault analysis using reported alarms from Supervisory Control and Data Acquisition (SCADA) to allow the use of diagnosis systems in large power systems. The proposal can be used in real-time decision support systems to assist control center's operators during the decision-making after unscheduled contingencies with relevant information to power system restoration. This work expects to contribute to the development of advanced alarm management logics that allow modifying the chronological sequence of reported alarms, event mapping and the generation of operating patterns of protection systems according to topology network. Still, mathematical programming models have been formulated as a parsimonious set covering problem to fault section estimation and identification of protective devices with improper operation. Among these models, it stands out the model that deals with integrated analysis of reported alarms, events and diagnosis that better explain the alarms. The proposed approach has been tested in different portions of the Southern Brazilian power system. The results show that alarm processing allows the practical implementation of intelligent diagnosis methods in existing supervisory systems. The proposed diagnosis methods show better performance and accurate solutions than other methods presented in literature.

Keywords: Fault Diagnosis. Fault Section Estimation. Intelligent Alarm Processing. Power System Protection.

LISTA DE TRABALHOS ORIGINAIS

No que tange a divulgação dos resultados são enumeradas os artigos publicados durante o desenvolvimento da tese:

OLIVEIRA, A. L.; ARAÚJO, O. C. B.; CARDOSO JR., G.; MORAIS, A. P.; MARIOTTO, L. Mixed integer programming model for optimal fault section estimation in power systems. **International Journal of Electrical Power and Energy Systems**, v. 77, p. 372-384, maio 2016.

OLIVEIRA, A. L.; ARAÚJO, O. C. B.; CARDOSO JR., G. Ferramenta para análise automática de distúrbios em sistemas de geração e transmissão. **Anais do Decimo sexto Encuentro Regional Iberoamericano de Cigré (ERiac)**, Puerto Iguazú, Argentina, 2015.

OLIVEIRA, A. L.; ARAÚJO, O. C. B.; CARDOSO JR., G.; RIBEIRO, J. C.. Desenvolvimento de um processador de alarmes para diagnóstico de faltas em sistemas elétricos de potência. **Proceedings of the XI Latin-American Congress Electricity Generation and Transmission (CLAGTEE)**, São José dos Campos, SP, 2015.

OLIVEIRA, A. L.; ARAÚJO, O. C. B.; CARDOSO JR., G.; MORAIS, A. P.; BRUM, A.F.; MARCHESAN, G. An automatic fault diagnosis solution for electrical power systems. **Proceedings of the 12th IET International Conference on Developments in Power System Protection (DPSP)**, Copenhagen, Dinamarca, p. 12-33, 2014.

OLIVEIRA, A. L.; ARAÚJO, O. C. B.; CARDOSO JR., G.; MORAIS, A. P.; FARIAS, P. E. Treatment of alarms applied to fault diagnosis in power systems. **Proceedings of the 49th International Universities Power Engineering Conference (UPEC)**, Cluj-Napoca. Romênia, 2014.

OLIVEIRA, A. L.; ARAÚJO, O. C. B.; CARDOSO JR., G. Power system event classification by means of reported alarms. **Proceedings of the 11th IEEE/IAS International Conference on Industry Applications (INDUSCON)**, Juiz de Fora, MG, 2014.

OLIVEIRA, A. L.; ZAUk, J. M.; ARAÚJO, O. C. B.; CARDOSO JR., G. Binary integer programming applied to fault section estimation in power systems. **Proceedings of the 48th Universities' Power Engineering Conference (UPEC)**, Dublin, Irlanda, 2013.

Durante o período de doutorado, também foi realizado o registro do *software*:

DIGFAULT. OLIVEIRA, A. L. et al., Registro de software BR 51 2015 000264-3, **Instituto Nacional de Propriedade Intelectual**, 13 out. 2015.

LISTA DE ILUSTRAÇÕES

Figura 2.1 – Categorias e dispositivos para o monitoramento de distúrbios.....	46
Figura 2.2 – Módulos que compõem um processador inteligente de alarmes.....	49
Figura 2.3 – Classificação de um sistema de alarmes de um sistema de energia.....	52
Figura 3.1 – Rotinas implementadas no PIA proposto.....	55
Figura 3.2 – Grafo relativo a conexão entre uma linha e uma barra.....	57
Figura 3.3 – Estrutura de dados do PIA proposto.....	58
Figura 3.4 – Religamento automático <i>single-shot</i> para faltas temporárias.....	61
Figura 3.5 – Religamento automático <i>single-shot</i> para faltas permanentes.....	62
Figura 3.6 – Diagrama de transição de estados da proteção de LTs.....	62
Figura 3.7 – Diagrama de transição de estados da proteção em um sistema de transmissão...	63
Figura 3.8 – Fluxograma do mapeamento de eventos.....	65
Figura 3.9 – Fluxograma de atualização dos dispositivos lógicos seccionadores.....	67
Figura 3.10 – Fluxograma para rastreamento da topologia de rede.....	69
Figura 3.11 – Esquema de proteção de barras de 230 kV.....	73
Figura 3.12 – Esquema de proteção de LTs de 230 kV.....	74
Figura 3.13 – Esquema de proteção de transformadores 138/13,8/230 kV.....	76
Figura 3.14 – Esquema de proteção de geradores síncronos de 13,8 kV.....	78
Figura 3.15 – Esquema de proteção da banco de capacitores.....	79
Figura 3.16 – Fluxograma para determinação das classificações de evento.....	86
Figura 3.17 – Arranjo disjuntor e meio com falta em L3 e falha em CB5.....	90
Figura 3.18 – Cenário pós-falta na barra B1.....	91
Figura 3.19 – Sistema de transmissão.....	92
Figura 4.1 – Rede causal para diagnóstico de faltas em um transformador.....	98
Figura 4.2 – Fluxograma da metodologia AD.....	100
Figura 4.3 – Fluxograma da metodologia ED.....	104
Figura 4.4 – Fluxograma para cálculo da probabilidade $P(A e_i)$	106
Figura 4.5 – Fluxograma da metodologia AED.....	115
Figura 5.1 – Topologia pré falta do sistema teste 1.....	119
Figura 5.2 – Topologia pós-falta do sistema teste 1.....	120
Figura 5.3 – Sistema teste 2.....	125
Figura 5.4 – Topologia da rede após a falta na barra B5.....	126
Figura 5.5 – Modificações na estrutura após caso 1.....	127
Figura 5.6 – Topologia de rede após recomposição da SE3.....	128
Figura 5.7 – Modificações na estrutura após caso 2.....	129
Figura 5.8 – Topologia pós-falta na linha L2.....	130
Figura 5.9 – Modificações na estrutura pós-falta do caso 3.....	130
Figura 5.10 – Sistema teste 3.....	131
Figura 6.1 – Sistema teste proposto por Wen e Han (1995).....	138
Figura 6.2 – Diagrama unifilar da SE JAG 179.....	140
Figura 6.3 – Ruído amostral médio após inserção de 1 alarme aleatório.....	141
Figura 6.4 – Ruído amostral médio após inserção de 2 alarmes aleatórios.....	142
Figura 6.5 – Desempenho de métodos com erro em 1 alarme em nível local.....	144
Figura 6.6 – Desempenho de métodos com erro em 2 alarmes em nível local.....	144
Figura 6.7 – Desempenho de métodos com 1 alarme de ruído em nível de sistema.....	145
Figura 6.8 – Desempenho de métodos com 2 alarmes de ruído em nível de sistema.....	146
Figura 6.9 – Parte do sistema de potência da Eletrosul de 230 kV.....	148
Figura 6.10 – Diagrama unifilar do sistema de 138/230 kV da CEEE-GT.....	153

Figura A.1 – Dados do sistema teste 2.....	173
Figura D.1 – Topologia pós-falta da instância 1 de Leão, Pereira e Mantovani (2010)	191
Figura D.2 – Topologia pós-falta da instância 2 de Leão, Pereira e Mantovani (2010)	192
Figura D.3 – Topologia pós-falta da instância 3 de Leão, Pereira e Mantovani (2010)	193
Figura D.4 – Topologia pós-falta da instância 4 de Leão, Pereira e Mantovani (2010)	194
Figura D.5 – Topologia pós-falta da instância 5 de Leão, Pereira e Mantovani (2010)	195
Figura D.6 – Topologia pós-falta da instância 6 de Leão, Pereira e Mantovani (2010)	196
Figura D.7 – Topologia pós-falta da instância 7 de Leão, Pereira e Mantovani (2010)	197
Figura D.8 – Topologia pós-falta da instância 8 de Leão, Pereira e Mantovani (2010)	198
Figura D.9 – Topologia pós-falta da instância 9 de Leão, Pereira e Mantovani (2010)	199
Figura D.10 – Topologia pós-falta da instância 10 de Leão, Pereira e Mantovani (2010)	200

LISTA DE TABELAS E QUADROS

Tabela 2.1 – Índices de desempenho EEMUA x SEP.....	51
Tabela 2.2 – Níveis de desempenho do sistema de alarmes.....	52
Tabela 3.1 – Regras da proteção de disjuntores.....	72
Tabela 3.2 – Classificações das regras de disjuntores.....	72
Tabela 3.3 – Regras da proteção de barras.....	73
Tabela 3.4 – Classificações das regras de barras.....	74
Tabela 3.5 – Regras da proteção de LTs.....	75
Tabela 3.6 – Classificações das regras de LTs.....	75
Tabela 3.7 – Regras da proteção de transformadores.....	77
Tabela 3.8 – Classificações das regras de transformadores.....	77
Tabela 3.9 – Regras da proteção de geradores síncronos.....	78
Tabela 3.10 – Classificações das regras de geradores síncronos.....	79
Tabela 3.11 – Regras da proteção de banco de capacitores.....	80
Tabela 3.12 – Regras da proteção de banco de capacitores.....	80
Tabela 3.13 – Sub-rotinas utilizadas para a determinação de classificações.....	86
Tabela 5.1 – Lista de alarmes original.....	120
Tabela 5.2 – Diagnóstico obtido a partir dos dados da Tabela 5.1.....	121
Tabela 5.3 – Lista de alarmes após uso das máquinas de estado.....	122
Tabela 5.4 – Diagnóstico obtido a partir dos dados da Tabela 5.3.....	123
Tabela 5.5 – Lista de alarmes após uso do critério de tempo.....	123
Tabela 5.6 - Diagnóstico obtido a partir dos dados da Tabela 5.5.....	124
Tabela 5.7 – Alarmes reportados no caso 3.....	129
Tabela 5.8 – Dados das arestas do grafo referente ao sistema teste 3.....	131
Tabela 5.9 – Padrões de eventos gerados.....	132
Tabela 6.1 – Instâncias de Fritzen et al. (2012) sem alarmes “não falta”.....	138
Tabela 6.2 – Alarmes reportados nos testes envolvendo o SEP da Eletrosul.....	149
Tabela 6.3 – Diagnósticos obtidos nas simulações de falta no SEP da Eletrosul.....	150
Tabela 6.4 – Testes computacionais e diagnósticos obtidos pelo método ED1.....	156
Tabela 6.5 - Testes computacionais e diagnósticos obtidos pelo método AED.....	159
Tabela B.1 – Regras da proteção de barras do sistema da Eletrosul.....	175
Tabela B.2 – Disjuntores associados ao alarme “CBs” de barras.....	175
Tabela B.3 – Classificações das regras das barras do sistema da Eletrosul.....	175
Tabela B.4 – Regras da proteção de linhas malhadas.....	175
Tabela B.5 – Classificações das regras de linhas malhadas do sistema da Eletrosul.....	176
Tabela B.6 – Regras da proteção de linhas radiais.....	176
Tabela B.7 – Classificação das regras de linhas radiais do sistema da Eletrosul.....	176
Tabela B.8 – Regras da proteção de transformadores.....	176
Tabela B.9 – Classificações das regras de transformadores do sistema da Eletrosul.....	176
Quadro C.1 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 1 evento e 1 alarme de ruído.....	177
Quadro C.2 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 2 eventos e 1 alarme de ruído.....	178
Quadro C.3 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 3 eventos e 1 alarme de ruído.....	179
Quadro C.4 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 4 eventos e 1 alarme de ruído.....	180

Quadro C.5 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 1 evento e 2 alarmes de ruído	180
Quadro C.6 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 2 eventos e 2 alarmes de ruído	181
Quadro C.7 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 3 eventos e 2 alarmes de ruído	182
Quadro C.8 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 4 eventos e 2 alarmes de ruído	183
Quadro C.9 – Desempenho médio de métodos em nível de sistema considerando instâncias com 1 evento e 1 alarme de ruído	184
Quadro C.10 – Desempenho médio de métodos em nível de sistema considerando instâncias com 2 eventos e 1 alarme de ruído.....	185
Quadro C.11 – Desempenho médio de métodos em nível de sistema considerando instâncias com 3 eventos e 1 alarme de ruído.....	186
Quadro C.12 – Desempenho médio de métodos em nível de sistema considerando instâncias com 4 eventos e 1 alarme de ruído.....	187
Quadro C.13 – Desempenho médio de métodos em nível de sistema considerando instâncias com 1 evento e 2 alarmes de ruído.....	187
Quadro C.14 – Desempenho médio de métodos em nível de sistema considerando instâncias com 2 eventos e 2 alarmes de ruído	188
Quadro C.15 – Desempenho médio de métodos em nível de sistema considerando instâncias com 3 eventos e 2 alarmes de ruído	189
Quadro C.16 – Desempenho médio de métodos em nível de sistema considerando instâncias com 4 eventos e 2 alarmes de ruído	190

LISTA DE ABREVIATURAS E SIGLAS

AG	Algoritmo genético
AGA	Algoritmo genético adaptativo
ASCP	Algoritmo de simulação do crescimento de plantas
BBO	<i>Biogeography-based optimization</i> (Otimização baseada em biogeografia)
BIP	<i>Binary integer programming</i> (programação inteira binária)
CB	<i>Circuit breaker</i> (disjuntor)
CEEE-GT	Companhia Estadual de Geração e Transmissão de Energia Elétrica
COS	Centro de operação do sistema
DS	Dispositivo lógico seccionador (aresta)
DMS	<i>Distribution management system</i> (sistema de gestão de distribuição)
EEMUA	<i>Engineering Equipment and Materials Users Association</i> (Associação de Equipamentos e Materiais de Engenharia)
EMS	<i>Energy management system</i> (sistema de gerenciamento de energia)
FO	Função objetivo
FSE	<i>Fault section estimation</i> (estimação da seção em falta)
GPS	<i>Global position system</i> (sistema de posicionamento global)
GRNN	<i>Generalized regression neural network</i> (rede neural de regressão generalizada)
HBM	<i>Honey-bee mating optimization</i> (acasalamento de abelhas)
HC	Heurística construtiva
IA	<i>Immune algorithm</i> (algoritmo imunológico)
IED	<i>Intelligent electronic device</i> (dispositivo inteligente eletrônico)
LT	Linha de transmissão
MAS	<i>Multi-agent system</i> (sistema multi-agente)
ONS	Operador nacional do sistema
PEDA	<i>Protection engineering diagnostic agents</i> (Agentes de diagnóstico para engenharia da proteção)
PA	Processador de alarmes
PIA	Processador inteligente de alarmes
PMU	<i>Phasor measurement unit</i> (unidade de medição fasorial)
PSO	<i>Particle swarm optimization</i> (enxame de partículas)
RBFNN	<i>Radial basis function neural network</i> (rede neural com função de base radial)
RDP	Registrador digital de perturbação
SAGE	Sistema Aberto de Gerenciamento de Energia
SCADA	<i>Supervisory Control and Data Acquisition</i> (Sistema de supervisão e aquisição de dados)
SCP	<i>Set covering problem</i> (problema de recobrimento de conjunto)
SEP	Sistema elétrico de potência
TAL	Tabela de alarmes
TDC	Tabela de dispositivos de chaveamento
TDS	Tabela de dispositivos lógicos seccionadores
TED	Tabela de equipamentos desconectados
TEQ	Tabela de equipamentos
UBP	<i>Unconstrained binary programming</i> (programação binária irrestrita)
UTR	Unidade terminal remota
WAMS	<i>Wide area measurement system</i> (rede de medição de longa distância)
WAN	<i>Wide area network</i> (rede de longa distância)

SUMÁRIO

1	INTRODUÇÃO	25
1.1	Considerações gerais	25
1.2	Objetivos do trabalho.....	26
1.3	Motivação	27
1.4	Revisão bibliográfica	27
1.4.1	Métodos de diagnóstico por meio de regras de inferência	29
1.4.2	Métodos de diagnóstico formulados como problema de otimização	30
1.4.3	Aplicação de processadores inteligente de alarmes	34
1.4.4	Sistemas multi-agentes	35
1.5	Métodos de diagnóstico investigados	37
1.5.1	Método GRNN+AG	37
1.5.2	Método IA	38
1.5.3	Método HC+BIP	41
1.6	Contribuições da tese	43
1.7	Estrutura do trabalho	44
2	CARACTERIZAÇÃO DO PROBLEMA DE DIAGNÓSTICO.....	45
2.1	Considerações gerais	45
2.2	Registradores para análise de perturbações	45
2.3	Definição do problema de estimação da seção em falta	47
2.3.1	Variáveis do problema.....	47
2.4	Processador inteligente de alarmes.....	49
2.4.1	Problemas envolvidos.....	50
2.5	Considerações finais	54
3	PROCESSADOR INTELIGENTE DE ALARMES	55
3.1	Considerações gerais	55
3.2	Metodologia proposta.....	55
3.3	Estrutura de dados	56
3.4	Reordenação cronológica de alarmes	61
3.5	Mapeamento de eventos.....	65
3.6	Identificação da topologia de rede	66
3.7	Regras de inferência para diagnóstico de faltas	70
3.7.1	Regras da proteção	71
3.7.2	Geração automática de padrões de funcionamento de sistemas de proteção	81
3.8	Considerações finais	95
4	MODELOS DE PROGRAMAÇÃO MATEMÁTICA PARA DIAGNÓSTICO DE FALTAS.....	97
4.1	Considerações iniciais	97
4.2	Critérios utilizados na formulação dos modelos de otimização	97
4.3	Métodos propostos para a estimação da seção em falta.....	98
4.4	Método AD	100
4.4.1	Exemplo numérico das restrições (4.3) e (4.4).....	103
4.5	Métodos ED.....	104
4.5.1	Classificação de eventos.....	105
4.5.2	Método ED1	108
4.5.3	Método ED2	110
4.6	Método AED	114
4.7	Considerações finais	118
5	RESULTADOS DO PROCESSADOR DE ALARMES E DISCUSSÕES	119

5.1	Considerações gerais.....	119
5.2	Reordenação cronológica dos alarmes.....	119
5.3	Mapeamento dos eventos e identificação da topologia da rede	124
5.3.1	Estudo de caso 1 – Falta na barra B5	126
5.3.2	Estudo de caso 2 – Recomposição da subestação SE3	127
5.3.3	Estudo de caso 3 – Falta temporária na linha L2	129
5.4	Geração de padrões de eventos.....	131
5.5	Considerações finais	135
6	RESULTADOS DE MÉTODOS DE DIAGNÓSTICO E DISCUSSÕES	137
6.1	Considerações gerais.....	137
6.2	Efeito no diagnóstico do uso de padrões contendo eventos “não falta”	137
6.3	Análise dos métodos de dois níveis	139
6.3.1	Metodologia de testes	140
6.3.2	Resultados obtidos	143
6.4	Análise dos métodos em um sistema de transmissão radial e malhado	146
6.5	Testes computacionais em um SEP de grande porte	153
6.6	Considerações finais	161
7	CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS	163
7.1	Sugestões para trabalhos futuros	165
	REFERÊNCIAS.....	167
	APÊNDICE A – Estrutura de dados do sistema teste 2	173
	APÊNDICE B – Conjunto de regras da proteção do sistema Eletrosul	175
	APÊNDICE C – Diagnósticos obtidos por métodos no sistema AES-Sul.....	177
	APÊNDICE D – Topologias pós-falta do sistema da Eletrosul	191
	APÊNDICE E – Topologias pós-falta do sistema da CEEE-GT	201
	ANEXO A – Funções de proteção conforme IEEE C37.2 Std.....	203

1 INTRODUÇÃO

1.1 Considerações gerais

Os sistemas de proteção tem papel fundamental para a segurança elétrica e são responsáveis pela detecção e isolamento de defeitos na rede elétrica. A rede básica do Sistema Interligado Nacional (SIN) atende aos critérios estabelecidos nos procedimentos de rede do Operador Nacional do Sistema (ONS). O ONS estabelece os requisitos mínimos que sistemas de proteção de instalações elétricas (linhas de transmissão, barras e equipamentos) devem respeitar para a diminuição do impacto de faltas, redução da extensão do desligamento e do tempo de restabelecimento da área desconectada.

Nesse contexto, o desenvolvimento de novas tecnologias que permitam aumentar a disponibilidade dos equipamentos e melhorar a operação do sistema elétrico de potência (SEP) tem papel de destaque. Dentre as possíveis soluções tecnológicas que podem ser inseridas em Centro de Operação do Sistema (COS) para a melhoria operacional do sistema, encontra-se o Processador Inteligente de Alarmes (PIA). O objetivo do PIA é analisar distúrbios na rede elétrica automaticamente, a partir da leitura dos alarmes reportados em tempo real via Sistema de Supervisão e Aquisição de Dados (SCADA, do inglês *Supervisory Control and Data Acquisition*). Dessa forma, espera-se auxiliar operadores do COS na tomada de decisão após a ocorrência de faltas com informações que expliquem o distúrbio no menor tempo possível. O diagnóstico resultante pode ser utilizado para a determinação das ações que devem ser executadas durante o restabelecimento do sistema elétrico.

A importância do processador inteligente de alarmes cresce de acordo com a complexidade da contingência e do número de alarmes reportados. Nesses casos, o operador deve selecionar os alarmes mais importantes e analisar um conjunto de informações para estimar a seção em falta e determinar os dispositivos de proteção que atuaram indevidamente, para então executar as ações para reestabelecimento do sistema. Essa é uma tarefa vital para o SEP, complexa e deve ser realizada no menor intervalo de tempo possível. Ainda hoje, essa tarefa é altamente dependente do desempenho do operador humano.

Nesta tese é proposto um processador inteligente de alarmes que atenda aos requisitos operacionais e que seja capaz de identificar eventos, diagnosticar faltas e determinar a operação indevida de dispositivos de proteção. Para alcançar esses objetivos, foram desenvolvidos métodos para filtragem de alarmes, mapeamento de eventos e geração de padrões de funcionamento de sistemas de proteção de acordo com a topologia da rede. Além

disso, foram propostos modelos de programação matemática para a estimação da seção em falta e identificação dos dispositivos com atuação indevida.

Neste capítulo são apresentados os objetivos da pesquisa e as motivações do trabalho. Além disso, é apresentada uma revisão da bibliografia com ênfase nos últimos cinco anos. Na revisão são descritos métodos empregados para estimação da seção em falta em sistemas elétricos de potência e aplicações de processadores inteligentes de alarmes.

1.2 Objetivos do trabalho

O objetivo principal deste trabalho é propor um processador inteligente de alarmes que auxilie operadores do COS na tomada decisão após a ocorrência de grandes desligamentos. Dentro desse objetivo, procura-se desenvolver algoritmos que contemplem as funcionalidades requeridas por um processador inteligente de alarmes com modelos de programação matemática para a estimação da seção em falta.

Como objetivos específicos, este trabalho visa:

- desenvolver algoritmos que sirvam para auxiliar a implantação prática de um processador inteligente de alarmes em sistemas reais;
- propor uma metodologia para reordenação cronológica dos alarmes reportados no SCADA, de modo a descrever a sequência lógica da operação de esquemas de proteção;
- desenvolver uma representação da topologia da rede em termos dos esquemas de proteção associados a cada elemento do SEP;
- propor uma metodologia para geração automática de padrões de funcionamento da proteção de acordo com a topologia da rede. Esse deve funcionar em sistemas de potência que atendam aos requisitos técnicos e de proteção estabelecidos nos Procedimentos de Rede do Operador Nacional do Sistema (ONS, 2010);
- formular um modelo de programação matemática para diagnóstico de faltas que permita avaliar o funcionamento da proteção em níveis de equipamento e de sistema;
- realizar testes computacionais em um sistema de potência de grande porte e comparar os resultados obtidos com outros métodos de estimação da seção em falta.

1.3 Motivação

O ONS possui a prerrogativa de aplicar multas elevadas quando ocorrer indisponibilidade nos equipamentos ou linhas de transmissão contratados. Quando o desligamento for não programado, isto é, quando ocorrer uma interrupção no fornecimento de energia devido a uma falta intempestiva, a multa é cobrada. A ocorrência de desligamentos imprevistos é uma das situações mais críticas que operadores podem enfrentar.

Quando uma falta ocorre em uma seção do sistema de potência, os sistemas de proteção (conjuntos de relés e disjuntores) associados a esta devem operar com o intuito de isolar o defeito. A atuação dos dispositivos de proteção resulta em alarmes no COS que são reportados via SCADA. Tais eventos submetem os operadores a um altíssimo grau de estresse, uma vez que necessitam agir apropriadamente sobre o sistema desligado, de modo a restaurá-lo no menor tempo possível. Sendo assim, a tomada de uma decisão errada durante tal situação poder alcançar, como consequência natural, proporções catastróficas.

A disponibilidade de uma ferramenta computacional para auxílio à operação em tempo real e capaz de identificar a causa do desligamento é de extrema importância para a restauração do sistema, seja em nível de subestação (SE) ou centro de controle. Uma vez estimado o componente em falta, este é devidamente isolado e o processo de reenergização poderá ocorrer de forma rápida e segura, reduzindo os prejuízos aos consumidores e aos demais agentes do setor.

1.4 Revisão bibliográfica

Um relatório do *Electric Power Research Institute* (EPRI, 1960) estabeleceu as atividades que devem ser executadas pelo operador do COS na leitura do alarme. Essas ações estão diretamente ligadas ao método de diagnóstico empregado para analisar faltas no SEP, a saber, são:

- 1) O operador deve estar ciente do alarme recebido;
- 2) Determinar o evento que causou o alarme;
- 3) Analisar as consequências do evento;
- 4) Analisar a sequência de eventos ocasionada pelo alarme;
- 5) Definir as ações para contornar ou consertar o defeito.

A etapa 1 descrita no relatório acima é a única que independe do método de diagnóstico utilizado, pois está relacionada na forma como a informação é reportada ao operador. As demais etapas são ações que podem ser automatizadas a partir da aplicação de um método de diagnóstico de falta.

Desde então, inúmeros algoritmos têm sido desenvolvidos e incorporados em modernos Sistemas de Gerenciamento de Energia (EMS, do inglês *Energy Management System*). Alarmes possuem características de informar e alertar o operador as modificações ocorridas no sistema elétrico, e devido a isso, é natural que surjam técnicas de inteligência artificial para tratar e inferir diagnósticos mais precisos de ocorrências (STAHLHUT; HEYDT; CARDELL, 2008).

Desde o primeiro processador de alarmes baseado em regras proposto por Wollenberg (1986), diversos métodos têm sido desenvolvidos para lidar com diferentes aspectos do problema e uma variedade de protótipos tem sido instalada em centros de operação para auxiliar as operações diárias de sistemas de potência. Kirschen e Wollenberg (1992) definiram o processador inteligente de alarmes como um conjunto processador de alarmes e método de diagnóstico. A função de um processador de alarmes é agrupar, selecionar e apresentar os alarmes mais importantes para elaboração de diagnósticos. Já o método de diagnóstico tem como objetivo encontrar a explicação dos alarmes reportados e apresentar o diagnóstico obtido ao operador.

O volume de informações inerente da operação do SEP é o maior obstáculo para a aplicação de um PIA em um sistema real (LEÃO; PEREIRA; MANTOVANI, 2010). Ao longo das últimas duas décadas, um grande número de ferramentas e técnicas foi desenvolvido para automatizar a análise das informações da rede elétrica e auxiliar os engenheiros com informações explícitas relacionadas à operação do sistema de potência (DAVIDSON et al., 2006).

De acordo com Mu et al. (2012), as metodologias propostas para diagnóstico de faltas em sistemas de potência são divididas em dois grupos: métodos que inferem a seção em falta a partir dos alarmes disparados por meio de regras de inferência, ou modelos que formalizam o problema de diagnóstico como um problema de otimização combinatória.

1.4.1 Métodos de diagnóstico por meio de regras de inferência

Chen (2011) propôs uma técnica para estimar seções em falta em subestações de distribuição utilizando redes causa-efeito e lógica *fuzzy*. Nesse trabalho, as redes causa-efeito são utilizadas para modelar filosofias de proteção empregadas nos sistemas radiais de distribuição. As relações entre a atuação dos relés de proteção e a operação de disjuntores (CBs, do inglês *circuit breakers*) são modeladas considerando os dados históricos de ocorrência de eventos. A veracidade do evento é avaliada a partir de inferências *fuzzy*. O método indica a seção em falta e os dispositivos de proteção que falharam. No entanto, a modelagem das funções de pertinência da lógica *fuzzy* é uma grande desvantagem para a implementação prática desse método dada a necessidade de conhecimento extraído de banco de dados históricos, experiência ou tentativa e erro.

Chen, Tsai e Lin (2011) estenderam a aplicação do algoritmo proposto por Chen (2011) para diagnosticar faltas em níveis de distribuição e transmissão. A abordagem representa a filosofia de proteção num grafo melhorado através de nós virtuais e operações matriciais para tratar as redes causa-efeito derivados de sistemas de transmissão. O novo algoritmo também se distingue por empregar lógica booleana, ao invés de *fuzzy*, para estimar a seção em falta com uma ou múltiplas faltas, inclusive em ocorrências com falha de operação de relés e disjuntores. A rede causa-efeito deve ser modelada de acordo com topologia de rede, sendo inviável a criação manual da rede para um sistema de grande porte.

Fonseca et al. (2012) desenvolveram uma metodologia para estimação da seção em falta que se baseia na conversão de sinais lógicos de alarmes em valores percentuais com o objetivo de alimentar redes neurais artificiais. A técnica permite que um conjunto de redes neurais seja treinado e aplicado em diferentes regiões do sistema. Além disso, a rede neural apresenta baixo tempo de treinamento e é capaz de identificar alarmes falhos. Entretanto, alguns problemas permanecem não resolvidos em aplicações práticas, como a dificuldade na obtenção de um número suficiente de padrões de treinamento e a necessidade de retreinamento da rede quando houver modificações topológicas no SEP.

Ghainani, Zin e Ismail (2012) propuseram uma metodologia para tratar as incertezas na informação fornecida por relés baseada em redes de Petri *fuzzy* e temporizada. Uma rede de Petri temporizada é um caso particular de grafo direcionado contendo um conjunto de atrasos de tempo associado com cada arco. A necessidade de conhecimento do funcionamento da proteção e o tempo de transição entre um estado de proteção a outro é fundamental para a criação da rede e dificulta consideravelmente a aplicação da técnica em sistemas reais.

Xiong et al. (2013) propuseram uma sistema híbrido composto de uma rede neural com função de base radial (RBFNN, do inglês *Radial Basis Function Neural Network*) e o método da integral *fuzzy* de Choquet para o diagnóstico de faltas. A metodologia propõe a divisão do sistema de potência em várias sub-redes, cada uma possuindo uma rede RBFNN independente, de forma a reduzir a magnitude do problema de diagnóstico. O diagnóstico final é obtido através dos módulos Choquet, que medem a relação das respostas locais das RBFNNs. Essa proposta poderia ser otimizada inserindo uma lista de candidatos gerados a partir da identificação da área desligada decorrente de falta. Além disso, o estudo de incertezas em relés e disjuntores deve ser incorporado para identificação de alarmes inconsistentes.

1.4.2 Métodos de diagnóstico formulados como problema de otimização

A primeira formulação do problema de diagnóstico de faltas como um problema de otimização combinatória foi proposta por Wen, Chang e Srinivasan (1995). O princípio da parcimônia foi utilizado para formular o problema, de tal forma que o modelo permita encontrar a explicação mais simples para os alarmes reportados. A função objetivo (FO) do modelo lista as seções em falta e relaciona os estado esperados de relés com os alarmes reportados de relés. Por outro lado, o modelo proposto ignora a relação entre proteções principais e de retaguarda. O Algoritmo Genético (AG) foi empregado para resolver o problema e determinar as hipóteses que melhor expliquem os alarmes reportados. Desde então, houve um considerável aumento de publicações de modelos e métodos de resolução para estimação da seção em falta, com uma tendência para o uso de metaheurísticas.

He et al. (2009) reformularam o modelo proposto Wen, Chang e Srinivasan (1995) com a inclusão de eventos de religamento e falha da proteção de disjuntores na FO. No total, existem sete grupos de variáveis de decisão classificadas de acordo com a função de proteção específica: proteção principal; proteção de retaguarda local; proteção de retaguarda remota; religamento instantâneo; religamento temporizado; proteção contra falha de disjuntor; e estado de disjuntores. Pesos são utilizados para classificar o grau de importância de cada variável de decisão, além de um fator de penalização relativo ao mau funcionamento de relés e disjuntores. O enxame de partículas (PSO, do inglês *Particle Swarm Optimization*) é empregado pelos autores para o problema de estimação da seção em falta.

Guo et al. (2010a) formularam o problema como um problema de programação inteira incluindo o mal funcionamento de dispositivos de proteção na função objetivo em função da

área desligada da rede elétrica, e utilizaram a busca tabu para a resolução do modelo. O modelo formulado é semelhante ao proposto por Wen, Chang e Srinivasan (1995). Um *software* para diagnóstico de falta baseado no modelo proposto foi desenvolvido e colocado em operação em um SEP localizado em Guangdong, China. Numa continuação desse trabalho, Guo et al. (2010b) incluíram restrições lógicas temporais no modelo analítico descrito anteriormente para relacionar alarmes com sequências de eventos. A metodologia possibilita estimar a relação temporal de ocorrências agrupando os alarmes relatados com diferentes eventos.

Lin et al. (2010) reformularam o modelo proposto por Wen, Chang e Srinivasan (1995) de forma a considerar a influência da atuação das proteções principais e de retaguarda. Os autores empregaram um sistema híbrido para solucionar o problema de diagnóstico que combina as vantagens de duas metaheurísticas tradicionais: a habilidade dos algoritmos genéticos em obter boas soluções iniciais durante a busca global, e o bom desempenho da busca tabu no refinamento da solução na busca local. Em um estudo comparativo com um algoritmo genético, Lin et al. (2010) obteve desempenho superior considerando o tempo médio de convergência em cenários com múltiplas faltas.

Leão, Pereira e Mantovani (2010) propuseram um modelo de programação binária irrestrita (UBP, do inglês *Unconstrained Binary Programming*) que relaciona os estados esperados de relés de proteção e os alarmes reportados de relés e disjuntores. A otimização tem como objetivo minimizar a cobertura dos relés reportados, a inconsistência entre alarmes esperados e reportados de relés, o número de seções em falta e o número de SEs com falta na alimentação. O valor das variáveis de decisão é obtido por meio de uma função que avalia o estado esperado de relés a partir dos alarmes reportados de relés e disjuntores. Os sistemas imunológicos artificiais (IA, do inglês *Immune Algorithm*) são utilizados para resolver o problema de diagnóstico, e buscam por soluções que possuam maior afinidade dos anticorpos (estados esperados de relés) e o antígeno (alarmes reportados). A função que calcula o estado esperado dos relés depende da topologia do sistema e precisa ser formulada para cada esquema de proteção do SEP.

Bedekar, Bhide e Kale (2011) apresentaram uma metodologia para estimação de seção em falta por meio das redes neurais com treinamento baseado na regra de Hebb e algoritmo genético com parâmetros contínuos. A regra de Hebb é utilizada para definir os pesos da FO com base nos padrões de funcionamento da proteção do SEP, enquanto o algoritmo genético contínuo é aplicado para resolver o modelo matemático que relaciona o estado esperado de relés e disjuntores. Para treinar a rede neural, os autores determinaram, de maneira heurística,

que o número de padrões necessários é equivalente ao dobro do número de seções existentes na rede elétrica.

Huang e Liu (2013) propuseram um método baseado na otimização por colônia de abelhas para resolução do modelo UBP proposto por Leão, Pereira e Mantovani (2010). O algoritmo de resolução é inspirado no comportamento natural de forrageamento de abelhas para estimar a seção em falta. De acordo com as características da metodologia aplicada, o processo inicia com abelhas explorando aleatoriamente os campos de flores na busca de promissoras fontes de energia. Nessa metáfora, cada fonte de energia representa uma seção do sistema de potência suspeita de estar em contingência. As informações relevantes à qualidade (valor da função de aptidão) e distância do alimento encontrado são trazidas para a colmeia para análise e compartilhamento com as demais abelhas, de forma a definir se novas abelhas deverão ser recrutadas ou se a fonte de néctar deverá ser descartada.

Huang et al. (2013) propuseram uma metodologia híbrida composta de uma otimização de acasalamento de abelhas (HBM, do inglês *Honey-Bee Mating Optimization*) e um algoritmo de simulação do crescimento de uma planta (ASCP) para resolução do modelo UBP proposto por Leão, Pereira e Mantovani (2010). O algoritmo HBM funciona da seguinte maneira: a rainha (solução corrente) voa até encontrar um zangão no ar (seção em falta) para acasalar. O processo de acasalamento é avaliado de acordo com probabilidade do cruzamento do zangão e a velocidade de voo da abelha. Quando houver o cruzamento, se um indivíduo da prole possuir melhor material genético que a rainha (melhor função de avaliação), a coroa é repassada para este indivíduo, caso contrário, o indivíduo se torna um novo zangão. A seguir, o algoritmo ASCP analisa as fases de crescimento de uma planta (raiz, caule e folhas) de forma a caracterizar uma busca local por melhores soluções. Em um estudo comparativo com outras metaheurísticas, a técnica obteve resultados mais precisos com melhor velocidade de convergência. Futuros estudos nessa linha de pesquisa deve se preocupar em desenvolver uma metodologia para ajuste dos parâmetros da técnica. Além disso, é fundamental analisar a aplicabilidade em sistemas reais que possuem lógicas de proteção mais complexas que as demonstradas no trabalho.

Leão, Pereira e Mantovani (2014) apresentaram uma nova proposta composta de equacionamento de funcionamento de proteções com o mesmo modelo UBP formulado no trabalho de 2010. A atuação de cada relé é avaliada a partir dos alarmes de relés e disjuntores reportados, por meio de uma equação específica para cada função de proteção. A grande complexidade de cada equação requer um estudo pontual no sistema de potência e vasto conhecimento de pessoal especializado, fatos que podem limitar uma possível aplicação

prática. O problema UBP é resolvido através de um algoritmo genético adaptativo (AGA), o qual se diferencia do AG tradicional por possuir apenas dois parâmetros a serem ajustados, enquanto os demais são ajustados automaticamente. A metodologia apresenta resultados satisfatórios, apesar da ausência de um estudo mais aprofundado sobre o impacto dos pesos da FO no diagnóstico. Além disso, os resultados apresentados mostram que a solução do AGA tende a variar bastante devido à diversificação populacional.

Huang e Liu (2015) empregaram a metaheurística bioinspirada baseada em biogeografia (BBO, do inglês *Biogeography-Based Optimization*) para resolver o modelo UBP proposto por Leão, Pereira e Mantovani (2010). A abstração de processos presentes na ciência da biogeografia é utilizada para formalizar uma estrutura computacional capaz de inferir a história biogeográfica de linhagens através da reconstrução dos eventos que motivaram a migração de espécies de um habitat para outro.

Sörensen (2012) fez fortes críticas ao direcionamento de pesquisas que visam propor novas metaheurísticas, mas que não apresentam inovações significativas a ponto de justificar a criação de um novo método. Ainda, o autor considera que tais métodos desviam o foco da pesquisa e pouco contribuem para o avanço da ciência e para o desenvolvimento de técnicas eficazes. Essa análise pode ser estendida ao campo de diagnóstico de faltas. Veja o caso do algoritmo BBO, proposto por Huang e Liu (2015) e do algoritmo genético empregado por Wen, Chang e Srinivasan (1995). A estrutura do algoritmo e os parâmetros ajustados no BBO (número de habitats, migração e mutação) apresentam certa verossimilhança com os parâmetros do AG (população inicial, reprodução e mutação), a tal ponto que não justifica o desenvolvimento de uma nova metáfora.

Uma forma alternativa de modelar o problema de estimação da seção em falta foi proposto por Cardoso Jr., Rolim e Zurn (2004). A metodologia consiste em estimar o local da falta em dois níveis distintos de análise: nível de equipamento e nível de sistema. O método híbrido utiliza redes neurais de regressão generalizada (GRNN, do inglês *Generalized Regression Neural Network*) para a classificação de eventos e sistemas especialistas para combinar eventos. A divisão da metodologia reduz o número de padrões de eventos necessários para o funcionamento do método de diagnóstico.

Baseada nesta metodologia, Fritzen et al. (2012) propuseram uma heurística construtiva (HC) para a classificação de eventos e um modelo de programação inteira binária (BIP, do inglês *Binary Integer Programming*) para o diagnóstico de faltas em nível de sistema. A heurística construtiva é executada em cada equipamento do SEP, a partir dos alarmes reportados no SCADA. O resultado da heurística é composto de eventos, que são

parâmetros do modelo BIP. Este modelo é baseado no problema de recobrimento de conjuntos (SCP, do inglês *Set Covering Problem*) (CAPRARÁ; TOTH, 2000) e com a inclusão de restrições que identificam a operação incorreta de eventos e alarmes de disjuntores. O modelo BIP foi resolvido utilizando o *solver* comercial *CPLEX* 12.4 com configurações *default*. O uso de técnicas de solução baseadas em métodos de programação matemática é uma grande vantagem em relação aos métodos resolvidos com metaheurísticas, visto que o problema sempre será resolvido na otimalidade.

Com base na revisão da literatura, foi possível identificar um grande número de publicações que se focam na aplicação de metaheurísticas para resolução dos modelos de estimação da seção em falta, e uma fraca evolução na modelagem do problema de diagnóstico em relação ao tipo de solução obtida. Poucos trabalhos se estendem até o campo do tratamento dos dados reportados no SCADA, incluindo os problemas de aquisição e processamento de alarmes. Ainda, pouco é comentado sobre as possíveis implicações práticas resultantes da inserção de métodos de inteligência artificial, que podem ser onerosas em relação ao tempo de implantação e ao uso de recursos técnicos e humanos.

1.4.3 Aplicação de processadores inteligente de alarmes

Nesta seção é apresentada a relação recente de trabalhos que discutem as características de processadores inteligentes de alarmes e a aplicabilidade técnica dos métodos de diagnóstico de faltas. Bauer et al. (2011) demonstraram e avaliaram os resultados obtidos da aplicação de um processador inteligente de alarmes em um sistema de transmissão australiano. A ferramenta computacional desenvolvida compreende três módulos integrados: um modelo de rede que descreve o comportamento de dispositivos de proteção de acordo com a topologia atual de rede; uma máquina de diagnóstico cujo funcionamento se baseia na busca da sequência de estados discreto mais compatível com as observações; e algoritmos para filtragem e clusterização de alarmes de acordo com os cenários de falta identificados. Os resultados mostram a capacidade do PIA em identificar uma grande quantidade de eventos. No entanto, as soluções obtidas pela máquina de diagnóstico não são descritas e comentadas no trabalho, impedindo uma crítica qualitativa a respeito das mesmas.

Wei et al. (2011) propuseram uma nova sistemática incluindo dois módulos lógicos para processamento de alarmes que operam em paralelo numa plataforma online. O sistema foi desenvolvido para classificar os alarmes de acordo com a norma IEC-61850 e foi aplicado

com sucesso na subestação digital Xingguo, a primeira construída na China. A norma IEC 61850 propõe uma arquitetura de comunicação única entre todos os dispositivos, independente da função que este exerce na subestação ou de seu fabricante. O protocolo foi desenvolvido com fins de interoperabilidade e compartilhamento de informações de dispositivos inteligentes e eletrônicos (IEDs, do inglês *Intelligent Electronic Devices*), proporcionando um método de mapeamento único para cada elemento do sistema.

Edwards et al. (2013) desenvolveram um *software* para realizar o processamento de alarmes do SCADA e validar o funcionamento de sistemas de proteção. O PIA desenvolvido é capaz de determinar a origem de distúrbios, filtrar alarmes irrelevantes, agrupar alarmes por tipo de evento, identificar alarmes falsos e validar o desempenho da proteção. O protótipo foi testado usando dados reais de eventos ocorridos em um sistema de transmissão no Reino Unido, cujos resultados atenderam aos requisitos de projeto. No entanto, o PIA requer manutenção de banco de dados com a inserção de regras de funcionamento esperado da proteção. Além disso, a solução não é integrada com outras ferramentas de análise disponibilizadas em COS.

Wang et al. (2016) apresentaram uma visão geral dos trabalhos propostos na literatura em relação aos sistemas de alarmes industriais. Os autores identificaram quatro causas principais para a sobrecarga de alarmes reportados: alarmes cíclicos devido a ruídos ou distúrbios; configuração incorreta de alarmes; *design* de alarmes de forma isolada em relação aos demais parâmetros do sistema; e propagação da anormalidade a outros dispositivos da rede. A partir deste artigo foi possível verificar que os trabalhos de sistemas de alarmes aplicados ao monitoramento de SEPs estão associados ao problema gerado pela propagação da anormalidade e se limitam à identificação da causa raiz de grandes desligamentos.

1.4.4 Sistemas multi-agentes

Nesta seção são apresentados trabalhos que visam integrar sistemas de alarmes com outras ferramentas disponibilizadas no COS para a consolidação de sistema de decisão multicriterial. A utilização de registradores digitais de perturbação (RDP) é prática comum em sistemas de geração e são empregados para o monitoramento dos níveis de tensão e corrente do sistema elétrico. Com o auxílio dos RDPs, engenheiros podem avaliar o desempenho do sistema de proteção e, se necessário, fazer novos ajustes para evitar disparos indevidos (MORETO; ROLIM, 2011).

Nesse sentido, Hossack et al. (2003) propuseram um sistema multi-agente (MAS, do inglês *Multi-Agent System*) baseado em dados de alarmes e registros de RDPs para automatização do processo de análise pós-falta. De acordo com os autores, para efetuar o diagnóstico pós-falta, engenheiros de proteção devem analisar as informações de diversos dispositivos (relés, disjuntores, RDP, etc.) para obter o melhor diagnóstico. No entanto, um conhecimento profundo do funcionamento do sistema ainda é exigido por profissionais para organizar dados e para correlacioná-los logicamente.

Davidson et al. (2006) apresentaram os resultados da aplicação *online* de sistemas multi-agentes para análise e tratamento do grande volume de informações operacionais associados ao SCADA e RDPs instalados num sistema de transmissão localizada no Reino Unido. O sistema multi-agentes implementado, intitulado *Protection Engineering Diagnostic Agents* (PEDA), foi testado durante o período de seis meses entre janeiro e junho de 2005. Nesse período foram tratados um total de dois milhões de alarmes, tendo identificado e classificado corretamente 402 ocorrências de falta. A aplicação do PEDA indicou que a tecnologia MAS atingiu resultados significativos para a automatização completa da análise pós-falta, entretanto, ainda deve ser aperfeiçoada em termos de robustez para aplicações industriais.

Dobakhshari e Ranjbar (2014) introduziram uma metodologia para diagnóstico de faltas utilizando medidas de unidades fasoriais sincronizadas (PMU, do inglês *Phasor Measurement Unit*) que pode representar uma nova linha de pesquisa aplicada a sistemas de potência. Essa abordagem tem a vantagem de utilizar uma fonte de dados independente do sistema de proteção, podendo aumentar a confiabilidade de um sistema de apoio à decisão. O problema de diagnóstico emprega sinais de tensão e corrente, antes e após a ocorrência de faltas, obtidas através de uma rede de medição de longa distância (WAMS, do inglês *Wide Area Measurement System*) consistindo de várias PMUs sincronizadas pelo sistema de posicionamento global (GPS, do inglês *Global Position System*). A formulação do problema é baseada na comparação entre os fasores esperados e os medidos pelas PMUs durante faltas.

A partir da revisão da literatura foi possível notar que os estudos sobre lógicas avançadas de processamento de alarmes são discretos e requerem o desenvolvimento de rotinas que possibilitem a aplicação prática de métodos de diagnóstico. Além disso, poucos trabalhos se preocupam com possíveis problemas de implementação que possam surgir devido à incompatibilidade técnica-prática, uma possível falta de dados e pessoal técnico especializado capaz de alimentar os algoritmos com as informações requeridas.

1.5 Métodos de diagnóstico investigados

Nesta seção são descritas as vantagens e desvantagens das metodologias consideradas nos estudos comparativos desta tese. Os métodos considerados abrangem as técnicas mais utilizadas na literatura recente e classificados conforme divisão definida por Mu et al. (2012). As técnicas analisadas são: método GRNN+AG; método IA; e método HC+BIP.

1.5.1 Método GRNN+AG

O método híbrido GRNN+GA é um método de diagnóstico em dois níveis distintos de análise: nível de equipamento e nível de sistema. A análise em nível de equipamento relaciona alarmes e regras de funcionamento de esquemas de proteção para classificar eventos. A análise em nível de sistema emprega o conjunto de alarmes de disjuntores e eventos classificados localmente como dado de entrada para obtenção do diagnóstico da falta.

A metodologia empregada Cardoso Jr., Rolim e Zürn (2004) é utilizada para a classificação de eventos por meio de redes neurais artificiais. O AG empregado por Wen e Han (1995) para estimação da seção é adaptado para obter diagnósticos a partir da leitura dos alarmes de disjuntores e classificações de evento. A adaptação foi proposta por Toller (2011) e se limita a substituir alarmes por eventos como parâmetros de entrada do algoritmo. O AG adaptado é alimentado com todas as respostas fornecidas pelos módulos neurais. A função de avaliação (FA) é formulada como um problema de programação inteira cuja função de avaliação é dada por:

$$\min -w_1 + w_2 \sum s_i + w_3 \sum |e_j - e_j^*| \quad (1.1)$$

em que,

w_1 é um número suficientemente grande para garantir a minimização;

w_2 e w_3 são pesos da função de avaliação;

s_i é a condição da seção i (1, falta; 0, normal);

e_j é a condição do evento j (1, operou; 0, não operou);

e_j^* é a condição esperada do evento j (1, deveria operar; 0, caso contrário).

Em relação ao problema abordado, a metodologia GRNN+AG apresenta as seguintes vantagens:

- o processo de aprendizado da GRNN ocorre em um único passo (não é iterativo);
- o resultado da GRNN é limitado aos valores mínimos e máximos das observações;
- base de conhecimento permite a inclusão de padrões de funcionamento de qualquer sistema de proteção;
- novos cenários de falta podem ser aprendidos automaticamente, bastando adicionar novas regras à base de treinamento da GRNN;
- a divisão do problema em dois níveis permite o uso de bases de conhecimento reduzidas;
- modelo de otimização permite a estimação da seção em falta e a identificação dos eventos falsos e falhos.

Por outro lado, o método GRNN+AG apresenta as seguintes desvantagens:

- pode convergir a um mínimo local da função de avaliação, devido à erros na classificação de eventos;
- dificuldade em garantir um resultado confiável, pois a GRNN depende de um conjunto de amostras significativas;
- a criação da base de conhecimento é realizada heurísticamente e depende de especialistas que conheçam o funcionamento de todos os sistemas de proteção;
- modelo de otimização não restringe o número de alarmes e eventos indevidos;
- não permite a identificação de falha na fonte CC de SEs;
- alto custo computacional;
- o AG não garante resolução do problema modelado na otimalidade;
- grande número de parâmetros devem ser ajustados empiricamente para o correto funcionamento da GRNN e do AG.

1.5.2 Método IA

A metodologia proposta por Leão, Pereira e Mantovani (2010) é baseada em um modelo de programação binária irrestrita (UBP, do inglês *Unconstrained Binary Programming*) e resolvida por otimização artificial imunológica. O modelo UBP é formulado

a partir da teoria de recobrimento de conjuntos parcimoniosa, cujo objetivo é minimizar a seguinte função de avaliação:

$$\min k_1 \sum_{i=1}^{nf} Co_i + k_2 \sum_{i=1}^{nf} + k_3 \left(\sum_{j=1}^{ns} s_j + \sum_{h=1}^{nb} b_h \right) \quad (1.2)$$

em que,

k_1, k_2 e k_3 são pesos da função de avaliação, tal que $k_1 > k_2 > k_3$;

nf é o número de relés de proteção;

ns é o número de seções em falta;

nb é o número de fontes de corrente contínua (CC) do sistema elétrico;

$$Co_i = \begin{cases} 1, & \text{se o alarme } i \text{ é reportado e esperado} \\ 0, & \text{se o alarme } i \text{ é reportado e não é esperado} \end{cases}$$

$$ln_i = \begin{cases} 1, & \text{se o alarme } i \text{ é inconsistente} \\ 0, & \text{caso contrário} \end{cases}$$

$$s_j = \begin{cases} 1, & \text{se o seção } j \text{ está em falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$b_h = \begin{cases} 1, & \text{se a fonte CC } h \text{ é considerada falha} \\ 0, & \text{caso contrário} \end{cases}$$

Na metáfora de sistemas imunológicos, cada célula é uma possível solução do problema e é formada por uma sequência binária de genes. Um gene é formado de acordo com as condições de cada seção (em falta ou normal) e de cada fonte de corrente contínua (CC) de subestações (falho ou normal). Para determinar a condição do gene é calculado o estado esperado de relés a partir dos alarmes reportados de relés e disjuntores. O cálculo dos estados esperados dos relés de proteção é realizado por meio da seguinte equação:

$$f_i = \text{MAX}_{j \in J_i} \left\{ s_j \cdot \left[1 - \text{ORC} \left(\sum_{k \in \Omega_{i,j}} c_{sck} \right) \right], s_j \cdot \left(1 - \sum_{t \in \Omega_{i,j}} f_{sct} \right) \right\} \cdot (1 - b_h) \quad (1.3)$$

em que,

$$f_i = \begin{cases} 1, & \text{se o relé } i \text{ é esperado} \\ 0, & \text{caso contrário} \end{cases}$$

$$c_{sck} = \begin{cases} 1, & \text{se o disjuntor } k \text{ é aberto} \\ 0, & \text{caso contrário} \end{cases}$$

$$f_{set} = \begin{cases} 1, & \text{se o alarme do relé } t \text{ é reportado} \\ 0, & \text{caso contrário} \end{cases}$$

t é o relé principal que deve falhar para causar atuação do relé i ;

$\Omega_{l_{i,j}}$ é o conjunto de disjuntores existentes no trecho entre o relé i e a seção j ;

$\Omega_{t_{i,j}}$ é o conjunto de seções j que são protegidas, simultaneamente, pelo relé principal t e pela retaguarda i ;

MAX é uma função que escolhe o valor do maior argumento;

ORC é uma função que resulta valor 1 se, pelo menos, um disjuntor c_{sck} é aberto.

O método IA apresenta as seguintes vantagens:

- o diagnóstico é realizado em etapa única;
- não utiliza conjunto de padrões de funcionamento da proteção;
- permite a estimação da seção em falta e a determinação dos disjuntores que atuaram indevidamente;
- permite identificar falhas na alimentação de relés (falta CC) em SEs.

Por outro lado, as desvantagens do método são as seguintes:

- não permite o aprendizado automático de novos cenários de falta;
- a equação (1.3) é específica do sistema testado por Leão, Pereira e Mantovani (2010) e precisa ser reformulada em SEPs que possuam sistemas de proteção mais complexos e próximos da realidade;
- apresenta dificuldades em cenários com falta em seções sem monitoramento da proteção e interligadas à área monitorada do SEP;
- apresenta alto custo computacional;
- modelo UBP não restringe o número de alarmes indevidos e não permite a identificação dos relés que atuaram indevidamente;
- o IA não garante resolução do problema modelado na otimalidade;
- mudanças topológicas implicam na mudança da função de avaliação dos estados esperados de relés;
- grande número de parâmetros devem ser ajustados empiricamente para o correto funcionamento do IA.

1.5.3 Método HC+BIP

A metodologia HC+BIP proposta por Fritzen et al. (2012) é dividida em dois níveis de análise: equipamento (alarmes geram eventos) e sistema (eventos geram diagnósticos). Uma HC é empregada para classificar eventos a partir dos alarmes reportados. Um modelo BIP baseado no problema SCP e no princípio da parcimônia foi formulado para estimação da seção. Abaixo são apresentados os conjuntos, parâmetros e variáveis utilizados no modelo BIP. A nomenclatura dos conjuntos utilizada por Fritzen et al. (2012) foi modificada pra ficar de acordo com a nomenclatura definida no capítulo 4.

Conjuntos

I é o conjunto de índices dos diagnósticos;

J é o conjunto de índices dos eventos e alarmes de disjuntores;

D_j é o conjunto de índices dos diagnósticos associados ao evento j ;

E_i é o conjunto de índices dos eventos e alarmes associados ao diagnóstico i .

Parâmetros

$$e_j = \begin{cases} 1, & \text{se o evento } j \text{ é acionado} \\ 0, & \text{caso contrário} \end{cases}$$

w_1, w_2, w_3 são os pesos da FO.

Variáveis

$$d_i = \begin{cases} 1, & \text{se o diagnóstico } i \text{ é escolhido para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$s_j = \begin{cases} 1, & \text{se o evento } j \text{ é falso} \\ 0, & \text{caso contrário} \end{cases}$$

$$f_j = \begin{cases} 1, & \text{se o evento } j \text{ é falho} \\ 0, & \text{caso contrário} \end{cases}$$

Modelo

$$\min w_1 \sum_{j \in J} s_j + w_2 \sum_{j \in J} f_j + w_3 \sum_{i \in I} d_i \quad (1.4)$$

sujeito a

$$s_j + \sum_{i \in D_j} d_i \geq e_j \quad \forall j \in J \quad (1.5)$$

$$d_i \leq f_j \quad \forall i \in I, \forall j \in \{E_i : e_j = 0\} \quad (1.6)$$

$$d_i \in \{0,1\} \quad \forall i \in I \quad (1.7)$$

$$s_j, f_j \in \{0,1\} \quad \forall j \in J \quad (1.8)$$

A eq. (1.4) é a FO do modelo, em que $w_1 \geq w_2 \geq w_3$ são os pesos empregados para refletir a importância relativa de cada variável de decisão e a característica do SEP monitorado. Fritzen et al. (2012) justificam que w_1 é maior que w_2 porque alarmes falsos são mais raros que alarmes falhos em sistemas de proteção de sistemas de proteção. A restrição (1.5) determina que um evento deve estar associado a um diagnóstico ao menos, caso contrário, o evento é considerado falso. Os alarmes falhos são determinados pela restrição (1.6). As restrições (1.7) e (1.8) são restrições de domínio das variáveis de decisão.

Na resolução do modelo BIP foi empregado o *solver* comercial *IBM ILOG CPLEX Optimization Studio* versão 12.4 com configurações *default*. As principais vantagens do método HC+BIP são as seguintes:

- a modelagem do problema em dois níveis permite o uso de bases de conhecimento reduzidas;
- a base de conhecimento permite a inclusão de padrões de funcionamento de qualquer sistema de proteção;
- a HC não possui parâmetros a serem ajustados;
- a HC é matematicamente simples e de fácil implementação;
- o modelo BIP permite estimar a seção em falta, identificar os disjuntores com operação indevida e identificar os eventos falsos e falhos;
- os métodos exatos utilizados pelo *solver* possibilitam resolver o problema modelado na otimalidade ou encontrar a diferença entre a menor solução factível e o maior limitante inferior (*gap*);
- o método apresenta baixo custo computacional.

As desvantagens da metodologia são as seguintes:

- a metodologia em dois níveis pode convergir a um mínimo local da função de avaliação, devido à erros na classificação de eventos;
- requer a elaboração de padrões de funcionamento dos sistemas de proteção;
- mudanças topológicas implicam na mudança do conjunto de padrões;
- a HC não emprega qualquer lógica comportamental da proteção durante a análise;
- os pesos da FO do modelo BIP deve ser ajustado empiricamente e deve refletir a característica de funcionamento do sistema de proteção do SEP analisado;
- o critério $w_1 \gg w_2$, pode induzir o modelo a encontrar soluções com mais eventos falhos que eventos reportados;
- modelo BIP não restringe o número de alarmes indevidos;
- o método não permite identificar relés com atuação indevida;
- o método não permite identificar falta CC em SEs.

1.6 Contribuições da tese

Do ponto de vista conceitual, as principais contribuições da tese são as seguintes:

- 1) desenvolvimento de um processador inteligente de alarmes que permite a conexão de métodos de diagnóstico ao sistema SCADA em tempo real. As lógicas avançadas de gerenciamento de alarmes incorporam rotinas de filtragem de alarmes, mapeamento de eventos e identificação da topologia da rede a partir dos alarmes reportados;
- 2) desenvolvimento de metodologia para reordenação cronológica de alarmes para tratar atrasos operacionais de dispositivos de proteção e erros cronológicos na aquisição de dados via sistema SCADA;
- 3) desenvolvimento de um gerador automático de padrões de eventos. O gerador permite a criação de regras para modelos de otimização de acordo com a topologia da rede e é aplicável em sistemas de proteção que atendam às normas estabelecidas nos Procedimentos de Rede do Operador Nacional do Sistema (ONS, 2010);
- 4) formulação de modelos de programação matemática para diagnóstico de faltas em SEPs que permitam a estimação da seção em falta; a restrição de diagnósticos com um número máximo de alarmes falsos ou falhos; e a identificação de dispositivos de proteção com atuação indevida e das fontes CC de SEs com falha;

- 5) formulação de modelo de programação matemática considerando a metodologia de diagnóstico em dois níveis e que permite a resolução do problema de forma integrada e simultânea.

1.7 Estrutura do trabalho

Este trabalho foi estruturado em sete capítulos, incluindo a introdução. O capítulo 2 aborda a definição e conceitos relacionados ao processamento inteligente de alarmes e ao problema de estimação da seção em falta em SEPs. Também são descritos as ferramentas empregadas atualmente para auxílio na tomada de decisão durante a operação de um sistema de potência.

Os capítulos 3 e 4 apresentam a metodologia proposta no trabalho. No capítulo 3 são descritas as rotinas desenvolvidas no processador inteligente de alarmes para a reordenação cronológica de alarmes, filtragem de alarmes, mapeamento de eventos e geração de padrões de funcionamento da proteção de acordo com a topologia de rede. O capítulo 4 descreve os modelos de programação matemática formulados para estimação da seção em falta.

Os capítulos 5 e 6 apresentam os resultados computacionais da metodologia proposta. O capítulo 5 discute os resultados experimentais obtidos pelo processador de alarmes, enquanto o capítulo 6 discute os resultados de testes computacionais envolvendo os métodos de diagnóstico propostos nesta tese e outros métodos presentes na literatura. Por fim, as conclusões obtidas ao longo do trabalho e sugestões para trabalhos futuros são apresentadas no capítulo 7.

2 CARACTERIZAÇÃO DO PROBLEMA DE DIAGNÓSTICO

2.1 Considerações gerais

O presente capítulo descreve os aspectos operativos referentes à análise das perturbações, desde a investigação das causas até a determinação de medidas preventivas e corretivas. Primeiramente, é apresentada uma visão geral do problema de estimação da seção em falta e as principais características. Por fim, é apresentada a definição de um processador inteligente de alarmes e os problemas inerentes ao processo de diagnóstico por meio de alarmes.

2.2 Registradores para análise de perturbações

O uso de registradores de perturbações para localização de faltas em linhas de transmissão tem sido objeto de pesquisa desde a invenção do registrador magnético por Knapp (1941). Esse sistema foi desenvolvido com o objetivo de registrar os efeitos de faltas transitórias e permanentes para posterior inspeção visual. Inicialmente, o uso destes dispositivos ficou restrito a localização de faltas monofásicas (STRINGFIELD; MARIHART; STEVENS, 1957). O primeiro relato do uso de oscilografias em sistemas reais foi realizado por Atkins (1949) e representou um grande avanço quanto ao entendimento de fenômenos eletromagnéticos.

O SEP é dotado de sistemas supervisórios capazes de monitorar um vasto número de variáveis digitais e analógicas a partir do advento de relés microprocessados e registradores digitais. A análise de uma perturbação pode levar em conta dados de diferentes fontes de dados: relés, disjuntores, oscilógrafos analógicos, registradores de sequências de eventos (SER, do inglês *Sequence-Of-Event Register*), registradores de distúrbios dinâmicos (DDR, do inglês *Dynamic Disturbance Register*), RDPs e PMUs (PSRC, 2005; 2006).

Por outro lado, o aumento no número de dados monitorados tornou a atividade de análise muito mais desafiadora. Cabe ao engenheiro responsável utilizar o conjunto de dados da melhor forma para inferir as ocorrências da rede e, especialmente, identificar o desempenho dos sistemas de proteção (PSRC, 2006). A Figura 2.1 apresenta a classificação dos registradores comumente utilizados para análise de perturbações.

Figura 2.1 – Categorias e dispositivos para o monitoramento de distúrbios



Fonte: Adaptada de PSRC (2006).

Durante um longo período, os oscilógrafos analógicos foram a principal fonte de dados em regime transitório, operando em uma faixa de frequências entre 1000 e 1200 Hz. Com o passar do tempo, essa tecnologia se tornou obsoleta e foi, gradativamente, substituída pelos RDPs. O RDP, comumente utilizado em usinas geradoras, registram os valores instantâneos de tensão e corrente com taxas de amostragem que variam entre 64 a 320 amostras por ciclo (IBRAHIM, 2011). No entanto, o uso de RDPs ainda é limitado à análise “pós-morte” de perturbações, onde o detalhamento do tipo de falta e a avaliação da proteção são realizados. Além disso, e apesar da precisão dos dados, o RDP leva em torno de 10 minutos para transmitir os dados para os centros de controle, inviabilizando a sua aplicação para diagnóstico de faltas em tempo real (BI; LI, 2007).

Os DDRs são registradores para análise de faltas, detecção e análise de oscilações de potência, quantificação de mudanças repentinas nos parâmetros do SEP e para obtenção de dados para verificação de modelos de estabilidade. Os DDRs armazenam valores RMS ou fasores de tensão e corrente, sendo o tempo da duração de gravação dos dados ajustado experimentalmente. O DDR pode ser um dispositivo dedicado ou integrado junto a um registrador de falta, cujos dados podem ser obtidos por meio de PMUs sincronizadas via GPS (PSRC, 2006).

Os eventos de curta duração consistem de fenômenos elétricos que não afetam a estabilidade do sistema. O SER registra o instante de operação e o estado binário dos dispositivos da subestação (relés, disjuntores transformadores) e esquemas de controle (manual ou automático). Tipicamente, esse registro é realizado a partir da ocorrência da falta, estendendo-se por até 50 ciclos ou até o tempo necessário para isolar a falta por parte do sistema de proteção. Sua aplicação abrange a avaliação do desempenho da proteção, localização de faltas e verificação de parâmetros do sistema (HERTZ; FAUQUEMBERGUE, 1992; PSRC, 2006).

2.3 Definição do problema de estimação da seção em falta

O sistema de potência consiste de diversas seções incluindo linhas de transmissão, transformadores, barramentos, etc. Cada seção é protegida por um esquema de proteção próprio, cuja função é detectar o estado anormal de operação e atuar com objetivo de mitigar possíveis efeitos da falta no sistema elétrico. A proteção em si pode ser efetuada por inúmeros dispositivos, na qual se destacam os relés de proteção e disjuntores, além de equipamentos de comunicação que auxiliam e aumentam a confiabilidade do sistema (ANDERSON, 1999).

Durante as contingências devido à faltas, a atuação de relés e disjuntores espalhados pelo sistema elétrico dá origem a um grande volume de mensagens de alarmes que é enviado através dos sistemas SCADA ao COS. No caso de sistemas de transmissão esses alarmes são enviados ao EMS, enquanto que para os sistemas de distribuição esses alarmes são enviados ao sistema de gestão de distribuição (DMS, do inglês *Distribution Management System*) (LEÃO, 2011).

Após o recebimento dos alarmes no EMS, o operador necessita selecionar as mensagens mais relevantes, diagnosticar a ocorrência, e restabelecer o sistema a um estado seguro de operação. A identificação do segmento ou equipamento em falta deve ocorrer a partir de informações fornecidas pelos dispositivos de proteção e é conhecida como estimação da seção em falta (FSE, do inglês *Fault Section Estimation*) (LUO; KEZUNOVIC, 2008).

A tarefa de estimar a seção em falta tende a crescer em complexidade em grandes desligamentos devido ao aumento substancial de alarmes reportados, o que pode tornar o sistema de alarmes um obstáculo a mais para a capacidade do operador em identificar a causa raiz dos problemas a serem tratados (CARDOSO JR.; ROLIM; ZURN, 2004). Em centros de controle não automatizados, somente faltas relacionadas à operação do sistema de proteção costumam ser analisadas. Os demais registros, apesar da possibilidade de evidenciar um defeito evolutivo, passam despercebidos até que uma falta grave chame a atenção dos especialistas (RODRIGUES et al., 2010).

2.3.1 Variáveis do problema

De acordo com a ISA-18.2 (2009), um alarme corresponde a uma indicação audível ou visual que informa os operadores sobre o mau funcionamento de equipamentos, desvio de processo ou condição anormal que deve ser tratada. No problema de estimação da seção em falta, um alarme corresponde à variação de estado de um dispositivo de proteção do SEP.

Dependendo do tipo de dispositivo de proteção monitorado, o alarme resultante possui um significado específico. No caso de relés, o alarme a_r é definido como:

$$a_r = \begin{cases} 1, & \text{se o relé operou} \\ 0, & \text{caso contrário} \end{cases} \quad (2.1)$$

No caso de disjuntores, o alarme a_{cb} é definido da seguinte forma:

$$a_{cb} = \begin{cases} 1, & \text{se o disjuntor abriu} \\ 0, & \text{caso contrário} \end{cases} \quad (2.2)$$

De acordo com Wen, Chang e Srinivasan (1995), alarmes podem ser classificados em falhos ou falsos, e estão associados às características do evento (faltas múltiplas, falha no canal de comunicação, mau desempenho de relés, etc.). Um alarme é considerado falho quando o alarme é esperado, mas não reportado. Um alarme é considerado falso quando o alarme é reportado, mas não esperado. Além dessas classificações, neste trabalho é introduzido o conceito de “alarme inexistente”, que corresponde aos alarmes falhos pertencentes à SEs com falha na alimentação de dispositivos ou com falha na unidade terminal remota (UTR).

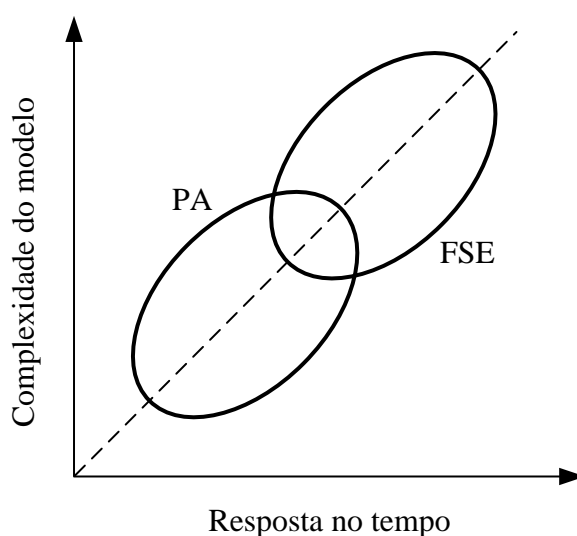
Segundo Oliveira et al. (2016), um evento é definido como um conjunto de alarmes associados à uma seção do SEP com esquema de proteção próprio. O número de eventos existentes em uma falta está relacionado ao número de esquemas de proteção sensibilizado pelo distúrbio. Se a metodologia de diagnóstico é dividida em dois níveis, então um evento pode ser considerado falho ou falso, cujas classificações de inconsistência são análogas às de alarme falho e falso, respectivamente.

O diagnóstico é definido como a melhor explicação do conjunto de alarmes recebidos no sistema SCADA. O diagnóstico corresponde a informação explícita da falta e deve conter a informação necessária para o operador executar as ações necessárias. Neste trabalho, o diagnóstico é caracterizado pela indicação da seção em falta e pelos dispositivos de proteção com atuação indevida.

2.4 Processador inteligente de alarmes

De acordo com Kirschen e Wollenberg (1992), um processador inteligente de alarmes é o resultado da junção de um processador de alarmes (PA) e métodos de FSE. O processador de alarmes tem a função de apresentar uma “fotografia” clara da condição do sistema elétrico ao operador, enquanto os métodos de diagnóstico têm como objetivo explicar os alarmes reportados. A Figura 2.2 mostra a distinção funcional destes módulos.

Figura 2.2 – Módulos que compõem um processador inteligente de alarmes



Fonte: Adaptada de Kirschen e Wollenberg (1992).

Os PAs devem ter um tempo de resposta pequeno e por isso devem basear-se em modelos mais simples para descrever o funcionamento do sistema de proteção. Os métodos de FSEs executam lógicas mais complexas e, portanto, requerem modelos mais complexos, já que um tempo de resposta maior é, usualmente, aceitável para estes sistemas. Além disso, os PAs e os FSEs não enxergam o fluxo de alarmes como reflexo da evolução do sistema, mas tentam dividir ele em eventos discretos que podem ser analisados separadamente. Uma janela de tempo deve ser definida para capturar todos os alarmes causados devido a um determinado evento (LEÃO, 2011).

A disponibilidade de um PIA para auxílio à operação em tempo real, capaz de identificar a causa do desligamento é de extrema importância ao passo subsequente, à restauração do sistema elétrico, seja em nível de subestação ou centro de controle. (LEÃO; PEREIRA; MANTOVANI, 2010, FRITZEN et al., 2012). Dados históricos de 2002 referentes a desligamentos da concessionária inglesa de energia, *SP PowerSystems*, são

relatados por Davidson et al. (2006), e confirmam as vantagens advindas do uso desta ferramenta computacional.

De maneira geral, é esperado que um PIA seja robusto para alcançar os seguintes objetivos (GUAN; KEZUNOVIC, 2009; STAHLHUT; HEYDT; CARDELL, 2008; MU et al., 2012):

- agrupar eventos de acordo com a ordem cronológica de alarmes;
- lidar com fluxo contínuo de alarmes;
- filtrar alarmes redundantes e que não condizem com o evento;
- tratar incertezas decorrentes do mau funcionamento de dispositivos de proteção;
- gerar um único diagnóstico através de uma relação de causa-efeito;
- automatizar o processo para obter respostas rapidamente;
- reconhecer os diferentes esquemas de proteção empregados no SEP;
- adaptar-se a mudanças topológicas da rede elétrica;
- identificar a importância, gravidade ou impacto de um determinado evento;
- fornecer informação gráfica e numérica de forma concisa e de fácil interpretação.

2.4.1 Problemas envolvidos

A má gestão de alarmes é um grande obstáculo para alcançar a excelência operacional de processos industriais, sendo uma das principais causas de interrupções não programadas. A norma ANSI/ISA-18.2 (2009) estabeleceu as terminologias, modelos e processos para a implementação e gestão eficiente de um sistema de alarmes. O objetivo básico da ISA-18.2 (2009) é aumentar a segurança de processos industriais evitando consequências indesejáveis decorrentes de problemas comuns de sistemas de alarmes. De acordo com Araújo (2010), o sistema de alarmes em um sistema de potência apresenta os seguintes problemas:

- alarmes gerados e ignorados pelo operador;
- grande número de alarmes gerados para pequenos distúrbios;
- lista de alarmes cheia, mesmo em condições normais de operação;
- alarmes continuamente presentes na lista de alarmes por longos períodos de tempo;
- operadores desconhecem a ação a ser executada após alarmes;
- durante um distúrbio o operador é sinalizado com vários alarmes que ele não sabe como priorizar;

- diferentes configurações de alarmes são atribuídas por diferentes operadores;
- surgimento de muitos alarmes em um curto período de tempo (PIRES, 2010);
- efeito “cascata de alarmes”, cujo conceito está associado ao aparecimento de eventos secundários originados a partir de um evento primário (PIRES, 2010).

Uma grande quantidade de alarmes é a primeira razão para o operador não conseguir realizar todas as ações necessárias. Araújo (2010) relaciona os índices de desempenho estabelecidos pela Associação de Equipamentos e Materiais de Engenharia (EEMUA, do inglês *Engineering Equipment and Materials Users Association*) em sua publicação 191 de 2007, para a avaliação do funcionamento adequado de um sistema de alarme.

A Tabela 2.1 apresenta a comparação entre os valores observados em sistemas de energia e o recomendado pela EEMUA 119 (2007). É possível verificar que os sistemas de alarme de setores de energia estão muito aquém do desempenho considerado aceitável pela instituição.

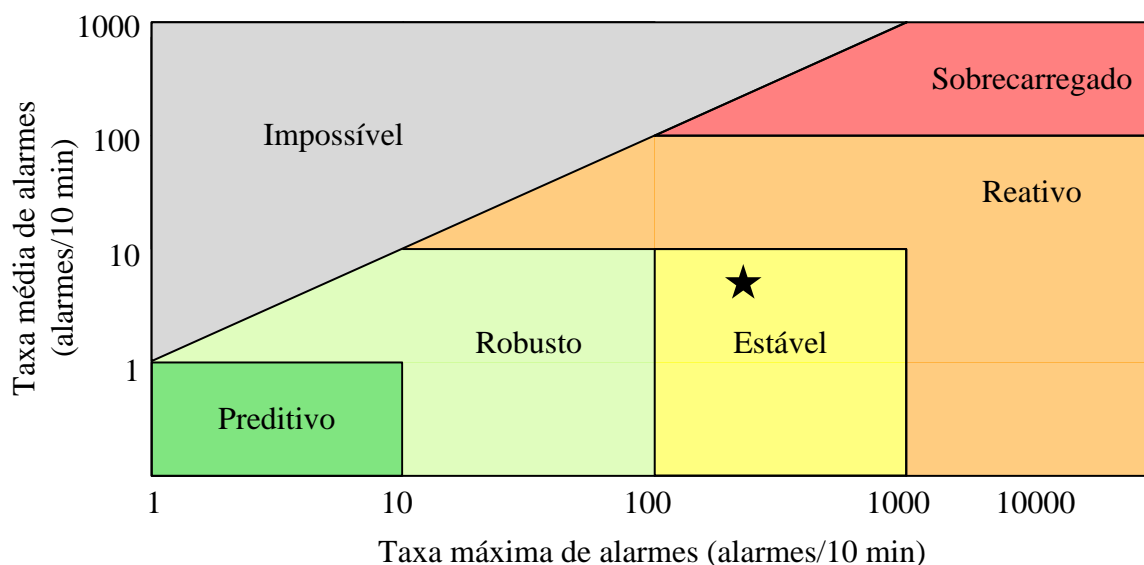
Tabela 2.1 – Índices de desempenho EEMUA x SEP

Indicadores	EEMUA	SEP
Alarmes por dia	144	2000
Alarmes constantes	9	65
Pico de alarmes por 10 minutos	10	350
Média de alarmes por 10 minutos	1	8
Distribuição de prioridades (baixa/média/alta)	80/15/5	25/40/35

Fonte: Adaptada de ARAÚJO (2010).

Conforme estabelece a norma EEMUA 191 (2007), a Figura 2.3 mostra a relação entre a taxa média de alarmes e o número máximo de alarmes por intervalo de 10 min. O símbolo “★” indica o nível de desempenho de um sistema típico de energia.

Figura 2.3 – Classificação de um sistema de alarmes de um sistema de energia



Fonte: Adaptada de Brown (2003).

A classificação de desempenho do sistema de alarmes de um sistema de energia típico é definida como estável. A área triangular é definida como impossível, pois a média de alarmes não pode exceder o valor máximo de alarmes. A Tabela 2.2 apresenta o significado das classificações conforme a EEMUA 191 (2007).

Tabela 2.2 – Níveis de desempenho do sistema de alarmes

Nível	Descrição
Sobrecarregado	O sistema de alarme é sujeito a uma alta taxa contínua de alarmes e piora rapidamente durante distúrbios do processo.
Reativo	É considerado o nível inicial mínimo da maioria das plantas. O sistema de alarmes é caracterizado por alarmes persistentes sem nenhum significado real (alarmes “ <i>bad actors</i> ”).
Estável	O sistema é bem definido para a operação normal, mas menos útil durante distúrbios ou emergências. Além disso, problemas com alarmes “ <i>bad actors</i> ” devem ser mantido sobre controle.
Robusto	O sistema é confiável em qualquer modo de operação, incluindo operação normal, distúrbios e emergências.
Preditivo	O sistema de alarme é estável e provê a informação correta ao operador no momento certo para evitar distúrbios ou minimizar o impacto de qualquer distúrbio que possa ocorrer.

Mesmo que o sistema de gerenciamento de alarmes de um sistema elétrico seja capaz de atender aos requisitos dispostos em normas, ainda existe a possibilidade de desenvolvimento de técnicas dinâmicas que permitam melhorar o desempenho em tempo real do sistema de alarme (BROWN, 2003). A produção, aquisição e apresentação de alarmes pelo SCADA estão sujeitas a problemas associados ao tráfego de dados pela rede de comunicação. Os problemas mais comuns são (MALHEIRO et al., 2005):

- falta de sincronização entre subestações (fonte de dados) e o centro de operação (recepção) em conjunto com a atribuição de tempo ao alarme no instante da produção, podendo ocasionar em diferenças cronológicas na ordem de alarmes;
- inconsistência lógica de alarmes decorrente do fato da ordem cronológica estar incorreta. Esse tipo de inconsistência também pode estar vinculado à alteração de estado de um dispositivo para o mesmo estado que este já estava anteriormente, ou seja, ocorre uma sinalização no SCADA referente a uma variação de estado apesar de não haver qualquer atuação ou operação do dispositivo correspondente ao alarme;
- informações incompletas devido à ausência de alarmes esperados num determinado instante ou a manifestações de mensagens não associadas à ocorrência.

Existem outros problemas, não diretamente ligados ao SCADA, que também dificultam o desenvolvimento de um PIA, dos quais é possível citar:

- mapeamento incorreto e redundância de alarmes cadastrados no banco de dados da concessionária de energia. Esse problema pode se manifestar durante a leitura dos alarmes em tempo real com o surgimento de mensagens repetidas ou redundantes (JUNG et al., 2001);
- incerteza das informações disponíveis ao operador devido a atuações incorretas de esquemas de proteção causadas por falhas na abertura de disjuntores, ajustes incorretos em parâmetros de relés resultando em desligamentos indevidos em virtude de problemas de oscilação de potência, sobretensão, etc;
- informações corrompidas durante a transmissão de dados em razão de falhas na aquisição de dados, nos canais de comunicação e nas UTRs. Problemas em UTRs, invariavelmente implicam na perda completa de informações essenciais para análise do distúrbio;

- os sistemas elétricos de potência costumam variar em tamanho e em termos estruturais, podendo conter subestações modernas constituídas de diversos dispositivos inteligentes interligados através do protocolo de comunicação IEC-61850 (WEI, L. et al, 2011), coexistindo com subestações antigas que não possuem registro de sequência de eventos;
- dificuldade em modelar filosofias de proteção de acordo com os alarmes disponibilizados ao operador do sistema. Essa adversidade pode ser contornável caso haja engenheiros de proteção com experiência no sistema elétrico protegido com capacidade de passar esse conhecimento para o programa;
- conservadorismo no emprego de novas tecnologias no centro de controle por parte dos operadores. Essa atitude é compreensível, visto que em cenários reais de operação, a falta de convicção em uma solução correta pode levar operadores a abandonar a ferramenta a fim de prevenir futuros erros de decisão (RODRIGUES et al., 2010).

2.5 Considerações finais

Este capítulo apresentou o problema de diagnóstico de faltas em sistemas de potência e as ferramentas disponibilizadas no COS para o operador realizar a análise de distúrbios em tempo real. O problema de estimação da seção em falta e o processamento inteligente de alarmes são abordados no capítulo. Também foram discutidas as dificuldades encontradas para a formulação e desenvolvimento de um processador inteligente de alarmes que auxilie o operador na interpretação dos alarmes reportados e na tomada de decisão. Por fim, foram mostradas as justificativas e benefícios da adoção de um processador inteligente de alarmes junto ao sistema SCADA.

3 PROCESSADOR INTELIGENTE DE ALARMES

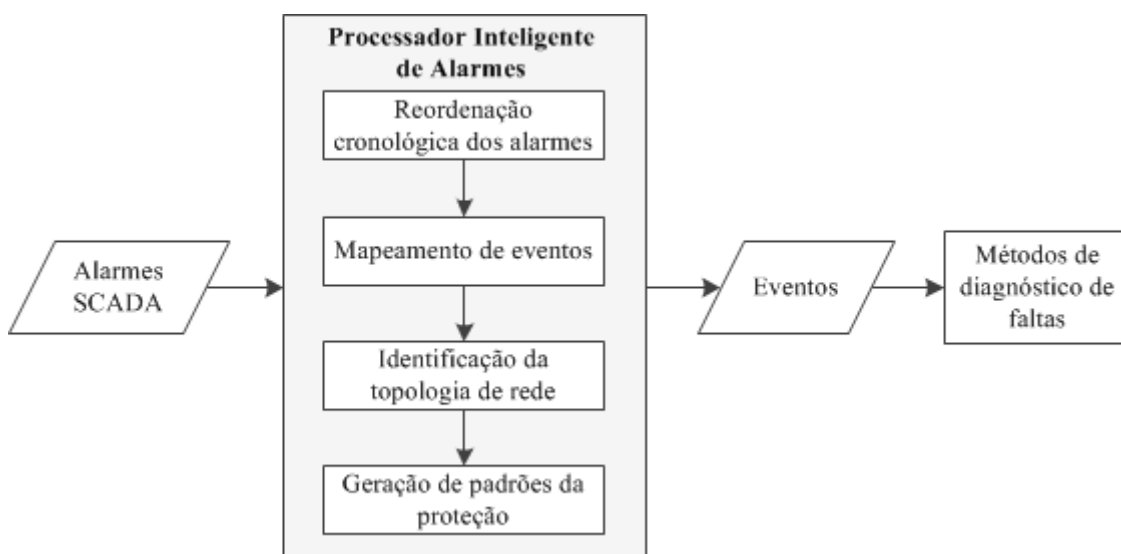
3.1 Considerações gerais

Este capítulo apresenta uma visão detalhada do processador inteligente de alarmes proposto para diagnóstico de faltas em sistemas elétricos de potência. Funções e lógicas avançadas de gerenciamento de alarmes foram incorporados ao processador para propiciar aplicação de modelos de otimização. Também são descritos os métodos incorporados ao PIA para reordenação cronológica de alarmes, mapeamento de eventos, identificação topológica da rede elétrica e geração automática de padrões de funcionamento de sistemas de proteção.

3.2 Metodologia proposta

De acordo com Leão (2011), o diagnóstico de faltas em tempo real deve ser computacionalmente eficiente, robusto em relação aos alarmes reportados e capaz de fornecer soluções precisas que permitam ao operador tomar as decisões corretas para restauração do sistema no menor intervalo de tempo possível. De forma a atender esses critérios, é proposto PIA que incorpora métodos para o pré-processamento de alarmes e métodos para estimação da seção em falta. A Figura 3.1 ilustra as rotinas desenvolvidas no PIA desde a leitura dos alarmes no SCADA até a identificação dos eventos para análise dos métodos de diagnóstico.

Figura 3.1 – Rotinas implementadas no PIA proposto



O processamento de alarmes inicializa imediatamente após o disparo do primeiro alarme no SCADA. A partir deste instante, todos os alarmes reportados são armazenados até que se encerre a janela de tempo. Neste trabalho, a duração da janela de tempo é ajustada em 60 segundos, cujo valor foi obtido heurísticamente. Um ajuste inadequado da janela de dado pode resultar em perda de informação útil para o diagnóstico ou distinção de eventos secundários, e aparecimento de ruídos entre os alarmes reportados.

3.3 Estrutura de dados

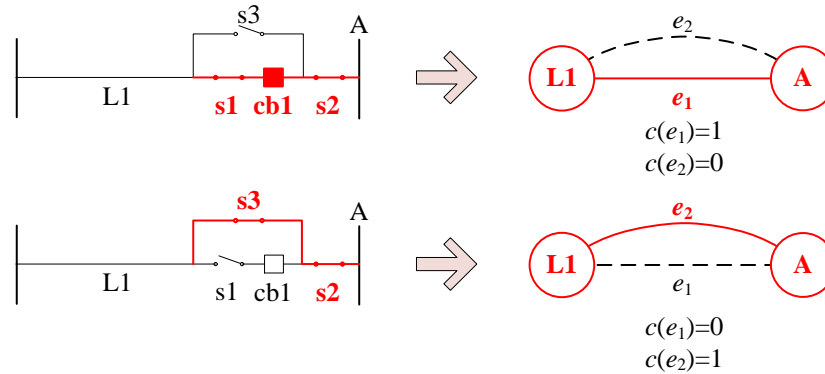
O processador de alarmes foi projetado para ser integrado a sistemas supervisórios existentes no COS e operado de forma independente. Dados reais do Sistema Aberto de Gerenciamento de Energia (SAGE/SCADA) referentes ao monitoramento do sistema de potência sob concessão da Companhia Estadual de Geração e Transmissão de Energia Elétrica (CEEE-GT) foram utilizados para a modelagem do banco de dados do problema. A estrutura de dados é embasada na teoria de grafos, cuja topologia de rede é representada por meio de uma lista de incidência em conjunto com listas auxiliares. Essa escolha visa acelerar as buscas no grafo com o intuito de determinar as filosofias de proteção ativas após uma mudança topológica.

A topologia da rede é obtida utilizando os estados de chaves seccionadoras e disjuntores fornecidos pelo SCADA. A topologia da rede é definida como $G = (V, E)$, em que V é o conjunto de componentes do SEP (vértices), $V = \{v_1, v_2, \dots, v_m\}$; enquanto E é o conjunto de dispositivos lógicos seccionadores (arestas), $E = \{e_1, e_2, \dots, e_n\}$. Um dispositivo lógico seccionador (DS) é definido como uma combinação lógica de dispositivos de chaveamento, conectados em série, que ligam dois equipamentos. Portanto, para cada aresta e_k ($1 \leq k \leq n$) existe um par de vértices $e_k = (V_i, V_j)$, sendo que $1 \leq i \leq m$ e $1 \leq j \leq m$.

Além disso, considere $D = \{d_1, d_2, \dots, d_q\}$ o conjunto de dispositivos de chaveamento e $S = \{S_1, S_2, \dots, S_k, \dots, S_n\}$ uma coleção de subconjuntos de D , $S \subset D$, em que $S(e_k)$ é o conjunto de dispositivos de chaveamento pertencentes à aresta e_k . Se todos os dispositivos de $S(e_k)$ estiverem fechados, é possível concluir que e_k também está fechada. Esta condição é representada na estrutura como $c(e_k) = 1$ (verdade). Qualquer chave $d_{ki} \in S_k$ aberta resulta na abertura da aresta e_k , ou seja, $c(e_k) = 0$ (falso).

Os conjuntos acima são utilizados para a representação topológica da rede e para o manuseio básico de alarmes. A Figura 3.2 apresenta o grafo equivalente para duas possíveis conexões entre uma linha de transmissão (L1) e uma barra (A).

Figura 3.2 – Grafo relativo a conexão entre uma linha e uma barra



As arestas com linhas contínuas representam os dispositivos lógicos seccionadores fechados, enquanto as com linhas tracejadas representam os abertos. O grafo representativo ao sistema teste é o seguinte:

$$\begin{aligned}
 V &= \{A, L1\}, \\
 E &= \{e_1, e_2\}, \\
 D &= \{cb1, s1, s2, s3\}, \\
 S(e_1) &= \{cb1, s1, s2\}, \\
 S(e_2) &= \{s2, s3\}.
 \end{aligned}$$

O estado $c(e_k)$ de cada aresta e_k depende dos estados individuais dos dispositivos de chaveamento pertencentes ao conjunto $S(e_k)$, e é utilizado para a determinação da topologia de rede. O primeiro exemplo da Figura 3.2 mostra que o disjuntor cb1 e as chaves s1 e s2 estão fechados, logo o dispositivo e_1 formado por essas chaves também estará fechado. Como o estado de e_2 depende do estado da chave de manobra s3, a qual está aberta, então esta aresta também estará aberta. O segundo exemplo mostra a mudança no grafo relativa ao fechamento da chave de manobra s3 e abertura dos dispositivos s1 e cb1.

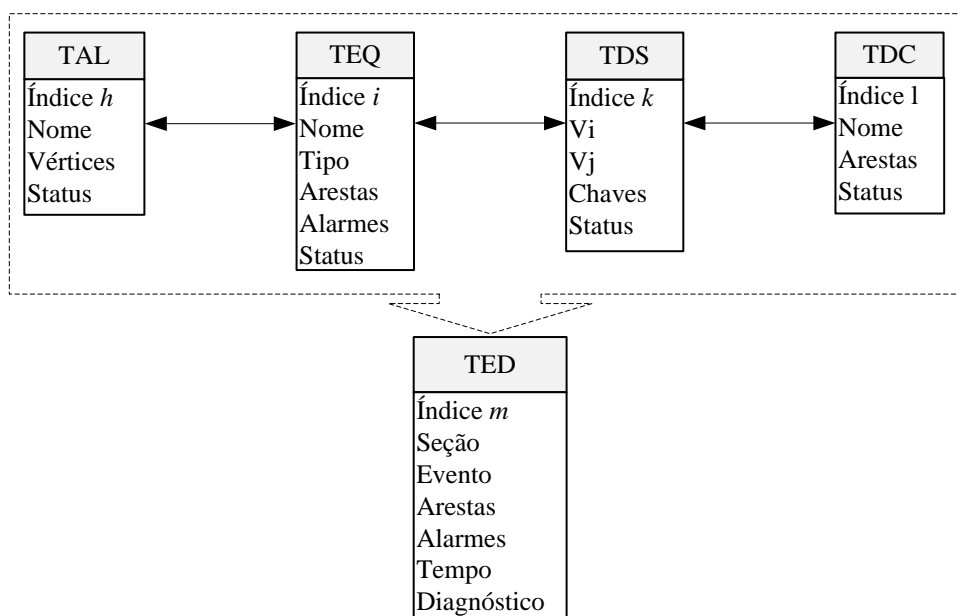
Com o objetivo de acelerar as operações de pesquisa no grafo e organizar dados para o diagnóstico são criados os seguintes conjuntos:

- $A = \{a_1, a_2, \dots, a_p\}$ é o conjunto dos alarmes de operação de relés;
- $AS(v_i) \subset A$ é o conjunto dos alarmes monitorados na seção v_i ;
- $VS(a_h) \subset V$ é o conjunto das seções monitoradas pelo alarme a_h ($1 \leq h \leq p$) e corresponde à relação inversa do conjunto AS ;
- $ES(v_i) \subset E$ é o conjunto dos DSs conectadas à seção v_i ;
- $ES'(d_l) \subset E$ é o conjunto de DSs do dispositivo de chaveamento d_l ($1 \leq l \leq q$) e corresponde à relação inversa do conjunto S .

3.3.1.1 Implementação da estrutura de dados

A pesquisa, leitura, escrita e a manipulação de dados na estrutura de dados devem ser otimizadas para permitir a implantação de métodos de análise automática de faltas (POPOVIC; KEZUNOVIC, 2012). Nesse sentido foi desenvolvida uma estrutura de dados específica para processamento de alarmes para reduzir o tempo necessário para a entrega de resultados necessários para o diagnóstico. A estrutura de dados proposta é mostrada na Figura 3.3 e é composta de cinco tabelas: tabela de equipamentos (TEQ), tabela de dispositivos lógicos seccionadores (TDS), tabela de dispositivos de chaveamento (TDC), tabela de alarmes (TAL), e tabela de equipamentos desconectados (TED).

Figura 3.3 – Estrutura de dados do PIA proposto



A tabela TEQ armazena os vértices do grafo, onde cada índice i corresponde a um equipamento v_i . A descrição dos campos da tabela TEQ é a seguinte:

- Nome: identificação do componente do SEP;
- Tipo: Tipo de equipamento;
- Arestas: contém os dispositivos lógicos seccionadores conectados ao equipamento v_i , ou seja, $ES(v_i)$. Essa informação é utilizada para o reconhecimento da vizinhança de v_i ;
- Alarmes: contém os alarmes monitorados pela proteção do equipamento v_i , ou seja, $AS(v_i)$. Essa informação é utilizada para acessar os dados da proteção durante o diagnóstico;
- Status: estado do vértice. Se o equipamento estiver energizado, possui conexão com uma unidade geradora, o status é igual a 1. Caso contrário, o valor é nulo.

A tabela TDS armazena as arestas do grafo, onde cada índice k representa um dispositivo lógico seccionador e_k . A descrição dos campos da tabela TDS é a seguinte:

- Vi: índice de TEQ referente ao primeiro vértice conectado por e_k ;
- Vj: índice de TEQ referente ao segundo vértice conectado por e_k ;
- Chaves: contém os dispositivos de chaveamento pertencentes à e_k , ou seja, $S(e_k)$. Essa informação é utilizada para determinar o estado da própria aresta e_k ;
- Status: estado do dispositivo lógico seccionador. Se, e somente se, todas as chaves da aresta estiverem fechadas, então a aresta está ligada e com valor igual a 1. Caso contrário, o valor de estado é nulo.

A tabela TDC armazena os dados de dispositivos de chaveamento (chaves seccionadoras e disjuntores), onde cada índice l representa uma chave d_l . A descrição dos campos da tabela TDC é a seguinte:

- Nome: identificação do dispositivo de chaveamento. A codificação do identificador deve possuir um formato que permita a distinção entre chave seccionadora e disjuntor, além de incluir o local de origem do ponto;
- Arestas: contém os dispositivos lógicos seccionadores que possuem d_l , ou seja, $ES'(d_l)$. Essa informação é utilizada para definir os estados das arestas $e_k \in ES'(d_l)$ após a variação de estado da chave d_l ;
- ID_SCADA: campo que relaciona a tabela TDC com a tag do SCADA;

- *Status*: estado do dispositivo de chaveamento. Se a chave d_l estiver aberta, então todas as arestas $e_k \in ES'(d_l)$ devem estar abertas. Caso contrário, se d_l estiver fechado, então o estado de cada $e_k \in ES'(d_l)$ deve ser checado em conjunto com os estados dos outros dispositivos de chaveamento contidos na aresta e_k .

A tabela TAL armazena os alarmes monitorados de relés de proteção, onde cada índice h representa um alarme a_h . A descrição dos campos da tabela TAL é a seguinte:

- Nome: identificação e descrição da função de proteção. A codificação utilizada deve possuir um formato que permita identificar se o alarme é de partida ou de *trip*, e se a função é temporizada ou instantânea;
- Vértices: contém os equipamentos monitorados pelo alarme a_h , $VS(a_h)$;
- ID_SCADA: campo que relaciona a tabela TAL com a *tag* do SCADA;
- *Status*: estado operacional do relé. Se a proteção atuou o estado é igual a 1 (verdadeiro), caso contrário, este valor é nulo.

A tabela TED armazena a lista de seções suspeitas de falta após uma contingência, onde cada índice m representa um suspeito e_m . A descrição dos campos da tabela TED é a seguinte:

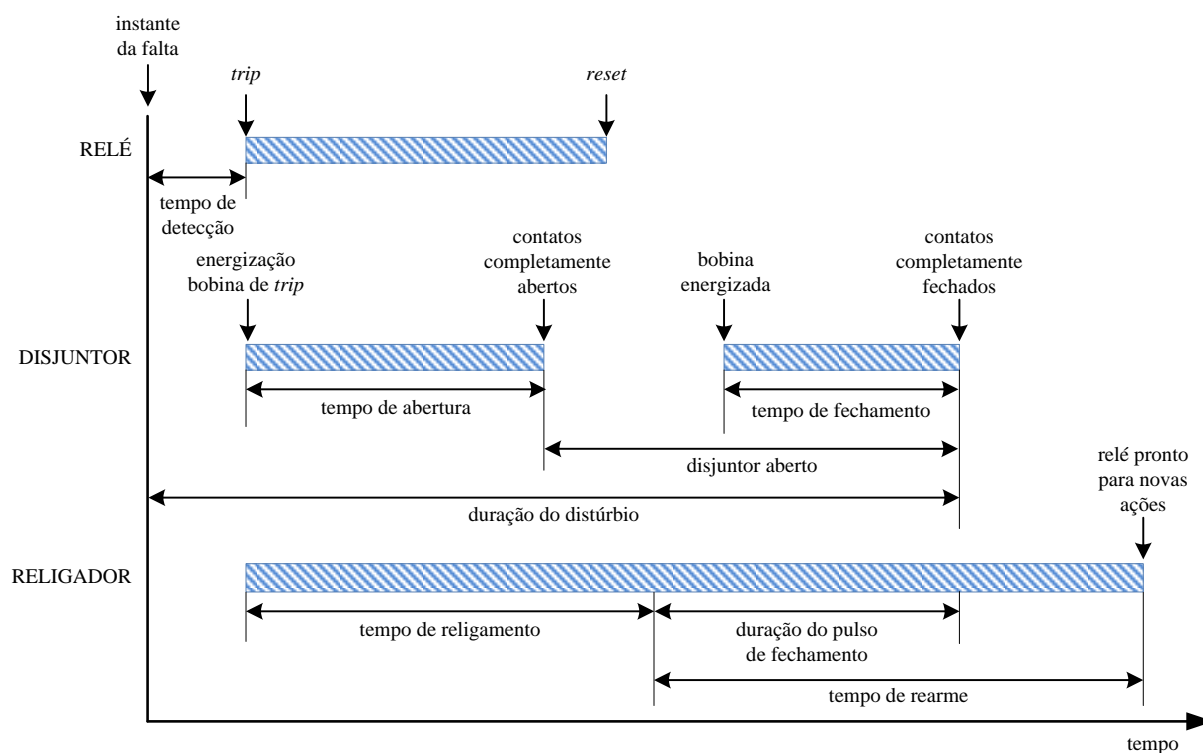
- Seção: índice de TEQ referente à seção suspeita e_m ;
- Evento: índice do evento a ser diagnosticado;
- Arestas: armazena a topologia da rede imediatamente anterior à ocorrência da falta;
- CBs: armazena os índices de TDC que sofreram perturbação durante o evento e associados com a seção e_m ;
- Alarmes: índices de TAL referente aos alarmes disparados durante o evento e associados com a seção e_m ;
- Tempo: armazena o instante de início (recebimento do primeiro alarme) e de finalização (recebimento do último alarme) do evento;
- Diagnóstico: Solução encontrada pelo método de estimação da seção em falta e armazenada para fins de histórico.

3.4 Reordenação cronológica de alarmes

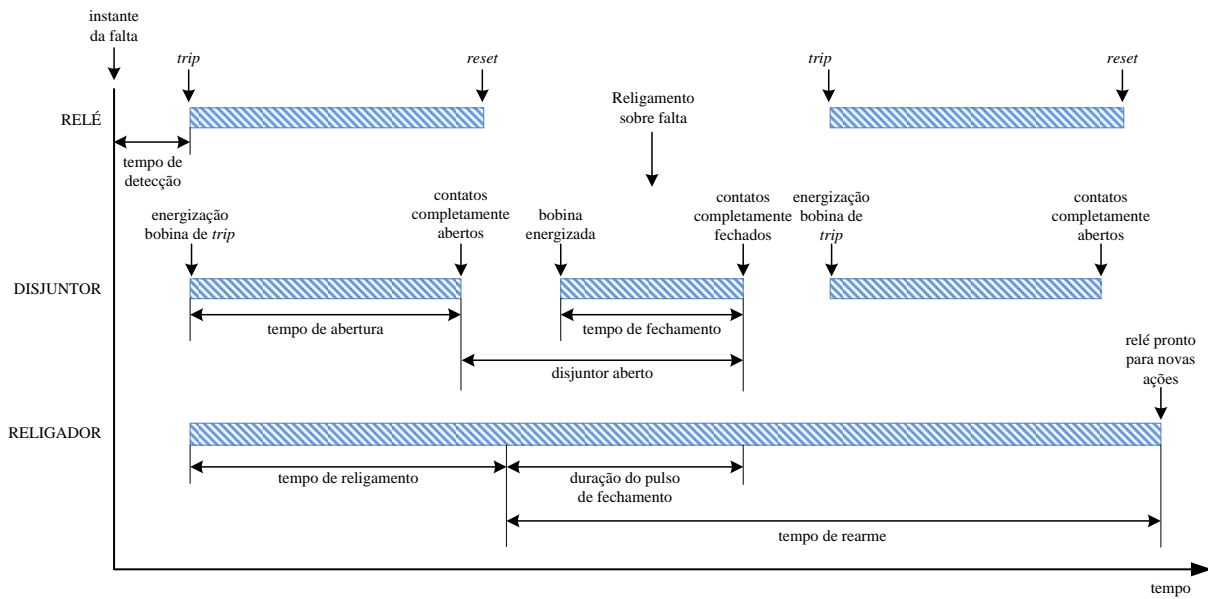
A cronologia incorreta de alarmes é um problema causado, majoritariamente, por erros na aquisição e na transmissão de dados em uma rede de longa distância (WAN - *Wide Area Network*). Além disso, falhas na UTR da subestação pode, invariavelmente, implicar na perda completa de dados que podem ser essenciais para uma análise de distúrbio (MALHEIRO et al., 2005). Com base nisso, foi proposta uma metodologia para reordenação de alarmes baseado na sequência lógica de eventos por meio de máquinas de estados finitos. O diagrama de máquina de estados demonstra o comportamento de um elemento por meio de um conjunto finito de transições de estado, ou seja, uma máquina de estados (LARMAN, 2002).

No contexto da pesquisa, cada estado corresponde ao estado do alarme reportado e cada transição está associada a uma condição específica. A sequência de religamento automático de LTs com uma única tentativa (*single-shot*) é utilizada para a modelagem do diagrama de transição de estados para alarmes associadas a linhas de transmissão. Os diagramas de tempo para o esquema de religamento automático *single-shot* para faltas transitórias e permanentes são mostrados na Figura 3.4 e na Figura 3.5, respectivamente.

Figura 3.4 – Religamento automático *single-shot* para faltas temporárias



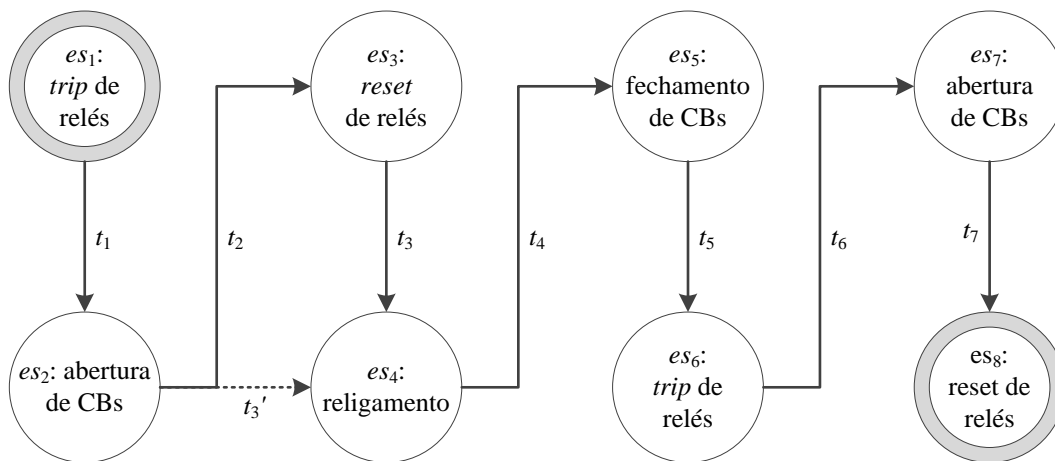
Fonte: Adaptada de ALSTON (2011).

Figura 3.5 – Religamento automático *single-shot* para faltas permanentes

Fonte: Adaptada de ALSTON (2011).

A Figura 3.6 apresenta o diagrama de transição de estados para alarmes associadas a linhas de transmissão, em que cada círculo representa um estado (es_1 - es_8) e cada arco representa a transição de um estado para outro (t_1 - t_7).

Figura 3.6 – Diagrama de transição de estados da proteção de LTs



O diagrama acima pode ser aplicado tanto para faltas temporárias quanto permanentes. Após uma falta, é esperada a atuação dos relés de proteção principal da linha (es_1), envio de *trip* aos disjuntores da linha (t_1) e abertura destes disjuntores (es_2). Após um intervalo de tempo ajustado no relé (t_2), a função de proteção sensibilizada é “resetada” (es_3). Dependendo da configuração do sistema supervisor, o *reset* do relé não gera alarme. Neste caso, o es_3 é

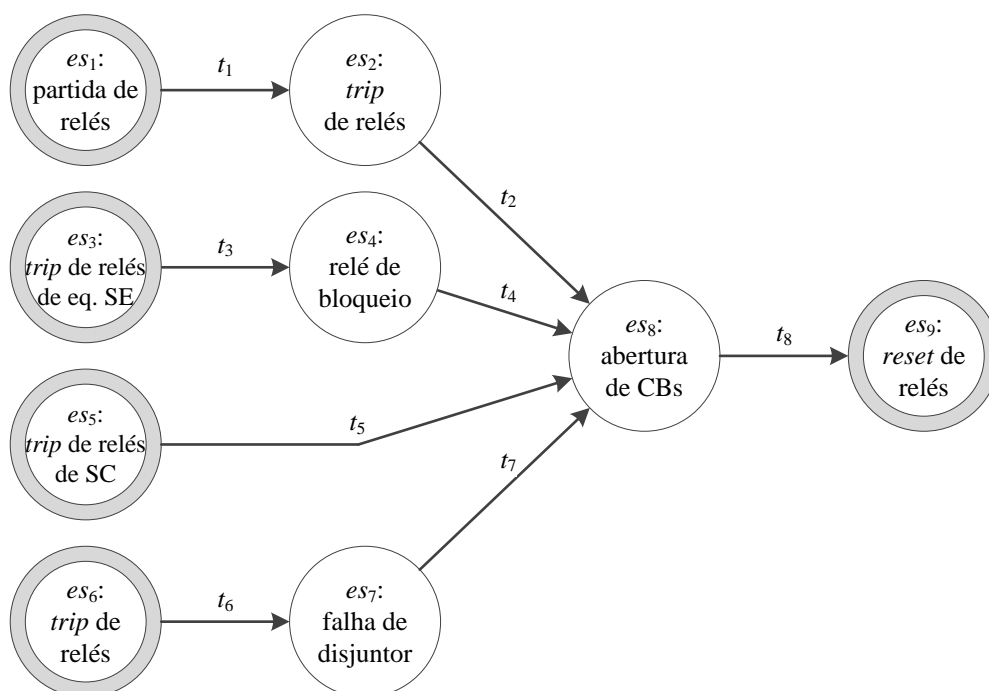
omitido da máquina de estado e a transição t_2 substituída por t_3' . Se a linha possuir função de religamento automático 79, a transição t_3 , ou t_3' , é executada. O disparo da função 79 (es_3) deve ocorrer após um intervalo de tempo ajustado no relé. A ação do relé 79 causa o fechamento dos disjuntores abertos (es_5) por meio da transição t_4 .

Se a falta é temporária, nenhum alarme adicional deve ser reportado, e o estado es_5 corresponde ao último estado da máquina de estados da linha. Por outro lado, se a falta é permanente (t_5), a proteção principal ou de retaguarda da linha deve atuar (es_6) e abrir os disjuntores associados (es_7) por meio da transição t_6 . Dependendo da configuração do sistema supervisorio, o *reset* do relé pode gerar alarme ou não (es_8) após o tempo ajustado no relé (t_7). Nesse momento, novos alarmes não são esperados e o ciclo de operação da máquina de estados é encerrado.

Além do diagrama de estados de linhas, são propostas mais quatro máquinas de estados para possíveis eventos de um sistema de transmissão, conforme é visto na Figura 3.7. A descrição das máquinas de estado é a seguinte:

- proteção de retaguarda remota de linhas (es_1 - es_2 - es_8 - es_9);
- proteção principal de barras e transformadores (es_3 - es_4 - es_8 - es_9);
- proteção de sobrecorrente (SC) em transformadores (es_5 - es_8 - es_9);
- proteção contra falha de disjuntor (es_6 - es_7 - es_8 - es_9).

Figura 3.7 – Diagrama de transição de estados da proteção em um sistema de transmissão



Observe que a representação das máquinas de estado de forma conjunta é utilizada por simplicidade, uma vez que cada máquina tem funcionamento independente. Observe também que o estado final es_9 depende da configuração do sistema supervisorio, podendo o mesmo ser descartado da modelagem caso o alarme de *reset* não esteja disponível.

A aplicação de máquinas de estados permite um melhor diagnóstico em nível local, uma vez que a classificação de eventos utiliza informações apenas de um equipamento. No entanto, essa representação pode ser problemática na análise coletiva de alarmes em nível de sistema, devido à possibilidade dos alarmes estarem inter-relacionados. Isso acontece porque existe a possibilidade de um alarme reportado em um equipamento *B* ser reflexo do disparo de um alarme em um equipamento *A*.

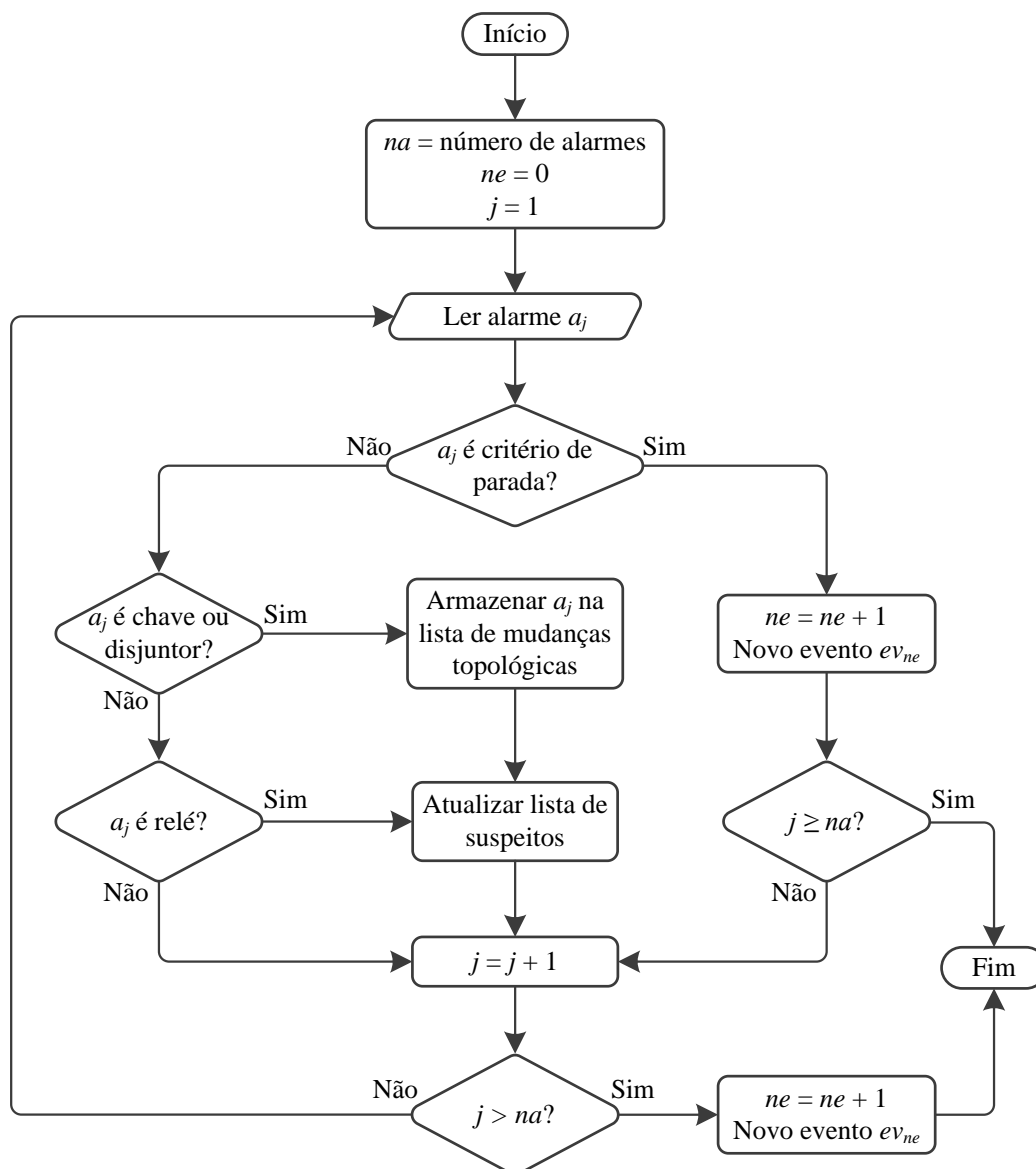
Tendo em vista este problema, duas rotinas devem ser executadas após a aplicação das máquinas de estados. A primeira rotina altera a ordem dos alarmes de *reset* de relés e do disparo da função 79, o qual é utilizado como critério de quebra de janela no mapeamento de eventos. Qualquer reinicialização de relés antes do alarme 79 apaga a informação de disparo de relés, que é fundamental para o diagnóstico, uma vez que o processo se baseia em “fotografias” do sistema a partir do último estado de um alarme reportado. A segunda rotina emprega um critério de tempo para a concatenação de alarmes de diferentes equipamentos em uma única sequência lógica temporal. O tempo de religamento é um intervalo de tempo conhecido que corresponde ao intervalo entre o instante de operação do relé e o instante de energização do circuito de fechamento do disjuntor e é utilizado como critério de tempo neste trabalho. O funcionamento desta rotina é a seguinte:

- a sequência cronológica da linha religada é utilizada como cronologia-base;
- os alarmes de outros equipamentos cujos instantes de disparo antecedem o disparo do 79 da linha são movidos para o intervalo anterior do 79;
- os demais alarmes permanecem inalterados cronologicamente.

3.5 Mapeamento de eventos

O mapeamento de eventos tem como objetivo principal identificar os eventos ocorridos em uma janela de tempo. O processo de mapeamento de eventos é mostrado na Figura 3.8.

Figura 3.8 – Fluxograma do mapeamento de eventos



O mapeamento inicia com o recebimento da lista de alarmes reordenados pela rotina anterior do PIA. Desta lista, obtêm-se o número total de alarmes na a serem processados e são definidas as seguintes variáveis: ne é o número total de eventos mapeados e j é o índice do

alarme analisado. Se um alarme a_j da lista de alarmes é um critério de parada (*reset* de relés ou alarme79), então um novo evento ne é identificado e os dados correspondentes são armazenados na tabela TED.

Caso o alarme a_j não seja um critério de parada, é realizada a filtragem dos alarmes de proteção. Se o alarme a_j corresponde a uma variação de estado de um dispositivo de chaveamento, então a_j é armazenado na lista de modificações topológicas e a lista de suspeitos é atualizada com o equipamento monitorado pelo alarme a_j . A lista de suspeitos corresponde às seções desconectadas em virtude da falta e que devem ser diagnosticadas. Esse laço se encerra com o incremento do índice j .

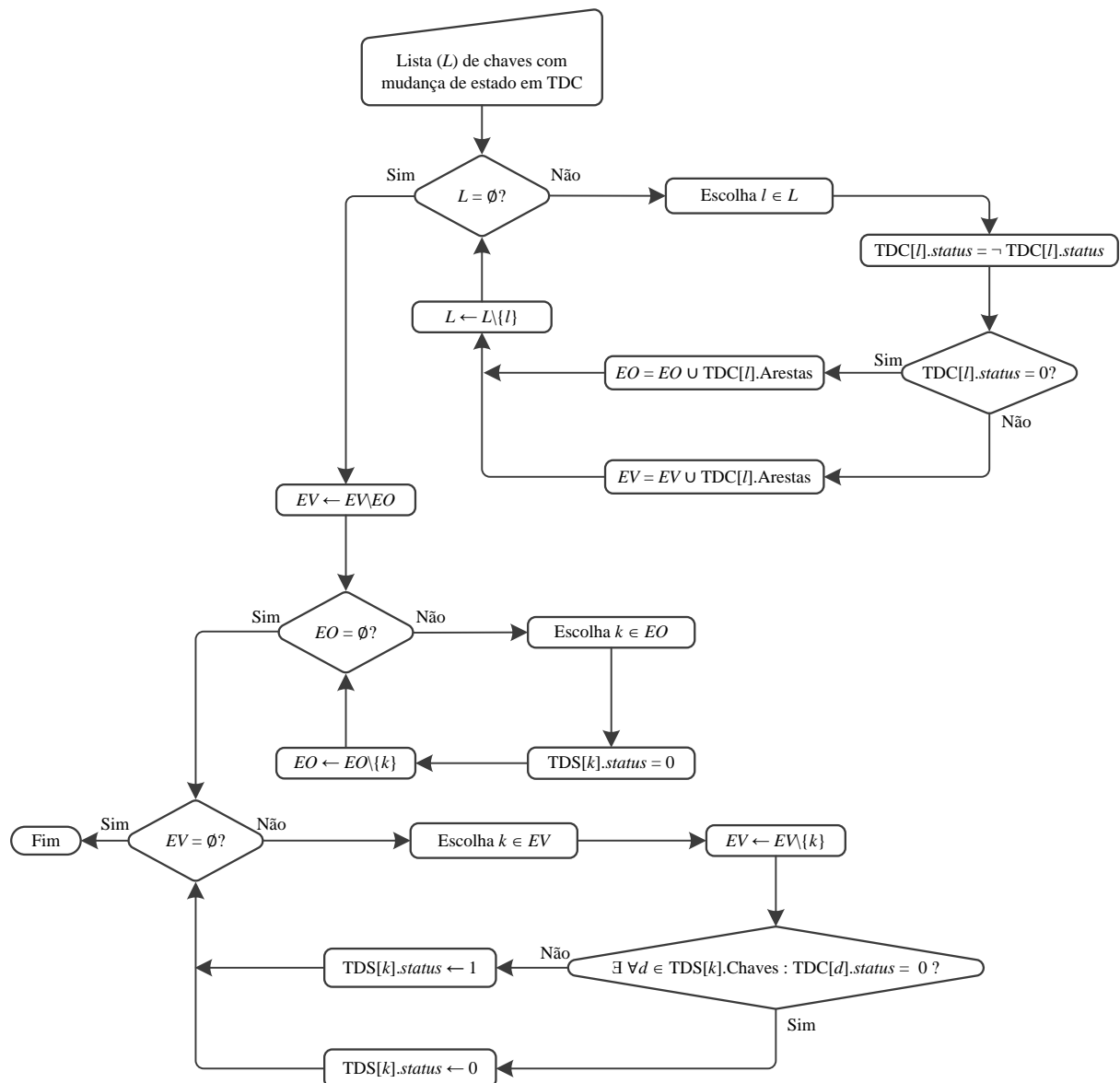
Caso o alarme a_j não corresponda à variação de estado de um dispositivo de chaveamento, deve-se verificar se o alarme a_j corresponde a uma função de proteção (*partida* ou *trip* de relés). Se positivo, o equipamento protegido por este alarme é armazenado na lista de suspeitos e o índice j é incrementado. Se negativo, apenas o índice j é incrementado. Por fim, se o índice j for maior que o número de alarmes na lista de alarmes, $j > na$, então um novo evento é identificado e o mapeamento é encerrado.

Os dados dos eventos mapeados são transferidos para a tabela TED da estrutura de dados. Cada registro da tabela TED armazena os dados de equipamentos cujas proteções foram sensibilizadas pelo distúrbio, equipamentos desconectados pelo distúrbio, a topologia de rede no instante anterior ao distúrbio, os instantes de tempo inicial e final de cada evento, os estados dos alarmes reportados no SCADA e os estados de alarmes não reportados e armazenados no banco de dados da estrutura. Note que a presença dos estados de todos os alarmes monitorados em cada registro da tabela TED possibilita o diagnóstico de eventos quem tenham duração maior do que o tempo ajustado na janela de dados. Com isso, evita-se perda de informação útil para o diagnóstico.

3.6 Identificação da topologia de rede

A região desconectada do sistema elétrico por ocorrência de falta pode ser encontrada utilizando um processador topológico. A identificação desta região permite reduzir a dimensão do problema e acelerar o processo de diagnóstico. Dois algoritmos foram implementados para a identificação topológica da rede. A Figura 3.9 mostra a rotina desenvolvida para atualizar o estado de dispositivos lógicos seccionadores após o chaveamento de dispositivos associados.

Figura 3.9 – Fluxograma de atualização dos dispositivos lógicos seccionadores



O algoritmo acima inicializa com o recebimento da lista L contendo os dispositivos de chaveamento que tiveram variação de estado e identificadas durante o mapeamento de eventos. No primeiro laço, cada chave l listada em L é selecionada a fim de atualizar o campo *status* na linha l da tabela TDC ao seu estado atual. Ainda, a linha possui um campo *Arestas* contendo os índices dos DSs que podem ter o estado alterado devido alteração de estado de uma chave associada. Dessa forma, se o dispositivo de chaveamento abrir, os índices em $TDS[l].Arestas$ são incluídos no conjunto EO de arestas abertas. Essas arestas não necessitam qualquer avaliação aprofundada, visto que se houver ao menos uma chave aberta em TDS, então o estado do DS será, consequentemente, aberto. Caso contrário, se o dispositivo de

chaveamento fechar, os índices deste campo são incluídos no conjunto EV de arestas que devem ser verificadas.

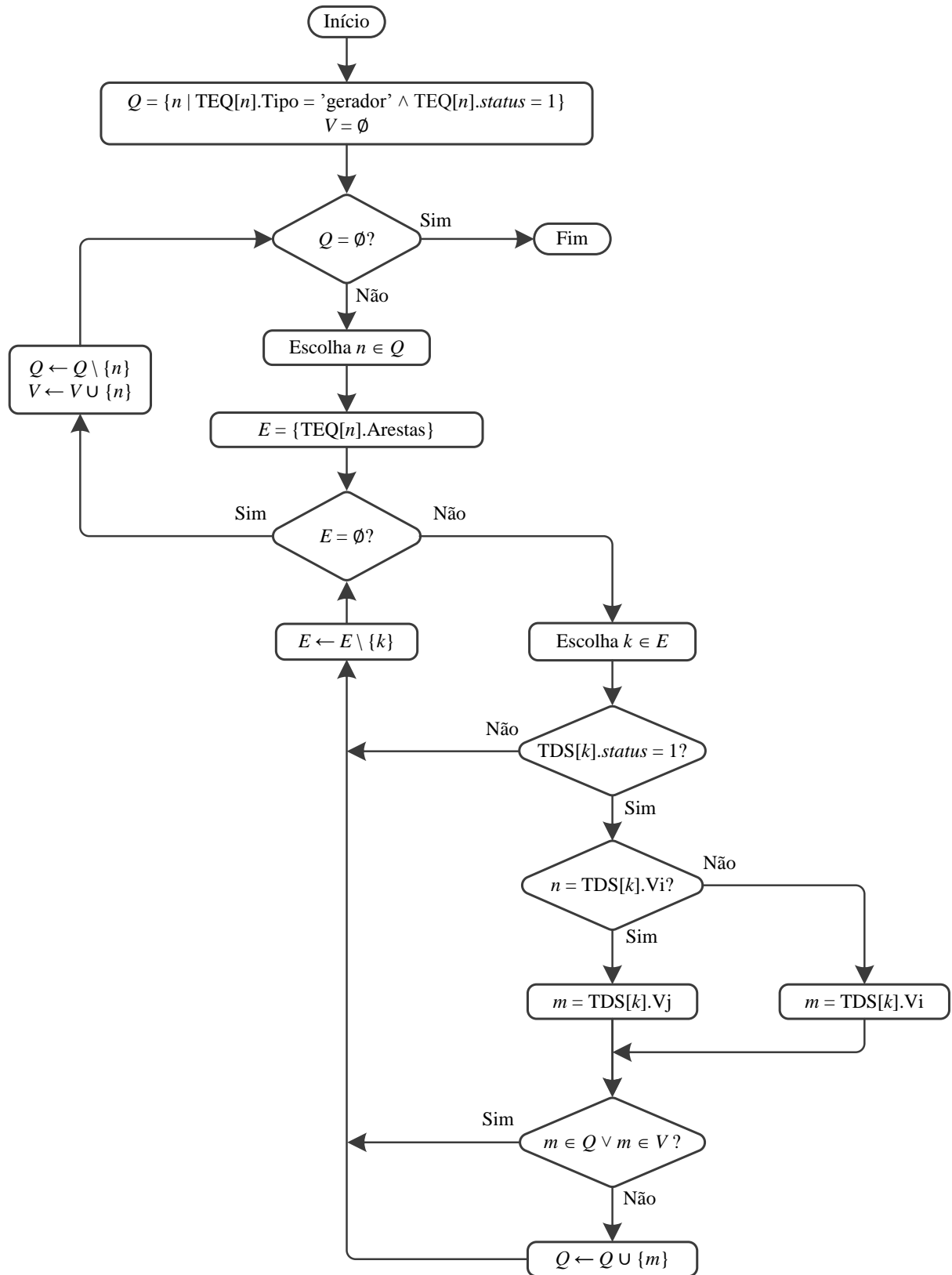
Quando o conjunto L ficar vazio, as arestas presentes em ambos os conjuntos (EV e EO) são removidos do conjunto EV . O laço seguinte atribui *status* igual à zero em cada aresta presente no conjunto EO . Após isso, outro laço é executado verificando os estados dos DSs pertencentes ao conjunto EV . Em cada iteração, um DS k é escolhido e removido de EV . Nesta aresta, é verificada a existência de, pelo menos, um dispositivo aberto em $TDS[k].Chaves$ (lista de chaves que combinadas formam o DS k). Se isso ocorrer, o estado do DS k é definido como aberto, caso contrário, ele é definido como fechado. Quando todos os DSs são testados e removidos do EV , o laço é finalizado.

O número de iterações desta rotina pode ser definido como o produto da dimensão de L , a dimensão de $ES'(d_i)$ (ou $TDC[l].Arestas$) e a dimensão de $S(e_k)$ (ou $TDS[k].Chaves$). O pior caso de complexidade de tempo da rotina pode ser expressa como $O(|L|.|ES'(d_i)|.|S(e_k)|)$. Observe que as mudanças topológicas são muito menos frequentes do que mudanças em dispositivos de chaveamento, resultando em poucos elementos contidos nos conjuntos $ES'(d_i)$ e $S(e_k)$. Sendo assim e considerando o uso diário da rotina em uma aplicação real, o produto $|ES'(d_i)|.|S(e_k)|$ pode ser considerado como uma constante de pequena magnitude.

Uma vez conhecidos os estados de todos os DSs do sistema, é possível determinar a topologia de rede atual, cuja rotina é apresentada na Figura 3.10. A rotina de rastreamento da topologia inicia com a criação de um conjunto Q , que recebe os índices das unidades geradoras ativas e cujas vizinhanças devem ser exploradas a fim de encontrar os equipamentos energizados. Em termos de estrutura, o conjunto Q contém todos os equipamentos listados na tabela TEQ identificados como geradores e energizados ($TEQ[n].Status = 1$). Outro conjunto (V) é criado para conter os equipamentos cuja vizinhança já tenha sido visitada, e começa vazio.

Com ambos os conjuntos criados, a rotina inicia um laço até que o conjunto Q fique completamente vazio. Cada iteração representa a busca por um equipamento energizado na vizinhança de um gerador $n \in Q$. O conjunto das arestas incidentes no vértice n é atribuído ao conjunto E , e então é realizado um laço interno para verificar se a vizinhança de n está ligada por meio destas arestas. Assim, o equipamento n é removido de Q e incluído em V .

Figura 3.10 – Fluxograma para rastreamento da topologia de rede



O laço interno, responsável por verificar cada aresta em E , é executado da seguinte forma: escolhe-se e testa-se um DS k . Se o DS estiver aberto, o índice k é removido a partir do conjunto E , prosseguindo com a verificação de uma próxima aresta em E . Se o DS estiver fechado, verifica-se se o equipamento n está armazenado na tabela TDS como o primeiro ou o segundo vértices da aresta k , $TDS[k].Vi$ e $TDS[k].Vj$ respectivamente. Dessa forma, obtém-se o segundo vértice conectado através da aresta k , a qual é definida como m . O vértice m é incluído no conjunto Q caso o mesmo não tenha sido encontrado até o momento, caso contrário, ele é desprezado. Assim, o índice k é removido do conjunto E , e a iteração é finalizada.

Encerrada a rotina, os vértices contidos em V são os equipamentos energizados, ou seja, os que estão conectados aos geradores do sistema. A comparação dos equipamentos contidos em V com o campo *status* das seções armazenados na tabela TEQ permite determinar a área desligada, usando a tabela TED para armazenar os dados de equipamentos desligados. A complexidade desta rotina é $O(m+n)$, uma vez que todo vértice e toda aresta do grafo devem ser explorados uma vez durante a busca no pior dos casos.

É importante salientar que após uma falta, uma seção pode estar energizada mesmo sem fluxo de potência através dele. Por exemplo, a operação da proteção de contra falha de disjuntor pode abrir apenas um terminal de linha, mantendo a outra extremidade conectada ao resto do sistema. Embora a falta não esteja presente nesses equipamentos, os sistemas de proteção das mesmas ainda podem oferecer informação útil para estimar a seção em falta. Sendo assim, estas seções também são inclusas na tabela TDE para posterior análise.

3.7 Regras de inferência para diagnóstico de faltas

De forma geral, os relés têm a função de detectar faltas dentro de suas zonas de proteção, enquanto aos disjuntores têm a função de isolar a região defeituosa do resto do SEP. Um padrão pode ser definido como a relação entre possíveis seções em falta e atuação esperada de dispositivos de proteção. Essencialmente, a modelagem dos padrões requer o conhecimento da lógica de proteção empregada em cada esquema de proteção do SEP. Além disso, os padrões devem ser adaptáveis às mudanças topológicas na rede e às mudanças em sistemas de proteção. Logo, a modelagem de padrões requer as seguintes informações:

- dados estatísticos de distúrbios;
- dados de desempenho das funções de proteção;

- ajustes utilizados nos dispositivos de proteção;
- condição de estado de dispositivos de medição e proteção;
- particularidades operativas do sistema monitorado.

A metodologia para diagnóstico de faltas proposta por Cardoso Jr., Rolim e Zurn (2004) permitiu a divisão da base de conhecimento em níveis local e de sistema. No nível local, cada equipamento possui um conjunto de regras de proteção que ilustra o funcionamento esperado do esquema de proteção. Em nível de sistema, é empregado um conjunto de padrões que relaciona eventos com possíveis locais de falta. A divisão dos conjuntos de padrões possui as seguintes vantagens:

- reduz o número de padrões a serem modelados devido à redução de combinações lógicas de alarmes em ambos os níveis de análise;
- permite analisar o desempenho de esquemas de proteção de forma isolada devido ao número menor de alarmes associados ao evento;
- as regras de proteção podem ser utilizadas em outros equipamentos com esquemas de proteção semelhantes (com as mesmas funções de proteção ativas);
- a base de conhecimento local permite o escalonamento do conjunto de padrões em nível de sistema de acordo com as mudanças topológicas;
- permite automatizar a modelagem de padrões da proteção em nível de sistema.

3.7.1 Regras da proteção

Uma regra de proteção é definida como um conjunto de alarmes esperados que reflete um possível funcionamento da proteção de um equipamento do SEP. As regras de proteção são utilizadas para classificar eventos em nível de equipamento. A modelagem das regras requer o conhecimento da lógica de funcionamento do esquema de proteção do equipamento considerado, sendo que cada evento inserido no conjunto de regras deve ser consistente logicamente e validado por especialistas.

As regras modeladas para esquemas de proteção que contemplem as funções de proteção mais utilizadas para proteção de componentes em um sistema de geração e de transmissão de 230 kV são apresentadas a seguir. Os esquemas de proteção considerados são baseados em esquemas reais utilizados no SEP sob concessão da CEEE-GT. As funções de proteção são enumeradas conforme estabelece a norma IEEE C37.2 (2008) e podem ser vistas

no Anexo A. Nas tabelas de regras, os alarmes são representados através dos códigos binários definidos na seção 2.3.1 desta tese.

3.7.1.1 Proteção de disjuntores

A determinação do estado real de disjuntores é importante para a determinação da área desligada em virtude da falta. Dessa forma, qualquer mudança de estado do disjuntor deve ser avaliada para confirmar se o mesmo operou ou não (CARDOSO JR., 2003). A Tabela 3.1 relaciona as regras modeladas com os alarmes monitorados em disjuntores.

Tabela 3.1 – Regras da proteção de disjuntores

Alarmes	Regras							
	1	2	3	4	5	6	7	8
Controle manual	0	0	1	1	0	0	1	1
<i>Status</i>	0	1	0	1	0	1	0	1
Proteção própria	1	1	1	1	0	0	0	0

Cada regra (coluna) corresponde a uma combinação lógica dos três alarmes monitorados no disjuntor: controle manual, *status* e proteção própria. Neste caso específico, as regras consideram todas as possibilidades de atuação dos alarmes do disjuntor. A Tabela 3.2 apresenta as classificações das regras modeladas em disjuntores.

Tabela 3.2 – Classificações das regras de disjuntores

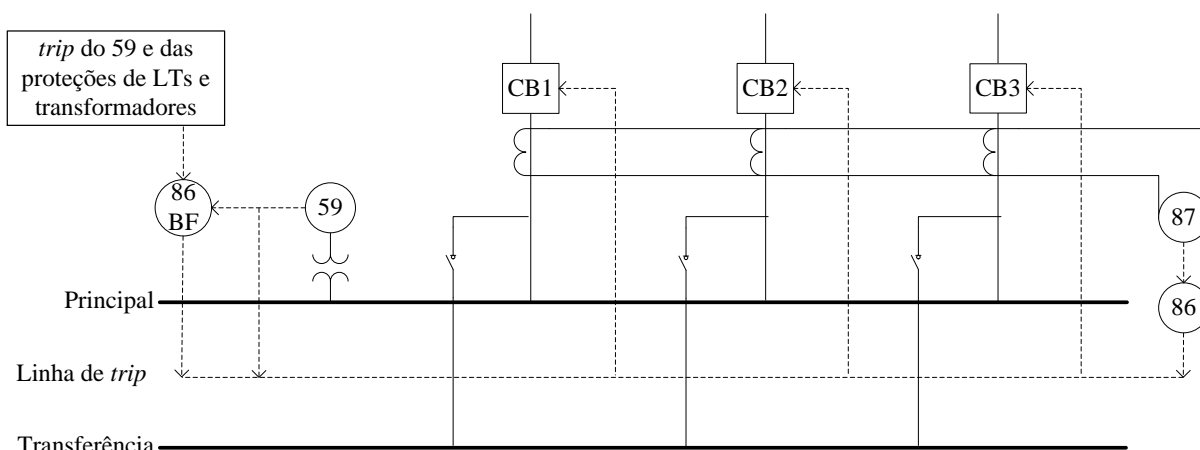
Classificações	Regras							
	1	2	3	4	5	6	7	8
CB com defeito	1	1	1	1	0	0	0	0
Normal	0	0	0	0	1	1	1	1

As classificações “CB com defeito” e “Normal” são eventos que podem ser inferidos utilizando as regras de proteção de disjuntores. O disjuntor deve possuir um defeito interno se uma das regras 1-4 é escolhida para explicar os alarmes reportados. Por outro lado, se uma das regras 5-8 é escolhida, então o disjuntor deve estar funcionando adequadamente.

3.7.1.2 Proteção de barras

O esquema de proteção de barras de 230 kV instaladas em arranjo barra principal e barra de transferência é mostrado na Figura 3.11.

Figura 3.11 – Esquema de proteção de barras de 230 kV



O esquema de proteção das barras é composto de disjuntores e dos relés diferencial (87), sobretensão (59), bloqueio (86) e contra falha de disjuntor (86BF). A Tabela 3.3 relaciona as regras modeladas com os alarmes da proteção de barras.

Tabela 3.3 – Regras da proteção de barras

Proteções	Alarmes	Regras							
		1	2	3	4	5	6	7	8
Diferencial	87	1	1	1	1	0	0	0	0
Relé de bloqueio	86	1	1	1	1	0	0	0	0
Sobretensão	59	0	1	0	1	0	1	0	0
Falha de CB	86BF	0	0	1	1	1	0	0	0
CBs abertos	CB1 CB2 CB3	1	0	1	0	0	1	1	0

Quando uma falta ocorre na barra, o defeito somente é isolado quando todos os disjuntores conectados são devidamente abertos. Portanto, o alarme “CBs abertos” é igual a 1 (barra isolada) quando o estado de todos os disjuntores for igual a 1 (aberto), caso contrário, o valor é igual a 0 (barra conectada). A Tabela 3.4 apresenta as classificações das regras modeladas em barras.

Tabela 3.4 – Classificações das regras de barras

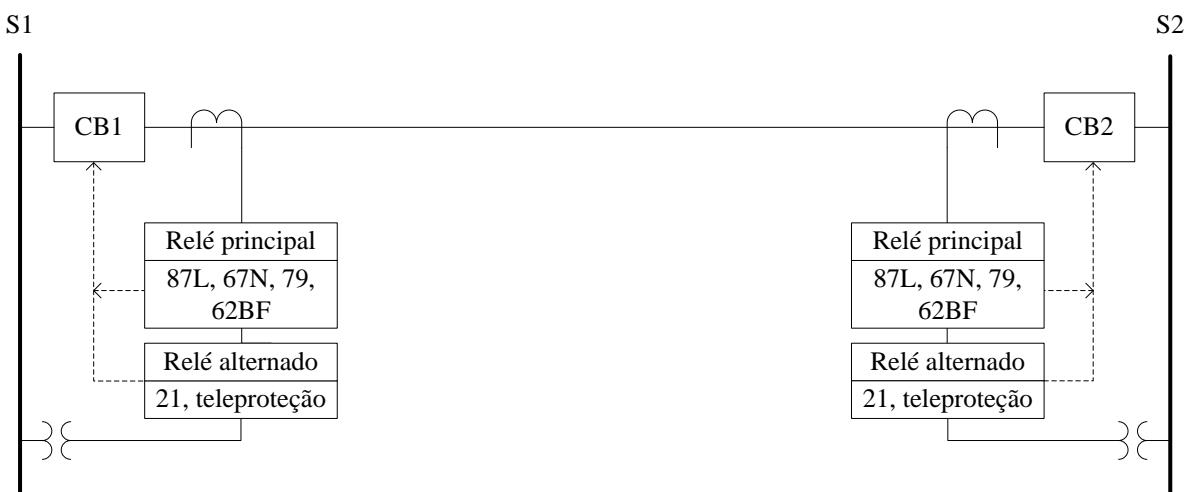
Classificações	Regras							
	1	2	3	4	5	6	7	8
Falta interna	1	1	1	1	0	0	0	0
Falta externa	0	0	0	0	1	1	0	0
Nornal	0	0	0	0	0	0	1	1

As classificações “Falta interna”, “Falta externa” e “Normal” são os eventos que podem ser inferidos utilizando as regras de proteção de barras. A barra deve estar em falta se uma das regras 1-4 for escolhida para explicar os alarmes reportados. Por outro lado, se uma das regras 7-8 é escolhida, então a barra deve estar funcionando adequadamente. Note que apesar da proteção utilizada em barras ser seletiva, é possível identificar faltas externas utilizando as sinalizações da proteção 86BF (regra 5) e do relé 59 (regra 6).

3.7.1.3 Proteção de linhas de transmissão

O esquema considerado para proteção de linhas de transmissão (LTs) de 230 kV é mostrado na Figura 3.12. Cada terminal da linha possui dois relés numéricos, principal e alternado, distintos com funções de proteção diferenciadas. Os relés são independentes e atendem aos requisitos técnicos de proteção em linhas de alta tensão estabelecidos no Submódulo 2.6 dos Procedimentos de Rede do ONS (2010).

Figura 3.12 – Esquema de proteção de LTs de 230 kV



O esquema de proteção da LT é composto de disjuntores, lógica de teleproteção (TPR) e dos relés diferencial de linha (87), distância (21), sobrecorrente direcional de neutro (67N), religamento automático (79) e contra falha do disjuntor (62BF). A proteção de distância é ajustada com uma unidade instantânea (21-1) e duas unidades temporizadas (21-2 e 21-3). A Tabela 3.5 relaciona as regras modeladas com os alarmes da proteção de linhas.

Tabela 3.5 – Regras da proteção de LTs

Proteções	Alarmes	Regras																					
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
PS	87L 21-1 TPR	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
PR_S1	67N 21-2 21-3	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	0	
PR_S2	67N 21-2 21-3	0	1	0	0	0	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	
Falha CB1	CB1 62BF	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	0	0	
Falha CB2	CB2 62BF	0	0	0	0	1	1	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	
CB1	CB1	1	1	0	0	1	1	0	1	0	1	0	0	0	1	0	1	1	0	0	0	1	
CB2	CB2	1	1	1	1	0	0	1	0	0	1	1	1	0	0	0	0	0	1	0	0	1	

Códigos: PS é proteção seletiva; PR_S1 é proteção de retaguarda instalada na subestação S1; e PR_S2 é proteção de retaguarda instalada na subestação S2.

Os alarmes 87L, 21-1 e TPR possuem a mesma característica de proteção, logo são considerados funções de proteção seletiva. Os alarmes 67N, 21-2 e 21-3 configurados no relé principal do terminal S1 são considerados proteções de retaguarda em S1. Os alarmes 67N, 21-2 e 21-3 configurados no relé principal do terminal S2 são considerados proteções de retaguarda em S2. A Tabela 3.6 apresenta as classificações das regras modeladas em linhas.

Tabela 3.6 – Classificações das regras de LTs

Classificações	Regras																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Falta interna	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
FEXT→S1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0
FEXT→S2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0
Normal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

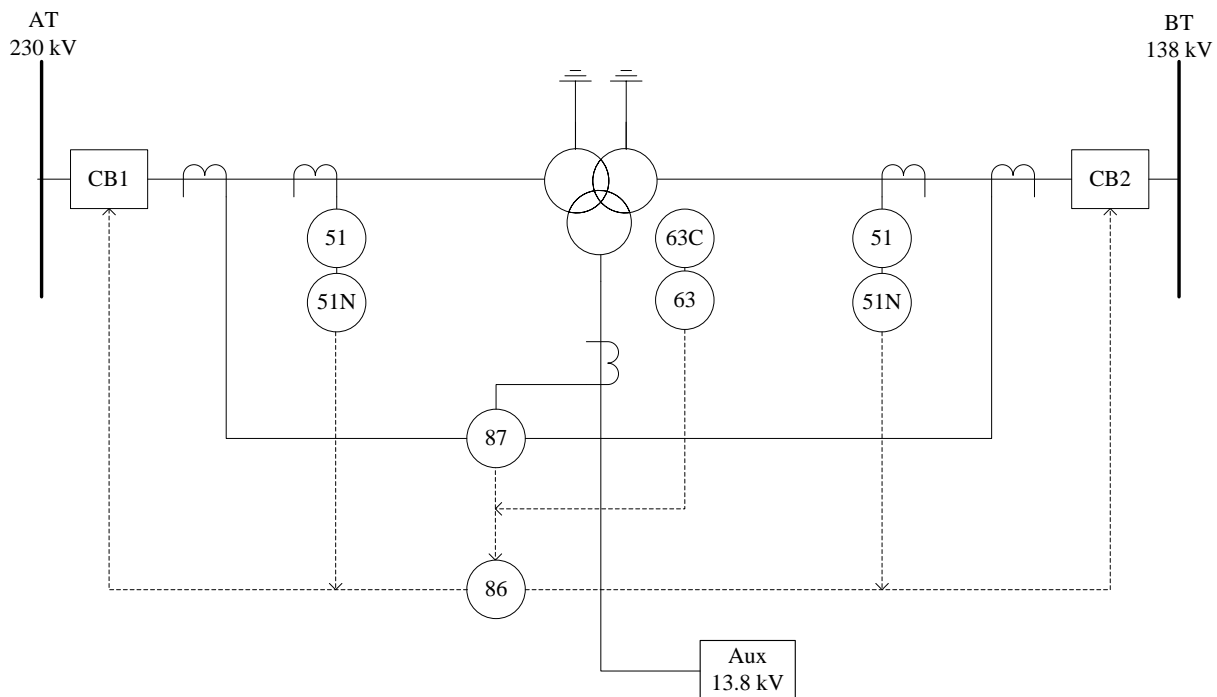
Códigos: FEXT→S1 é falta externa na direção da subestação S1; e FEXT→S2 é falta externa na direção da subestação S2;

As classificações “Falta interna”, “Falta externa na direção de S1”, “Falta externa na direção de S2” e “Normal” são os eventos que podem ser inferidos utilizando as regras de proteção de linhas. A linha deve estar em falta se uma das regras 1-10 for escolhida para explicar os alarmes reportados. Por outro lado, se uma das regras 21-22 é escolhida, então a linha deve estar funcionando adequadamente. As regras 11-15 e 16-20 são utilizadas para identificar faltas externas na direção das subestações S1 e S2, respectivamente. O motivo de diferenciar faltas externas é pelo fato da proteção de retaguarda ser direcional.

3.7.1.4 Proteção de transformadores

O esquema considerado para proteção de transformadores 138/13,8/230 kV é mostrado na Figura 3.13.

Figura 3.13 – Esquema de proteção de transformadores 138/13,8/230 kV



O esquema de proteção do transformador é composto de disjuntores e dos relés diferencial (87), Buchholz (63), pressão (63C), bloqueio (86), sobrecorrente temporizada de fase e de neutro (51/51N). A Tabela 3.7 relaciona as regras modeladas com os alarmes da proteção de transformadores.

Tabela 3.7 – Regras da proteção de transformadores

Proteções	Alarmes	Regras																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
PS	63 63C 87	1	1	1	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0
PR_BT	51 51N	0	1	0	1	0	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0
PR_AT	51 51N	0	0	1	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0
86	86	1	1	1	1	1	1	1	1	0	0	0	1	0	0	0	1	0	1	0	0
CB1	CB1	1	1	1	1	1	1	1	0	0	1	1	1	0	1	0	0	0	0	1	0
CB2	CB2	1	1	1	1	1	1	0	1	1	0	0	0	0	0	1	1	0	1	0	1

Códigos: PS é proteção seletiva; PR_BT é proteção de retaguarda no lado de baixa tensão; e PR_AT é proteção de retaguarda no lado de alta tensão.

Note que os alarmes 63, 63C e 87 indicam atuação da proteção seletiva, enquanto os alarmes 51 e 51N indicam atuação da retaguarda. Como a impedância do transformador é muito maior do que a de linhas, a operação do relé 51 deve ocorrer depois de transcorrido um tempo relativamente grande. Dessa forma, considera-se que os relés de sobrecorrente somente devem enxergar faltas no terminal do transformador no qual estão instalados. A Tabela 3.8 apresenta as classificações das regras modeladas em transformadores.

Tabela 3.8 – Classificações das regras de transformadores

Classificações	Regras																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Falta interna	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
FEXT→AT	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
FEXT→BT	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
Normal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

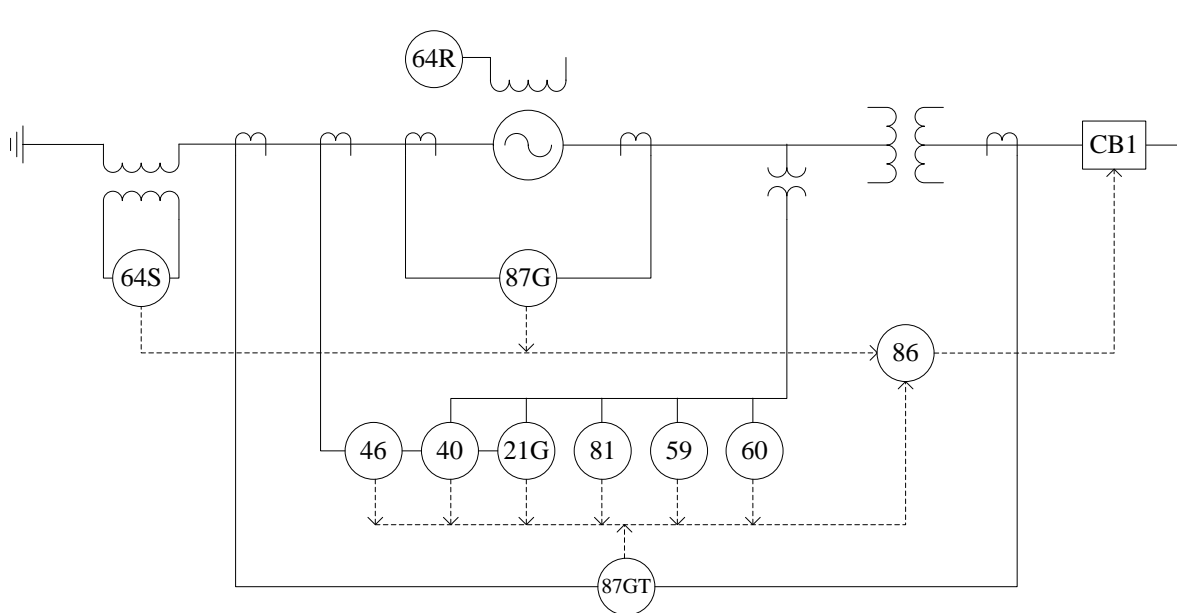
Códigos: FEXT→AT é falta externa no lado de alta tensão; e FEXT→BT é falta externa no lado de baixa tensão.

As classificações “Falta interna”, “Falta externa no lado de alta tensão”, “Falta externa no lado de baixa tensão” e “Normal” são os eventos que podem ser inferidos utilizando as regras de proteção de transformadores. O transformador deve estar em falta se uma das regras 1-10 for escolhida para explicar os alarmes reportados. Por outro lado, se uma das regras 11-20 é escolhida, então o transformador deve estar funcionando adequadamente. As regras 11-14 e 15-18 são utilizadas para identificar faltas externas nos lados de alta e baixa tensão.

3.7.1.5 Proteção de geradores síncronos

O esquema considerado para proteção de geradores síncronos de 13,8 kV é mostrado na Figura 3.14.

Figura 3.14 – Esquema de proteção de geradores síncronos de 13,8 kV



O esquema de proteção do gerador síncrono é composto do disjuntor e dos relés diferencial do gerador (87G), diferencial do grupo gerador-transformador (87GT), contra perda de excitação de campo (40), terra-rotor (64R), terra-estator (64S), contra desbalanço de corrente de sequência negativa (46), distância do gerador (21G), sobretensão (59), contra desbalanço de tensão (60), frequência (81) e bloqueio (86). A Tabela 3.9 relaciona as regras modeladas com os alarmes da proteção de geradores síncronos.

Tabela 3.9 – Regras da proteção de geradores síncronos

Proteções	Alarmes	Regras							
		1	2	3	4	5	6	7	8
PS	40 46 64R 64S 87G 87GT	1	1	1	1	1	0	0	0
PR	21G 59 60 81	1	1	0	1	1	1	1	0
86	86	0	0	0	1	1	0	1	0
CB1	CB1	1	0	1	1	0	1	1	1

Códigos: PS é proteção seletiva e PR é proteção de retaguarda.

Os alarmes 40, 46, 64R, 64S, 87G e 87GT são relativos a funções de proteção seletiva, enquanto os alarmes 21G, 59, 60 e 81 são proteções de retaguarda. A Tabela 3.10 apresenta as classificações das regras modeladas em transformadores.

Tabela 3.10 – Classificações das regras de geradores síncronos

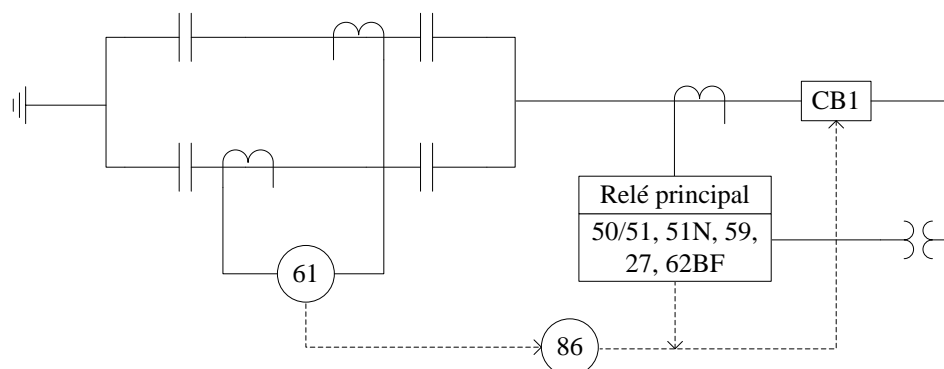
Classificações	Regras							
	1	2	3	4	5	6	7	8
Falta interna	1	1	1	1	1	0	0	0
Falta externa	0	0	0	0	0	1	1	0
Normal	0	0	0	0	0	0	0	1

As classificações “Falta interna”, “Falta externa” e “Normal” são os eventos que podem ser inferidos utilizando as regras de proteção de geradores. O gerador deve estar em falta se uma das regras 1-5 for escolhida para explicar os alarmes reportados. Por outro lado, se a regra 8 é escolhida, então o gerador deve estar funcionando adequadamente. As regras 6 e 7 são utilizadas para identificar faltas externas à unidade geradora.

3.7.1.6 Proteção de banco de capacitores

O esquema de proteção de banco de capacitores é mostrado na Figura 3.15.

Figura 3.15 – Esquema de proteção da banco de capacitores



O esquema de proteção do banco de capacitores é composto do disjuntor e dos relés de desbalanceamento de corrente (61), subtensão (27), sobretensão (59), bloqueio (86), sobrecorrente

instantâneo (50), sobrecorrente temporizado de fase e de neutro (51/51N). A Tabela 3.11 relaciona as regras modeladas com os alarmes da proteção de banco de capacitores.

Tabela 3.11 – Regras da proteção de banco de capacitores

Proteções	Alarmes	Regras																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
PS	61	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
PNS	50 51 51N	1	0	0	1	1	0	0	1	1	1	1	1	1	1	1	1	0	0	0
PST	27, 59	1	1	0	1	0	0	1	0	0	1	0	0	1	1	1	0	1	1	0
86	86	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
Falha CB1	CB1 62BF	1	0	0	0	0	0	0	1	1	1	0	1	0	1	1	1	0	0	0
CB1	CB1	1	1	1	1	1	0	0	1	0	1	1	1	1	1	0	0	0	1	1

Códigos: PS é proteção seletiva, PNS é proteção não-seletiva e PST é proteção de sub/sobretensão.

O alarme 61 é a única proteção seletiva do banco de capacitores. Os alarmes 50, 51 e 51N são considerados funções de proteção seletiva e permitem a detecção de faltas internas à unidade geradora. Os alarmes 21G, 59, 60 e 81 são considerados funções de retaguarda e permitem a detecção de faltas externas. A Tabela 3.10 apresenta as classificações das regras modeladas no banco de capacitores.

Tabela 3.12 – Regras da proteção de banco de capacitores

Classificações	Regras																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
Falta interna	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
Falta externa	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0
Normal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1

As classificações “Falta interna”, “Falta externa” e “Normal” são os eventos que podem ser inferidos utilizando as regras da proteção do banco de capacitores. O banco de capacitores deve estar em falta se uma das regras 1-10 for escolhida para explicar os alarmes reportados. Por outro lado, se uma das regras 17-18 é escolhida, então o banco de capacitores deve estar funcionando adequadamente. As regras 11-16 são utilizadas para identificar faltas externas ao banco de capacitores.

3.7.2 Geração automática de padrões de funcionamento de sistemas de proteção

Este algoritmo foi desenvolvido para gerar os padrões de funcionamento de um sistema de proteção após a ocorrência de uma falta. A geração automática de padrões de eventos para o diagnóstico de faltas possui duas vantagens principais:

- facilita a implantação de sistemas automatizados no COS. Padrões dependem dos estados de relés e disjuntores, além da disposição física dos equipamentos de rede, o que pode implicar em um número excessivamente grande de combinações lógicas de alarmes;
- pode ser aplicado a qualquer topologia de rede. Padrões utilizados por métodos de diagnóstico de falta necessitam ser previstos e selecionados para qualquer mudança topológica do SEP.

Com base nisso, foi desenvolvido um algoritmo que analisa a topologia da rede, simula possíveis cenários de falta e determina a ação esperada de disjuntores e as classificações de evento esperadas. Os padrões criados e validados são aqueles eventos que seguem uma filosofia de proteção composta de sistemas de proteção principal, retaguarda local e retaguarda remota.

O gerador de padrões é baseado na representação de topologia de rede proposta neste trabalho, onde cada vértice do grafo corresponde a uma seção protegida por um esquema de proteção adequada ao tipo de equipamento. Um padrão corresponde ao conjunto de alarmes esperados para uma determinada seção em falta. Os alarmes que compõem esse padrão podem variar caso haja falha na abertura de disjuntores, o que resulta em um padrão de evento. O conjunto de padrões corresponde à base de conhecimento utilizada pelos modelos de programação matemática para diagnosticar faltas.

Diferentemente de outros trabalhos (CARDOSO JR., 2003; FRITZEN, 2012), as classificações de “não falta” ou “operação normal” não são utilizadas para a caracterização dos padrões de eventos. Normalmente, as faltas ficam restritas a uma pequena área do sistema de potência. Isso pode resultar em um grande número de alarmes “não falta” e mascarar a solução ótima do problema. Desse modo, pretende-se com a retirada dos alarmes aumentar a capacidade de busca do modelo de programação matemática.

3.7.2.1 Descrição dos conjuntos utilizados para a geração de padrões

O funcionamento do algoritmo de geração de padrões requer dados extraídos do grafo representativo do SEP referentes à identificação dos equipamentos, disjuntores e alarmes monitorados no SEP. Abaixo são apresentados os conjuntos essenciais para o funcionamento do algoritmo proposto:

- De_j é o conjunto de disjuntores pertencentes à aresta j ;
- E é o conjunto de arestas do sistema;
- V é o conjunto de vértices do sistema;
- Ve_j é o conjunto de vértices conectados através da aresta j .

A partir dos dados acima, foram desenvolvidas rotinas para a geração de novos conjuntos de dados. Os conjuntos gerados são os seguintes:

- Bv_i é o conjunto de barras vizinhas da seção i ;
- C é o conjunto de classificações de eventos;
- Cv_i é o conjunto de classificações de evento da seção i ;
- D é o conjunto de disjuntores do sistema;
- Dv_i é o conjunto de disjuntores que recebem *trip* da proteção principal da seção i ;
- Ev_i é o conjunto de arestas conectadas à seção i ;
- Ed_k é o conjunto de arestas contendo o disjuntor k ;
- P é a matriz de padrões contendo m eventos e n alarmes;
- T_i é o conjunto de terminais da seção i ;
- Vv_i é o conjunto de vizinhos da seção i ;
- Vd_k é o conjunto de seções protegidas pelo disjuntor k ;
- VBv_i é o conjunto de vizinhos da barra vizinha que dão retaguarda à seção i ;
- VRv_i é o conjunto de seções que podem dar retaguarda à seção i ;
- bd_k é a barra de referência do disjuntor k ;
- bc_q é a barra de referência da classificação c_q ;
- c_q é o estado da classificação de evento q ;
- m é o número de padrões (linhas da matriz P);
- n é o número de alarmes (colunas da matriz P).

3.7.2.2 Rotinas para montagem dos conjuntos

A topologia de rede é obtida utilizando o algoritmo mostrado na Figura 3.10. Os demais dados de conjuntos são obtidos a partir das equações abaixo. O conjunto de disjuntores do sistema (D) é definido como a união dos conjuntos de disjuntores associados a cada aresta j (De_j), ou seja,

$$D = \bigcup_{j=1}^{|E|} De_j. \quad (3.1)$$

O conjunto de arestas do vértice i (Ev_i) é obtido através da seguinte condição: se o vértice i pertencer ao conjunto de vértices da aresta j (Ve_j), então a aresta j pertence ao conjunto E_i . Portanto,

$$Ev_i = \{j \in E : i \in Ve_j\}. \quad (3.2)$$

O conjunto de arestas do disjuntor k (Ed_k) é obtido através da seguinte condição: se o disjuntor k pertencer ao conjunto de disjuntores da aresta j (De_j), então a aresta j pertence ao conjunto Ed_k . Portanto,

$$Ed_k = \{j \in E : k \in De_j\}. \quad (3.3)$$

O conjunto de vértices vizinhos do vértice i (Vv_i) é obtido através da seguinte condição: se vértice i pertencer ao conjunto de vértices conectados pela aresta j (Ve_j), então o vértice diferente de i , $Ve_j \setminus \{i\}$, pertence ao conjunto de vértices vizinhos do vértice i (Vv_i). Portanto,

$$Vv_i = Ve_j \setminus \{i \in Ve_j : j \in E\}. \quad (3.4)$$

O conjunto de disjuntores que protegem a seção i (Dv_i) é obtido através da seguinte condição: se a aresta j pertence ao conjunto de arestas do vértice i (Ev_i) e a aresta j é formada por apenas um disjuntor, $|De_j| = 1$, então o disjuntor $k \in De_j$ pertence ao conjunto Dv_i . Portanto,

$$Dv_i = \{k \in De_j : |De_j| = 1 \wedge j \in Ev_i\}. \quad (3.5)$$

O conjunto de vértices do disjuntor k (Vd_k) é a relação inversa do conjunto Dv_i , e é obtido através da seguinte condição: se o disjuntor k pertence ao conjunto Dv_i , então o vértice i pertence ao conjunto Vd_k , ou seja,

$$Vd_k = \{i \in V : k \in Dv_i\}. \quad (3.6)$$

Se o vizinho l da seção i é uma barra, então existe um conjunto de barras vizinhas da seção i (Bv_i), ou seja,

$$Bv_i = \{l \in Vv_i : l \neq i \wedge l = bus\} \quad (3.7)$$

em bus é a variável utilizada para identificar barras. O valor de bus é obtido a partir do código identificador do equipamento.

Os vizinhos da barra l vizinha da seção i (VBv_i) deve conter seções que possuam esquemas de proteção de retaguarda, no caso, linhas, geradores ou transformadores. O conjunto VBv_i é formado pelos vizinhos ii da barra $l \in Vv_i$, tal que $ii \neq i$ e ii seja uma seção com proteção de retaguarda. Portanto,

$$VBv_i = \{ii \in Vv_i : l \in Bv_i \wedge ii \neq i \wedge ii = sr\} \quad (3.8)$$

em sr é a variável utilizada para identificar seções que oferecem retaguarda, no caso, linha, gerador ou transformador. O valor de sr é obtido a partir do código identificador do equipamento.

O resultado da união dos conjuntos VBv_i e Vv_i , desconsiderando barras, é igual ao conjunto das seções vizinhas que possuem esquemas de proteção de retaguarda ao equipamento VRv_i , ou seja,

$$VRv_i = VBv_i \cup \{l \in Vv_i : l = sr\}. \quad (3.9)$$

O algoritmo de geração de padrões foi desenvolvido para ser independente em relação ao uso de identificadores de subestações. Por esse motivo, o algoritmo requer a identificação de uma barra de referência em cada SE. As barras de referência substituem a informação da subestação e são utilizadas para determinar se um disjuntor deveria ou não atuar para uma dada situação de falta.

Em arranjos barra principal e transferência, a barra de referência bd_k do disjuntor k é a seção i pertencente ao conjunto Vd_k que seja uma barra. Se houver apenas uma barra, bd_k é encontrado da seguinte forma:

$$bd_k = \{i \in Vd_k : i = sr \wedge bd_k \neq \emptyset\}. \quad (3.10)$$

A condição $bd_k \neq \emptyset$ impede que um disjuntor k tenha mais de uma barra de referência, mesmo que Vd_k contenha mais de uma barra. O uso da eq. (4.10) não possui efeito em disjuntores localizados no centro de arranjos disjuntor e meio. Geralmente, esses disjuntores são operados a partir da proteção de linhas e transformadores. Nesse caso, é necessária uma condição adicional: se a aresta j pertencer ao conjunto de arestas do disjuntor k ($j \in Ed_k$) e o vértice i pertencente ao conjunto de vértices conectados através da aresta j ($i \in Ve_j$) é uma barra, então a barra i é a barra de referência do disjuntor central k , ou seja,

$$bd_k = \{i \in Ve_j : j \in Ed_k \wedge i = bus \wedge bd_k \neq \emptyset\}. \quad (3.11)$$

As barras de referência também são utilizadas para determinar as barras terminais de linhas e transformadores. Essa informação é empregada no reconhecimento das classificações de eventos provenientes da análise em nível de equipamento e que sejam do tipo direcional como, por exemplo, “falta externa vista pela linha L2 em direção da barra B2”.

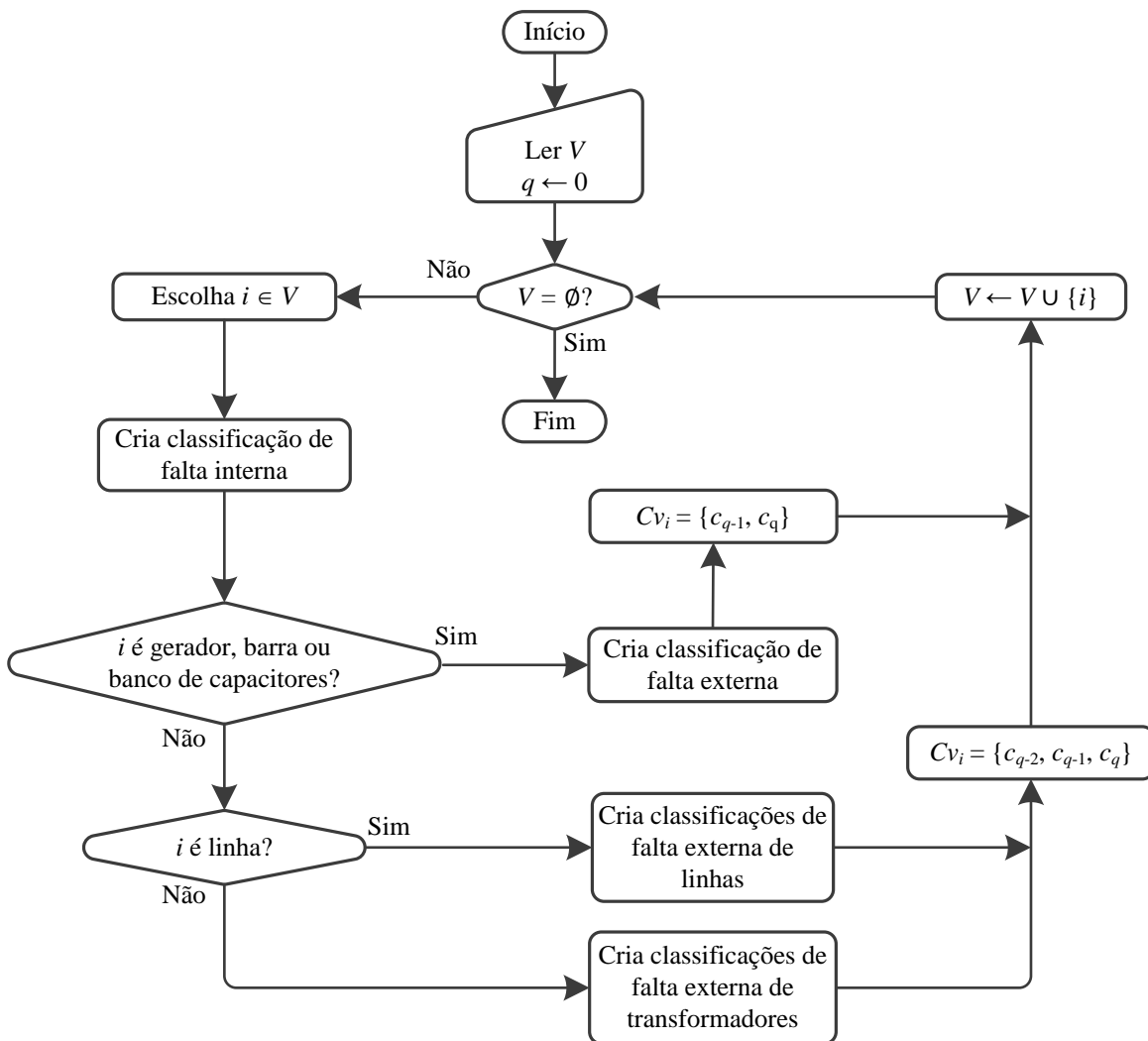
Sendo assim, o conjunto de terminais da seção i (T_i) contém as barras de referência bd_k de cada disjuntor k pertencente ao conjunto de disjuntores que protegem a seção i ($k \in Dv_i$). Além disso, no conjunto T_i não deve haver duas barras de referência iguais, resultando em:

$$T_i = \{bd_k : k \in Dv_i \wedge b_k \notin T_i\}. \quad (3.12)$$

Uma vez definidos os dados do sistema elétrico, é possível listar todas as classificações de evento. As classificações, em conjunto com os alarmes de disjuntores, são os dados de entrada utilizados para a geração de padrões. Cada combinação lógica de alarmes e classificações representa um possível funcionamento da proteção.

A Figura 3.16 mostra o fluxograma desenvolvido para identificação das possíveis classificações de evento para cada equipamento do SEP.

Figura 3.16 – Fluxograma para determinação das classificações de evento



O algoritmo implementado para as sub-rotinas existentes no fluxograma da Figura 3.16 é mostrado na Tabela 3.13.

Tabela 3.13 – Sub-rotinas utilizadas para a determinação de classificações

Sub-rotina	Algoritmo
Cria classificação de falta interna	$q = q + 1$ $c_q = \text{"falta interna"}$ $bc_q = T_i$
Cria classificação de falta externa	$q = q + 1$ $c_q = \text{"falta externa"}$ $bc_q = T_i$

Sub-rotina	Algoritmo
Cria classificações de falta externa em linhas	$q = q + 1$ $c_q = \text{“falta externa na direção de } T_i^{1\text{”}}$ $bc_q = T_i^2$ $q = q + 1$ $c_q = \text{“falta externa na direção de } T_i^{2\text{”}}$ $bc_q = T_i^1$
Cria classificações de falta externa em transformadores	$q = q + 1$ $c_q = \text{“falta externa na direção de } T_i^{1\text{”}}$ $bc_q = T_i^1$ $q = q + 1$ $c_q = \text{“falta externa na direção de } T_i^{2\text{”}}$ $bc_q = T_i^2$

A rotina acima inicia com a leitura da lista V de equipamentos e com o número de classificações q igual à zero. No primeiro laço, é selecionado um elemento i da lista V . A seguir é criada a classificação c_q definida como “falta interna” e os terminais do equipamento T_i são armazenados em bc_q .

Se a seção i é do tipo gerador, barra ou banco de capacitores, então existe a possibilidade da proteção do equipamento enxergar faltas fora da zona de proteção seletiva, mas sem direcionalidade. Para cada um desses componentes será criada uma classificação c_q definida como “falta externa” e a barra conectada ao equipamento T_i é armazenada em bc_q . Como esses equipamentos possuem apenas dois tipos de classificações possíveis, as classificações c_q e c_{q-1} são incluídas no conjunto Cv_i de classificações da seção i .

Se a seção i é uma LT, as seguintes classificações “falta na direção do terminal $T_i^{1\text{”}}$ e “falta na direção do terminal $T_i^{2\text{”}}$ devem ser criadas. A barra de referência de cada classificação bc_q indica o local onde o relé responsável pela retaguarda está instalado. Neste caso, bc_q é igual T_i^2 e T_i^1 , respectivamente. Note que a classificação c_q aponta para a direção do terminal da linha. Isso acontece porque em cada terminal existe um relé de distância que pode enxergar faltas na direção oposta da subestação na qual está instalada (sentido direto). As três classificações c_q geradas para a linha i são armazenadas no conjunto Cv_i .

Se a seção i é um transformador, são criadas as seguintes classificações “falta na direção do terminal $T_i^{1\text{”}}$ e “falta na direção do terminal $T_i^{2\text{”}}$. A barra de referência bc_q deve ser igual ao terminal visto pela classificação c_q , ou seja, T_i^1 e T_i^2 , respectivamente. Isso acontece

porque a proteção de retaguarda de transformadores é realizada por relés de sobrecorrente temporizados (51), que tendem a enxergar faltas apenas no terminal instalado. Por critério de coordenação, o relé 51 deve ser sensibilizado para faltas existentes no terminal oposto dele, porém com um tempo de atuação muito grande devido à impedância do transformador. Por fim, as três classificações c_q geradas para o gerador i são armazenadas no conjunto Cv_i .

Se não houver mais equipamentos em V , a rotina acima é encerrada. O conjunto das classificações de evento do sistema (C) é resultado da união dos conjuntos de classificações de cada equipamento i , ou seja,

$$C = \bigcup_{i=1}^{|V|} Cv_i. \quad (3.13)$$

3.7.2.3 Geração de padrões com atuação da proteção principal

Considere $P_{m \times n}$ a matriz formada pelos padrões gerados nesta etapa, composta de m linhas geradas iterativamente e de n colunas de alarmes e classificações. Considere também que D e C são vetores ordenados de índices dos alarmes de disjuntores e classificações de evento, respectivamente, e contidos nos conjuntos de mesmo nome. O número de colunas n é igual à soma das cardinalidades de D e C , ou seja,

$$n = |D| + |C|. \quad (3.14)$$

Os padrões criados a partir da operação da proteção principal é a primeira etapa do gerador proposto. Para cada equipamento $i \in V$ existe um padrão composto das classificações esperadas de eventos e alarmes esperados de disjuntores para uma falta na seção i . Matematicamente, o padrão de funcionamento da proteção principal m para faltas na seção i consiste dos seguintes dados:

- Alarmes de abertura dos disjuntores de Dv_i ;
- Classificação de “falta interna” c_q^i de Cv_i ;
- Classificações de “falta externa na direção de uma barra” vista por linhas vizinhas de V_i . Para a linha $l \in VRv_i$, se a barra bc_q^l referente à classificação de falta externa direcional c_q^l não pertencer ao conjunto de vizinhos da seção i , ($bc_q^l \notin Vv_i$), então a classificação c_q^l é esperada.

3.7.2.4 Geração de padrões com atuação da proteção retaguarda local

Neste trabalho, a proteção de retaguarda local é realizada pela função falha de disjuntor (86BF) e está associada diretamente com a classificação “falta externa” de barras. Apenas as linhas, transformadores e geradores em falta possuem padrões associados à operação da retaguarda local.

Considere uma seção i com sistema de proteção composta de $|Dv_i|$ disjuntores. Se a seção estiver em falta, a proteção principal atuar e um dos disjuntores falhar durante a abertura, então um sistema de retaguarda deve atuar e isolar a falta. Para cada disjuntor falho k existe um padrão m , cujo alarme de abertura não deve ser reportado, ou seja, $P_{mk} = 0$. Apenas as barras adjacentes à seção em falta i após a falha do disjuntor k devem operar as suas proteções de retaguarda local. Dessa forma, são esperados os seguintes dados para uma falta na seção i :

- Alarmes de abertura dos disjuntores de DV_i com exceção do disjuntor k ;
- Classificação de “falta interna” c_q^i de Cv_i ;
- Classificação de “falta externa” vista pela barra $l \in Vv_i$, tal que $l \in Vd_k$;
- Alarmes de abertura dos disjuntores de Dv_l com exceção do disjuntor k .

3.7.2.5 Geração de padrões com atuação da proteção retaguarda remota

Considere uma seção em falta i com sistema de proteção composta de $|DV_i|$ disjuntores. No caso da proteção principal atuar e se um dos disjuntores de Dv_i falhar haverá atuação da proteção de retaguarda remota. Para cada disjuntor falho k existe um padrão m , cuja sinalização de abertura não deve ser reportada, ou seja, $P_{mk} = 0$. Os padrões que consideram o funcionamento da proteção de retaguarda remota para uma falta na seção i devem conter alarmes e classificações oriundos da operação tanto da proteção principal quanto da retaguarda remota.

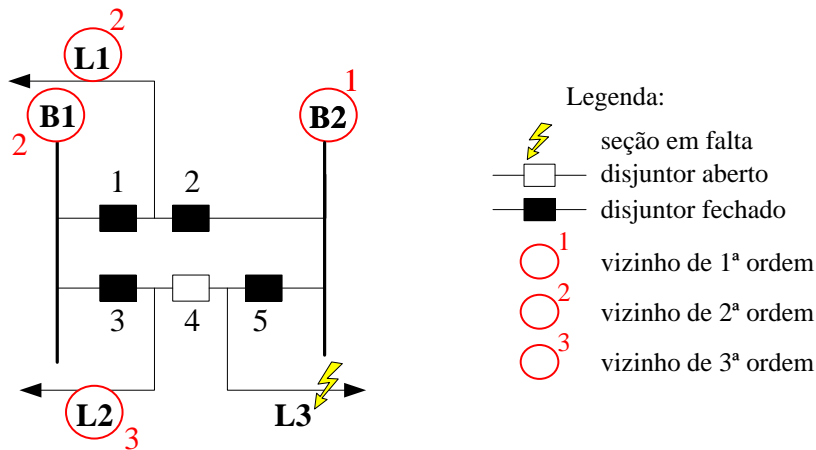
Após a falha de um disjuntor $k \in Dv_i$, devem-se identificar as linhas, geradores e transformadores que permanecem conectadas à seção i após atuação da proteção principal. Essa busca visa determinar as proteções de retaguarda remota que devem operar para a falha do CB k e faz uso das topologias de rede pré e pós-atuação da proteção principal.

O algoritmo de Dijkstra (1959) é empregado para rastrear o menor caminho entre o vértice i e um vértice $l \in VRv_i$. Se a menor distância entre o par de vértices i e l contiver mais

de três vértices (não repetidos e independentes do tipo de seção), então o vértice l não deve oferecer retaguarda remota à seção i . Sendo assim, a seção l é removida do conjunto VRv_i , ou seja, $VRv_i \leftarrow VRv_i \setminus \{ l \}$.

Na Figura 3.17 é mostrado um arranjo de barras disjuntor e meio para ilustrar a lógica de identificação dos sistemas de retaguarda ativos. Esse arranjo é parte de um sistema malhado e apresenta uma falta na linha L3 com falha na abertura do disjuntor CB5. Os equipamentos com círculos em vermelhos e os números junto a eles representam os vizinhos da linha L3 e a ordem de vizinhança, respectivamente.

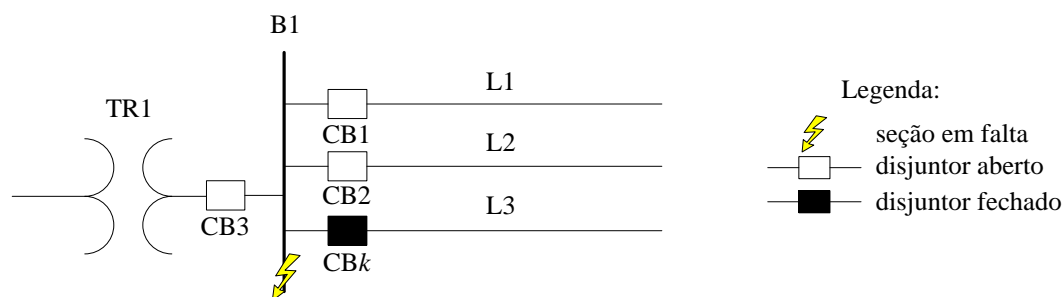
Figura 3.17 – Arranjo disjuntor e meio com falta em L3 e falha em CB5



A estrutura de dados armazena apenas os vizinhos de 1ª e 2ª ordem, logo é necessário analisar se há vizinhos de maior ordem que ofereçam retaguarda à seção em falta. Como as barras não possuem proteções de retaguarda remota, as barras B1 e B2 são desprezadas da análise. Analisando diversas configurações de sistema, chegou-se ao valor de três vértices como distância máxima entre a seção em falta e seções vizinhas para determinar a atuação da proteção de retaguarda.

A falta em barras deve ser tratada de uma maneira particular. Considere uma barra i e um disjuntor falho k conectado a uma linha l . Todas as seções paralelas à seção l devem ser removidas do conjunto VRv_i , visto que as mesmas já estão isoladas da seção i . Esse caso é exemplificado por meio da Figura 3.18, onde B1 corresponde à barra i e L3 corresponde a linha l conectada através do disjuntor k . Note que as linhas paralelas L1 e L2 estão isoladas de B1 pelos disjuntores CB1 e CB2, que foram abertos devido à operação da proteção principal da barra. Nesse caso, apenas a proteção de retaguarda remota da linha L3 deve atuar.

Figura 3.18 – Cenário pós-falta na barra B1



Ao fim das rotinas acima, as seções que permanecerem em VR_{v_i} são as seções cujos esquemas de proteção de retaguarda remota devem operar para a falta na seção i e falha do disjuntor k . Os disjuntores que devem abrir são identificados a partir de critérios especificados para cada tipo de seção vizinha l . Os critérios considerados neste trabalho são:

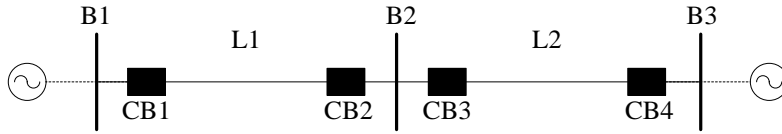
- Gerador: todos os disjuntores do grupo gerador devem operar, exceto o disjuntor k .
- Linha: o disjuntor p da linha l que deve operar é aquele localizado no terminal oposto à seção i e que pertence ao conjunto Dv_l . A atuação do disjuntor p é identificada por meio da seguinte condição: se a barra de referência do disjuntor p não é um terminal da seção i , então o disjuntor p deve operar. Caso contrário, não.
- Transformador: se a barra de referência do disjuntor $p \in Dv_l$ é um terminal da seção i , então o disjuntor p deve abrir. No entanto, se o disjuntor p é o próprio disjuntor k , então o disjuntor que deve abrir é o disjuntor localizado no terminal oposto do transformador.

Se um gerador pertencer ao conjunto VR_{v_i} , a classificação de falta externa vista pelo gerador deve ser reportado. As classificações de “falta externa direcional” vista por transformadores que devem ser adicionados ao padrão P_{mk} são identificados por meio da seguinte condição: se o alarme direcional c_q pertence a um transformador do conjunto V_{r_i} e a barra de referência desse alarme bc_q pertence ao conjunto de vizinhos da seção i , conjunto Vv_i , então o alarme c_q deve ser reportado.

3.7.2.6 Exemplo de aplicação

O sistema de transmissão mostrado na Figura 3.19 é utilizado para exemplificar o funcionamento do gerador automático de padrões. O sistema é composto por cinco seções, protegido por quatro disjuntores e pelos esquemas de proteção vistos no item 3.7.1 deste trabalho.

Figura 3.19 – Sistema de transmissão



As informações de topologia extraídas do banco de dados são as seguintes:

$$De_{e1} = \{CB1\}, De_{e2} = \{CB2\}, De_{e3} = \{CB3\} \text{ e } De_{e4} = \{CB4\},$$

$$E = \{e1, e2, e3, e4\},$$

$$V = \{B1, B2, B3, L1, L2\},$$

$$Ve_{e1} = \{B1, L1\}, Ve_{e2} = \{B2, L1\}, Ve_{e3} = \{B2, L2\} \text{ e } Ve_{e4} = \{B3, L2\}.$$

O conjunto de disjuntores do sistema é obtido aplicando da eq. (3.1):

$$D = De_{e1} \cup De_{e2} \cup De_{e3} \cup De_{e4} = \{CB1, CB2, CB3, CB4\}.$$

O conjunto de arestas do equipamento i é obtido aplicando a eq. (3.2):

$$Ev_{B1} = \{e1\}, Ev_{B2} = \{e2, e3\}, Ev_{e3} = \{e4\}, Ev_{L1} = \{e1, e2\} \text{ e } Ev_{L2} = \{e3, e4\}.$$

O conjunto de arestas do disjuntor k é obtido aplicando a eq. (3.3):

$$Ed_{CB1} = \{e1\}, Ed_{CB2} = \{e2\}, Ed_{CB3} = \{e3\} \text{ e } Ed_{CB4} = \{e4\}.$$

O conjunto dos vizinhos do equipamento i é obtido aplicando a eq. (3.4):

$$Vv_{B1} = \{L1\}, Vv_{B2} = \{L1, L2\}, Vv_{B3} = \{L2\}, Vv_{L1} = \{B1, B2\} \text{ e } Vv_{L2} = \{B2, B3\}.$$

O conjunto dos disjuntores da seção i é obtido aplicando a eq. (3.5):

$$Dv_{B1} = \{CB1\}, Dv_{B2} = \{CB2, CB3\}, Dv_{B3} = \{CB4\},$$

$$Dv_{L1} = \{CB1, CB2\} \text{ e } Dv_{L2} = \{CB3, CB4\}.$$

O conjunto das seções protegidas pelo disjuntor k é obtido aplicando a eq. (3.6):

$$Vd_{CB1} = \{B1, L1\}, Vd_{CB2} = \{B2, L1\}, Vd_{CB3} = \{B2, L2\} \text{ e } Vd_{CB4} = \{B3, L2\}.$$

O conjunto de barras vizinhas da seção i é obtido aplicando a eq. (3.7):

$$Bv_{B1} = \emptyset, Bv_{B2} = \emptyset, Bv_{B3} = \emptyset, Bv_{L1} = \{B1, B2\} \text{ e } Bv_{L2} = \{B2, B3\}.$$

O conjunto dos vizinhos da barra vizinha que podem oferecer proteção de retaguarda à seção i é obtido aplicando a eq. (3.8):

$$VBv_{B1} = \emptyset, VBv_{B2} = \emptyset, VBv_{B3} = \emptyset, VBv_{L1} = \{L2\} \text{ e } VBv_{L2} = \{L1\}.$$

O conjunto de todos os vizinhos que podem oferecer proteção de retaguarda ao equipamento i é obtido aplicando a eq. (3.9):

$$VRv_{B1} = \{L1\}, VRv_{B2} = \{L1, L2\}, VRv_{B3} = \{L2\}, VRv_{L1} = \{L2\} \text{ e } VRv_{L2} = \{L1\}.$$

As barras de referência dos disjuntores k são obtidas aplicando a eq. (3.10):

$$bd_{CB1} = B1, bd_{CB2} = B2, bd_{CB3} = B2 \text{ e } bd_{CB4} = B3.$$

Como todas variáveis bd_k já foram identificadas, a eq. (3.11) não é considerada neste exemplo. Os terminais do equipamento i são obtidos substituindo os valores de bd_k na eq. (3.12), ou seja,

$$T_{B1} = \{B1\}, T_{B2} = \{B2\}, T_{B3} = \{B3\}, T_{L1} = \{B1, B2\} \text{ e } T_{L2} = \{B2, B3\}.$$

A identificação das classificações de evento que serão utilizadas pelo gerador de padrões é realizada por meio do algoritmo mostrado na Figura 3.16:

$$Cv_{B1} = \{B1_FI, B1_FE\}, Cv_{B2} = \{B2_FI, B2_FE\}, Cv_{B3} = \{B3_FI, B3_FE\},$$

$$Cv_{L1} = \{L1_FI, L1_FD \rightarrow B1, L1_FD \rightarrow B2\} \text{ e } Cv_{L2} = \{L2_FI, L2_FD \rightarrow B2, L2_FD \rightarrow B3\}.$$

em que,

FI é falta interna;

FE é falta externa;

FD→B1 é falta externa na direção da barra B1;

FD→B2 é falta externa na direção da barra B2;

FD→B3 é falta externa na direção da barra B3.

O conjunto das classificações geradas é obtido por meio da eq. (3.13):

$$C = \left\{ \begin{array}{l} B1_FI, B1_FE, B2_FI, B2_FE, B3_FI, B3_FE, L1_FI, L1_FD \rightarrow B1, \\ L1_FD \rightarrow B2, L2_FI, L2_FD \rightarrow B2, L2_FD \rightarrow B3 \end{array} \right\}.$$

Os dados acima correspondem aos parâmetros utilizados para a geração de padrões. O número total de colunas da matriz de padrões P é calculado utilizando a eq. (3.14):

$$n = |B| + |C| = 4 + 12 = 16$$

sendo as colunas (1-4) referidas aos alarmes de disjuntores e as colunas (5-16) referidas as classificações de eventos em nível de equipamento.

A geração de padrões é dividida em três etapas: proteção principal, proteção de retaguarda local e proteção de retaguarda remota. O algoritmo desenvolvido para a determinação do evento de falta com operação da proteção principal é mostrado no item 3.7.2.3. Com fins didáticos, será apresentada a filtragem de classificações e alarmes considerando uma falta na linha L1. O padrão P_m é formado pelos seguintes alarmes e classificações:

- Os alarmes de disjuntores do conjunto $D_{v_{L1}}$, ou seja, {CB1, CB2};
- A classificação de falta interna na linha L1, {L1_FI};
- A classificação de falta externa na direção de B2 vista por L2, {L2→B2}.

A segunda etapa é a geração de padrões de funcionamento da proteção de retaguarda local. Considerando uma falta na linha L1 com falha na abertura de CB2, o padrão P_m é formado pelos seguintes alarmes e classificações:

- Alarmes disjuntores de $D_{v_{L1}}$, exceto CB2, ou seja, {CB1};
- A classificação de falta interna na linha L1 {L1_FI};
- Classificação de falta externa vista pela barra B2, {B2_FE};
- Alarmes dos disjuntores de $D_{v_{B2}}$, exceto CB2, {CB3}.

A terceira etapa é a geração de padrões de funcionamento da proteção de retaguarda remota. Considerando uma falta na linha L1 com falha na abertura de CB2, o padrão P_m é formado pelos seguintes alarmes e classificações:

- Alarmes disjuntores de $D_{v_{L1}}$, exceto CB2, ou seja, {CB1};
- A classificação de falta interna na linha L1 {L1_FI};

- Classificação de falta externa vista linha L2, $\{L2 \rightarrow B2\}$;
- Alarmes dos disjuntores de D_{VL2} , $\{CB4\}$. O disjuntor CB4 foi corretamente identificado, pois a barra de referência $bd_{CB4} = \{B4\}$ não é terminal da linha L1, $T_{L1} = \{B1, B2\}$.

3.8 Considerações finais

Neste capítulo foram apresentadas as rotinas desenvolvidas para o processamento de alarmes. Ao todo, foram propostas quatro rotinas: reordenação cronológica de alarmes, mapeamento de eventos, identificação da topologia da rede e geração de padrões de eventos. Os métodos propostos utilizam uma estrutura de dados específica para o problema de diagnóstico de faltas em SEPs.

O método proposto para reordenação cronológica de alarmes reportados é baseado em máquinas de estados finitos. Cada máquina descreve a cronologia esperada de alarmes reportados em diferentes esquemas de proteção. No total, foram modeladas cinco máquinas de estado: proteção principal e religamento de LTs; proteção principal de barras e transformadores; proteção de sobrecorrente em transformadores; lógica contra falha de disjuntor; e proteção de retaguarda remota em linhas.

O mapeamento de eventos tem como objetivo identificar eventos dentro de uma janela de dados recebidos. A identificação dos alarmes reportados é utilizada para determinar os equipamentos sensibilizados por distúrbios e para identificar a lista de seções suspeitas de estarem em falta. A identificação topológica da rede é realizada em tempo real por meio da identificação das adjacências de equipamentos.

Por fim, foi apresentado o algoritmo de geração de padrões de funcionamento do sistema de proteção. O algoritmo foi desenvolvido para sistemas de proteção que atendam os requisitos técnicos estabelecidos pelo ONS. O gerador utiliza quatro conjuntos de dados para determinar os alarmes que devem ser reportados caso cada seção do SEP esteja em falta. Os padrões gerados consideram a atuação das proteções principal, retaguarda local e retaguarda remota.

4 MODELOS DE PROGRAMAÇÃO MATEMÁTICA PARA DIAGNÓSTICO DE FALTAS

4.1 Considerações iniciais

Este capítulo apresenta quatro modelos de programação matemática desenvolvidos para diagnóstico de faltas em sistemas de potência. Os modelos são fundamentados na teoria da parcimônia e no problema de recobrimento de conjuntos, tendo como objetivos principais a estimação da seção em falta e a identificação dos dispositivos de proteção com atuação imprópria. Além disso, os modelos foram formulados de forma a incorporar diferentes características do sistema elétrico monitorado.

4.2 Critérios utilizados na formulação dos modelos de otimização

De acordo com Wen e Chang (1997), o problema de estimação da seção em falta tem como objetivo encontrar diagnósticos que expliquem os alarmes reportados. Após um distúrbio no sistema elétrico, um diagnóstico pode ser obtido respondendo as seguintes questões (DIJK, 1992):

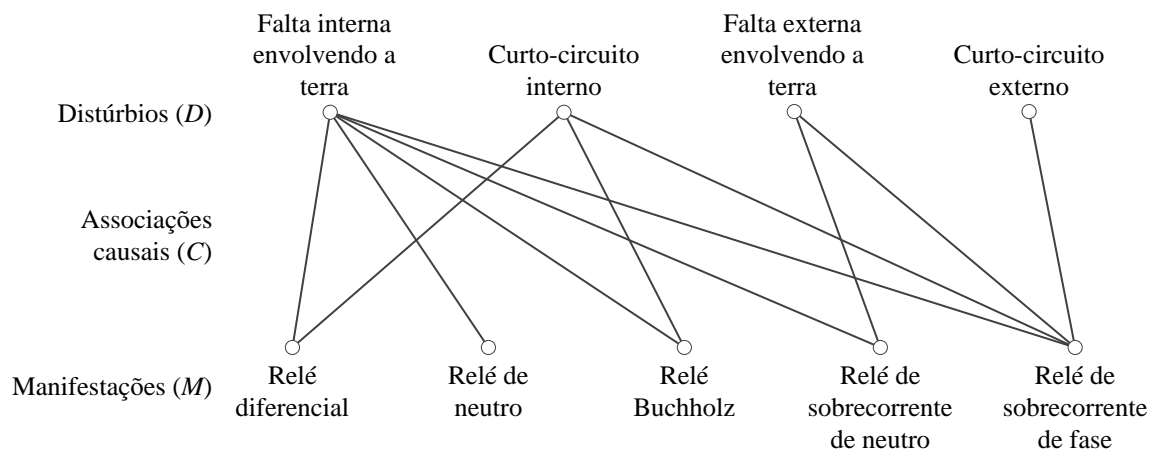
- o que aconteceu?
- em que local do sistema originou-se o distúrbio?
- houve mau funcionamento de dispositivos de proteção?
- existem alarmes inconsistentes?

Como regra geral, os sistemas de diagnóstico empregam regras de inferência para definir um conjunto de hipóteses plausíveis que expliquem satisfatoriamente um conjunto de manifestações observadas. A correlação entre hipóteses e manifestações é obtida utilizando uma base de conhecimento que contenha a relação entre distúrbios e suas possíveis manifestações. Um modelo de diagnóstico requer a definição de, no mínimo, quatro conjuntos (PENG; REGGIA, 1986):

- $D = \{d_1, \dots, d_n\}$ é o conjunto de distúrbios (causas);
- $M = \{m_1, \dots, m_k\}$ é o conjunto de manifestações (efeitos);
- $C \subseteq D \times M$ é a relação entre causas e efeitos;
- $M^+ \subseteq M$ é uma manifestação contida em M .

A Figura 4.1 exemplifica a relação de distúrbios com a atuação de relés da proteção em transformadores.

Figura 4.1 – Rede causal para diagnóstico de faltas em um transformador



O distúrbio que melhor representa um conjunto de manifestações pode ser identificado modelando o problema de diagnóstico como um problema SCP e utilizando a teoria da parcimônia. Um modelo formalizado a partir destes dois critérios adota o critério da plausibilidade, onde uma cobertura mais simples é preferível a uma cobertura mais complexa.

No exemplo do transformador, a atuação única do relé de sobrecorrente de fase pode indicar a ocorrência de qualquer tipo de distúrbio. Por outro lado, apenas o curto-circuito externo é caracterizado pela atuação única do relé de sobrecorrente de fase, visto que os demais distúrbios possuem outros dispositivos de proteção. Sendo assim, é dito então que a hipótese de curto-circuito externo é uma cobertura parcimoniosa (simples) para a manifestação à atuação única do relé de sobrecorrente.

Portanto, um conjunto de hipóteses plausíveis é definido como cobertura parcimoniosa de uma manifestação se ele cobrir todo M^+ e satisfizer o critério de ser, dentre todas as opções possíveis, o mais parcimonioso ou “simples”. Em geral, procura-se uma única hipótese, no entanto, podem existir mais do que uma explicação para M^+ . (PENG; REGGIA, 1986).

4.3 Métodos propostos para a estimação da seção em falta

Desde o trabalho pioneiro de Fukui e Kawakami (1986), diagnosticar faltas em sistemas elétricos de potência por meio de uma rede causa-efeito que relaciona alarmes de dispositivos de proteção e possíveis diagnósticos é a forma mais empregada para estimar a

seção em falta. No entanto, métodos baseados nesta base de dados possuem limitação de aplicabilidade em grandes sistemas de potência devido à grande complexidade de regras que precisam ser geradas. A complexidade se deve ao grande número de equipamento, esquemas de proteção e alarmes, além da necessidade de especialistas que conheçam, detalhadamente, a operação do sistema de potência tanto em nível de subestação quanto de sistema. Neste trabalho, o método que segue a metodologia de obter diagnósticos a partir da análise direta dos alarmes reportados no SCADA é denominado de Método AD.

Cardoso Jr., Rolim e Zurn (2004) dividiram o processo de diagnóstico em duas etapas: primeiramente, a falta é classificada de acordo com a operação de cada esquema de operação distinto; a seguir, o diagnóstico é gerado utilizando os eventos gerados na primeira etapa. Uma grande vantagem da divisão do problema em dois níveis é permitir a redução do custo computacional envolvido na resolução do problema de diagnóstico, além de usar bases de conhecimentos menores do que o método AD.

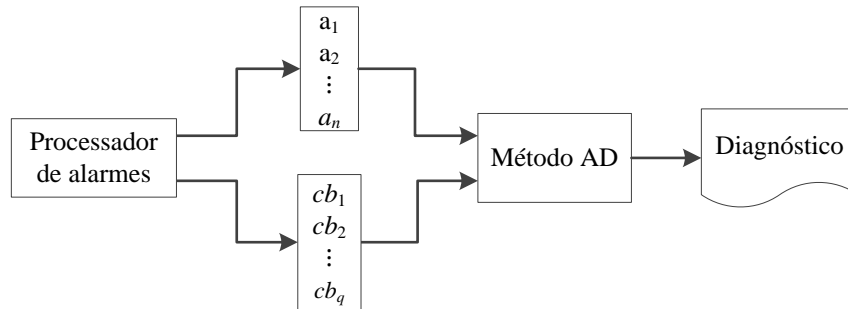
Os métodos baseados nessa metodologia são compostos por dois métodos de análise distintos: uma heurística pode ser empregada na análise local de alarmes para obtenção de eventos; e um método baseado em modelos de otimização para diagnóstico dos eventos processados. O método que incorpora um modelo de programação matemática para a obtenção de diagnósticos a partir de eventos é denominado de Método ED. Neste trabalho, são propostos dois métodos que seguem essa metodologia: Método ED1 e Método ED2. Em ambos os métodos, a análise local é realizada através de uma heurística baseada no Teorema de Bayes.

Uma grande desvantagem da metodologia dividida em duas etapas é que ela não garante a solução ótima do problema, visto que a primeira etapa é avaliada uma única vez de forma isolada. Para contornar esse problema, foi desenvolvida a metodologia AED que se propõe a analisar os alarmes e gerar eventos e diagnósticos por meio de um único método de diagnóstico. O Método AED incorpora um modelo de programação matemática que determina os eventos que melhor explicam os alarmes reportados ao mesmo tempo em que determina os diagnósticos que melhor explicam os eventos processados. Esse método combina as vantagens do método AD (garantia da melhor solução) e do método ED (bases de conhecimento reduzidas).

4.4 Método AD

O fluxograma da metodologia de diagnóstico AD é apresentado na Figura 4.2.

Figura 4.2 – Fluxograma da metodologia AD



Após um distúrbio, o processador de alarmes recebe os alarmes do SCADA e agrupa os alarmes de relés $[a_1, \dots, a_n]$ e de disjuntores $[cb_1, \dots, cb_q]$. Os alarmes reportados são analisados pelo método AD utilizando um conjunto de padrões que relaciona possíveis seções em falta com os alarmes esperados de sistemas de proteção. O diagnóstico corresponde à solução apresentada ao operador e é formado pelas seções em falta e pelos dispositivos de proteção com atuação indevida.

O método AD proposto incorpora um modelo de programação matemática baseado na teoria da parcimônia e no problema de recobrimento de conjuntos. Esse método tem aplicabilidade restrita a pequenos sistemas de potência, com pequeno número de subestações devido à alta complexidade da montagem de padrões de funcionamento dos sistemas de proteção. Por outro lado, a simplicidade deste modelo torna mais fácil a formalização de novos critérios. Nesse sentido, o modelo AD foi idealizado de forma a estimar a seção em falta, identificar os alarmes falsos e falhos, identificar subestações com falha na comunicação ou falta CC, e com restrição no número total de alarmes falhos. A seguir é mostrado o modelo desenvolvido para o método AD.

Conjuntos

B é o conjunto de índices das subestações sem alarmes reportados;

I é o conjunto de índices dos diagnósticos;

J é o conjunto de índices dos alarmes;

D_j é o conjunto de índices dos diagnósticos associados ao alarme j ;

A_i é o conjunto de índices dos alarmes associados ao diagnóstico i .

Parâmetros

$$a_j = \begin{cases} 1, & \text{se o alarme } j \text{ é acionado} \\ 0, & \text{caso contrário} \end{cases}$$

$$b_j = \begin{cases} 1, & \text{se o alarme } j \in B \\ 0, & \text{caso contrário} \end{cases}$$

M_i é um número suficientemente grande, no caso, $M_i = |A_i|$;

w_1, w_2, w_3 são os pesos da FO;

w_4 é o limite percentual de alarmes falhos de um diagnóstico.

Variáveis

$$bf_j = \begin{cases} 1, & \text{se o alarme } j \text{ é inexistente} \\ 0, & \text{caso contrário} \end{cases}$$

$$d_i = \begin{cases} 1, & \text{se o diagnóstico } i \text{ é escolhido para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$s_j = \begin{cases} 1, & \text{se o alarme } j \text{ é falso} \\ 0, & \text{caso contrário} \end{cases}$$

$$f_j = \begin{cases} 1, & \text{se o alarme } j \text{ é falho} \\ 0, & \text{caso contrário} \end{cases}$$

Modelo

$$\min w_1 \sum_{j \in J} s_j + w_2 \sum_{j \in J} f_j + w_3 \left(\sum_{i \in I} d_i + \sum_{j \in J} bf_j \right) \quad (4.1)$$

sujeito a

$$s_j + \sum_{i \in D_j} d_i \geq a_j \quad \forall j \in J \quad (4.2)$$

$$d_i \leq (1 - b_j) f_j + b_j bf_j \quad \forall i \in I, \forall j \in \{A_i : a_j = 0\} \quad (4.3)$$

$$\sum_{j \in A_i} (f_j + bf_j) \leq w_4 |d_i| + M_i (1 - d_i) \quad \forall i \in I \quad (4.4)$$

$$d_i \in \{0, 1\} \quad \forall i \in I \quad (4.5)$$

$$bf_j, s_j, f_j \in \{0, 1\} \quad \forall j \in J \quad (4.6)$$

A eq. (4.1) é a FO do modelo, em que $w_1 \geq w_2 \geq w_3$ são os pesos empregados para refletir a importância relativa de cada variável de decisão e atender ao princípio da parcimônia. A solução ótima do modelo é aquela que apresentar o menor número de diagnósticos, alarmes falsos, alarmes falhos e alarmes inexistentes. O alarme bf_j pertence a uma subestação com falha de comunicação ou falta CC e é definido como inexistente. Esse é um dos motivos pelo qual a penalização do alarme bf_j é menor do que em alarmes falhos f_j . Outro motivo é permitir ao modelo encontrar o máximo de informação necessária na subestação com falha para explicar a falta, de forma a tornar a solução elegível.

De acordo com a restrição (4.2), o alarme reportado j deve estar associado a um diagnóstico i ao menos, caso contrário o alarme j é considerado falso. A restrição (4.3) determina que para um diagnóstico i , o alarme j é falho ou não. Se o alarme j não é reportado e pertence a uma subestação sem alarmes reportados (possivelmente com falta CC), então o alarme j é considerado inexistente. Se o alarme j não é reportado e não pertence a uma subestação com falha, então o alarme j é considerado falho.

A restrição (4.4) determina que o número de alarmes falhos e inexistentes deve ser menor do que o número de alarmes reportados do diagnóstico i . Ainda sobre esta restrição, um parâmetro M_i (*Big-M*) é utilizado para determinar quando a restrição é válida, ou seja, a restrição só passa a ser efetiva se o diagnóstico d_i assumir valor 1. Para melhorar o desempenho de resolvidores de programação inteira baseados em relaxações lineares, o valor de M_i é definido como $|A_i|$.

O número de alarmes falhos não pode ser maior do que um percentual w_4 de alarmes do diagnóstico d_i , em que $0 \leq w_4 \leq 1$. Neste trabalho, considera-se $w_4 = 0,5$ para evitar a escolha de um diagnóstico d_i que tenha um número de alarmes falhos maior que o número de alarmes deste diagnóstico reportados. As equações (4.5) e (4.6) são restrições de domínio das variáveis de decisão.

Caso a proteção funcione corretamente, os alarmes reportados devem ser suficientes para diagnosticar a falta. Neste caso, o modelo do método AD fica reduzido a um problema SCP e não há identificação de alarmes falhos e falsos. Quando a proteção opera indevidamente, é necessário ajustar os pesos da FO (4.1), de forma a discriminar os alarmes indevidos. É comumente aceito que alarmes falsos são mais raros que alarmes falhos, cuja suposição resulta em $w_1 \geq w_2$. Neste trabalho, os valores dos pesos são obtidos heurísticamente de acordo com as características do SEP. Observe que os pesos w_1 , w_2 , w_3 e w_4 são parâmetros exógenos ao modelo matemático e relacionados ao SEP monitorado.

4.4.1 Exemplo numérico das restrições (4.3) e (4.4)

O exemplo abaixo ilustra matematicamente como a restrição (4.3) é interpretada no modelo. Considere $A_1 = \{1,2,3\}$, $a = \{1,0,1\}$. Como $a_1 = a_3 = 1$, a restrição (4.3) somente é válida para o alarme a_2 , ou seja,

$$d_1 \leq (1-b_2)f_2 + b_2bf_2.$$

Caso o alarme a_2 não pertença ao conjunto de SEs com nenhum alarme reportado, então $b_2 = 0$. Logo:

$$d_1 \leq (1-0)f_2 + 0 \cdot bf_2$$

$$d_1 \leq f_2.$$

Dessa forma, o alarme a_2 é considerado falho para d_1 . Caso $b_2 = 1$, então:

$$d_1 \leq (1-1)f_2 + 1 \cdot bf_2$$

$$d_1 \leq bf_2.$$

Dessa forma, o alarme a_2 é considerado inexistente para o diagnóstico d_1 .

O exemplo abaixo ilustra matematicamente como a restrição (4.4) é interpretada no modelo. Considere $A_1 = \{1,2,3\}$, $b = \{0,0,0\}$ e $w_4 = 0,5$. O *Big-M* (M_1) é igual à cardinalidade de A_1 , ou seja, $M_1 = |A_1| = 3$.

Caso $a = \{1,0,0\}$, a restrição (4.4) fica reduzida a:

$$f_2 + f_3 \leq 0,5 \cdot 3 + 3(1-d_1).$$

Se d_1 é escolhido como solução ($d_1 = 1$), a restrição é válida e somente um dos alarmes (a_2 ou a_3) pode ser considerado falho, pois:

$$f_2 + f_3 \leq 1,5.$$

Se d_1 não é escolhido como solução ($d_1 = 0$), devido ao *Big-M*, a restrição é trivialmente satisfeita e deixa de ser válida, ou seja,

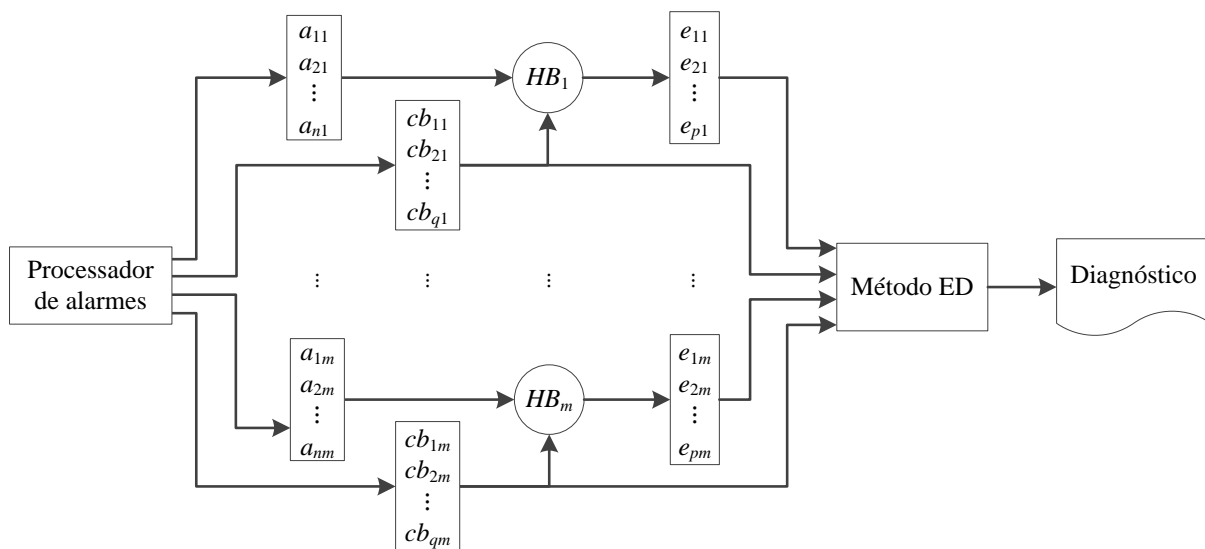
$$f_2 + f_3 \leq 4,5.$$

4.5 Métodos ED

A metodologia ED decompõe o problema de estimação da seção em falta em dois níveis distintos de análise: nível de equipamento e nível de sistema. A análise em nível de equipamento visa classificar eventos localmente, utilizando apenas os alarmes reportados de um esquema de proteção e regras que ilustram o funcionamento esperado da proteção. A análise em nível de sistema utiliza um procedimento para analisar os eventos processados em nível de sistema e determinar o diagnóstico da falta.

A Figura 4.3 mostra o processo de diagnóstico que segue a metodologia ED. A classificação de eventos é realizada por uma heurística baseada no teorema de Bayes (HB) e um método que incorpora um modelo de otimização que gera diagnósticos a partir de eventos analisados, chamado de Método ED.

Figura 4.3 – Fluxograma da metodologia ED



O processador de alarmes identifica e agrupa os alarmes $\{[a_{11}, \dots, a_{n1}], \dots, [a_{1m}, \dots, a_{nm}]\}$ e $\{[cb_{11}, \dots, cb_{q1}], \dots, [cb_{1m}, \dots, cb_{qm}]\}$ dos m equipamentos cujas proteções foram sensibilizadas após um distúrbio. Os alarmes reportados para cada equipamento são analisados, individualmente, pela heurística de Bayes (HB_1, \dots, HB_m) a fim de classificar o evento. A classificação obtida pertence ao conjunto de possíveis eventos do equipamento analisado, ou seja, $\{[e_1, e_2, \dots, e_{p1}], \dots, [e_1, e_2, \dots, e_{pm}]\}$.

Por fim, a instância contendo o conjunto de alarmes de disjuntores e eventos é analisado pelo método ED. O diagnóstico corresponde à solução apresentada ao operador e é

formado pelas seções em falta e pelos dispositivos de proteção com atuação indevida. É importante salientar que os conjuntos de regras da proteção e padrões de eventos utilizados pelos métodos não são representados na Figura 4.3.

Uma desvantagem desta metodologia recai na dependência do diagnóstico com relação à qualidade das soluções obtidas pelo classificador de evento. Sempre que a primeira etapa errar uma classificação, haverá uma redução de informações a serem processadas, podendo impedir o método ED de encontrar a solução ótima global do problema modelado. Essa característica é inerente a métodos sequenciais, nos quais a falha em um dos passos da sequência de solução pode impactar no sucesso do método como um todo.

4.5.1 Classificação de eventos

O método proposto para classificar eventos em nível de equipamento foi desenvolvido tendo como base o teorema de Bayes. A heurística permite calcular a probabilidade do evento A (conjunto de alarmes) ser explicado por uma regra de proteção r_i do equipamento analisado por meio da equação (4.7), ou seja,

$$P(r_i|A) = \frac{P(r_i)P(A|r_i)}{\sum_{j=1}^n P(r_j)P(A|r_j)} \quad (4.7)$$

em que,

r_i e r_j são regras de proteção (vetor binário de alarmes);

A é o evento analisado (vetor binário de alarmes reportados);

$P(r_i/A)$ é a probabilidade da regra r_i justificar os alarmes do evento A ;

$P(r_i)$ é a probabilidade inicial de ocorrência da regra r_i , antes do evento A ;

$P(A/r_i)$ é a probabilidade da regra r_i produzir os alarmes do evento A .

A eq. (4.7) pode ser interpretada da seguinte forma: se o conjunto de alarmes observados for igual ao evento A , a probabilidade do evento A ser explicado pela i -ésima regra de proteção é proporcional ao produto da probabilidade inicial da regra r_i pela probabilidade da regra r_i produzir A .

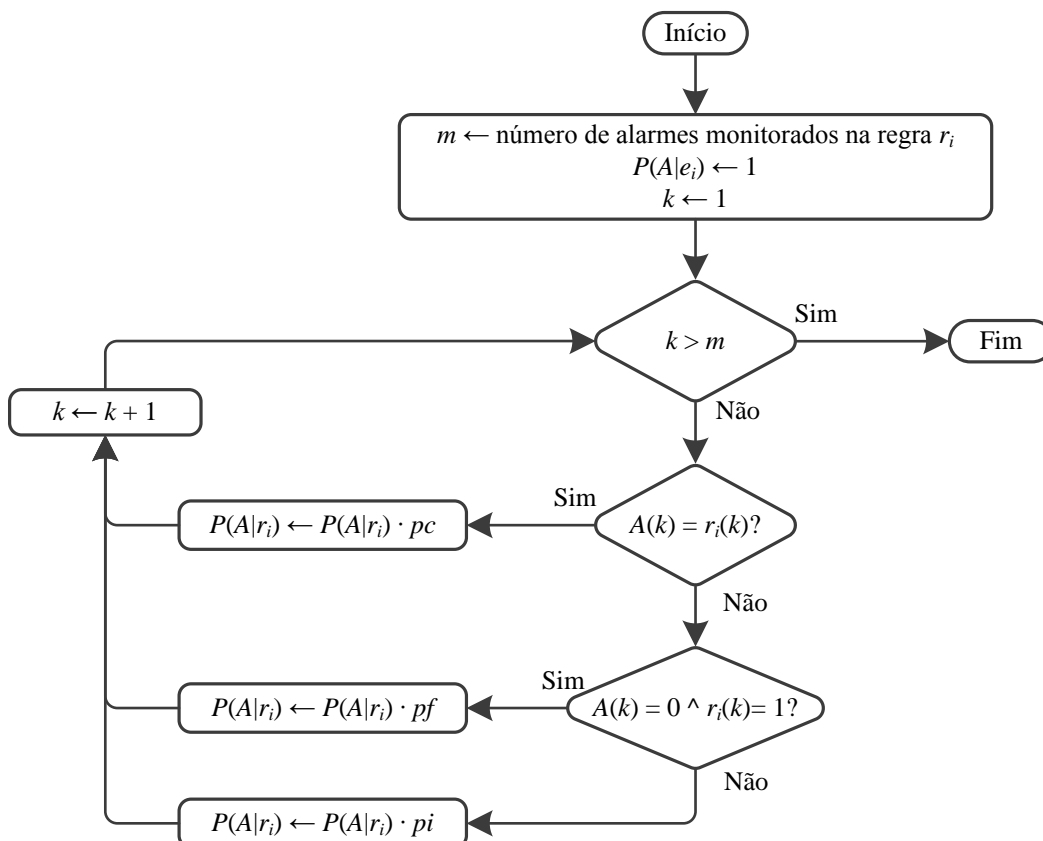
Note que o método requer dados estatísticos sobre a frequência de faltas e dados operativos de dispositivos de proteção para realização dos devidos cálculos. As concessionárias de energia, geralmente, classificam faltas de acordo com a sua causa

(descargas atmosféricas, influência externa, problemas técnicos, etc.) ou de acordo com o tipo de falta (monofásica, bifásica, bifásica-terra, trifásica). Esses dados são úteis para complementar um diagnóstico, mas não são suficientes para ajustar métodos de diagnóstico.

Dados estatísticos referentes ao funcionamento de lógicas de proteção podem ser utilizados para o ajuste da probabilidade inicial $P(r_i)$. No entanto, não existem relatos na literatura de concessionárias que possuam esse tipo de dado. Por esse motivo, $P(r_i)$ é definido como uma constante na eq. (4.7).

O cálculo da probabilidade condicional $P(A|r_i)$ também é afetado pela falta de dados estatísticos. Para contornar esse problema, foi desenvolvido um algoritmo para calcular a probabilidade $P(A|r_i)$ utilizando os seguintes dados históricos de um sistema de proteção em forma de pesos: operação correta (pc), operação falha (pf) e operação indevida (pi). A Figura 4.4 mostra o fluxograma para cálculo da probabilidade.

Figura 4.4 – Fluxograma para cálculo da probabilidade $P(A|e_i)$



A probabilidade $P(A|r_i)$ é igual ao produto dos pesos associados a cada alarme monitorado no equipamento. O valor do peso depende do estado do alarme reportado no SCADA e do estado esperado do alarme pela regra r_i . Os pesos são definidos como:

- pc é o peso de um alarme emitido em A e esperado pela regra r_i . Esse peso também é aplicado para situações onde um alarme não é emitido em A e nem esperado pela regra r_i ;
- pf é o peso de um alarme não emitido em A e esperado pela regra r_i (alarme falho);
- pi é o peso de um alarme emitido em A e não esperado pela regra r_i (alarme falso).

Na ausência de dados estatísticos da proteção, é necessário determinar o ajuste de pesos que melhor represente o sistema de proteção. As regras de proteção modeladas para os esquemas de proteção da CEEE-GT foram utilizadas para análise de sensibilidade dos pesos utilizados para cálculo de $P(A|r_i)$. Diversas simulações de falta incluindo instâncias aleatórias de alarmes foram consideradas no ajuste. Os resultados dos testes realizados mostram que o ajuste ótimo dos pesos deve respeitar as seguintes restrições:

$$0,8 \leq pc \leq 0,9 \quad (4.8)$$

$$0,33 \leq \frac{pi}{pf} \leq 3 \quad (4.9)$$

$$pc + pi + pf = 1 \quad (4.10)$$

As equações acima são utilizadas como referência para ajuste dos pesos e dependem das características da proteção empregada. No entanto, se dados estatísticos de faltas no SEP estiverem disponibilizadas, então as equações (4.8) e (4.9) podem ser ignoradas.

4.5.1.1 Exemplo numérico

Considere o evento $A = \{1,0,1\}$ (1, alarme reportado; 0, alarme não reportado), as regras $r_1 = \{1,1,0\}$, $r_2 = \{0,0,1\}$ e $r_3 = \{0,1,0\}$ (1, alarme esperado; 0, alarme não esperado), e os pesos $pc = 0,75$, $pi = 0,15$ e $pf = 0,10$. As probabilidades $P(A|r_i)$ são calculadas através do algoritmo da Figura 4.4, ou seja,

$$P(A|r_1) = P\left(\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \middle| \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}\right) = 0,75 \cdot 0,10 \cdot 0,15 = 0,01125$$

$$P(A|r_2) = P\left(\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \middle| \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}\right) = 0,15 \cdot 0,75 \cdot 0,75 = 0,084375$$

$$P(A|r_3) = P\left(\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \middle| \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}\right) = 0,15 \cdot 0,10 \cdot 0,15 = 0,00225 .$$

A probabilidade da regra r_i justificar A é calculada aplicando a eq. (4.7):

$$P(r_1 | A) = \frac{0,01125}{0,01125 + 0,084375 + 0,00225} = \frac{0,01125}{0,097875} = 0,11494$$

$$P(r_2 | A) = \frac{0,084375}{0,01125 + 0,084375 + 0,00225} = \frac{0,084375}{0,097875} = 0,86207$$

$$P(r_3 | A) = \frac{0,00225}{0,01125 + 0,084375 + 0,00225} = \frac{0,00225}{0,097875} = 0,02299.$$

Dessa forma, é possível concluir que a regra r_2 é a melhor explicação para os alarmes reportados no evento A com a probabilidade de 86,207%.

4.5.2 Método ED1

O método ED1 incorpora um dos possíveis modelos de programação inteira mista que podem ser formalizados para o problema de estimação da seção em falta. O modelo é semelhante ao modelo BIP proposto por Fritzen et al. (2012), com a inclusão de restrição que determina o número de eventos falhos para cada diagnóstico escolhido para explicar os alarmes reportados. Abaixo são apresentados os conjuntos, parâmetros e variáveis utilizados no modelo do método ED1.

Conjuntos

I é o conjunto de índices dos diagnósticos;

J é o conjunto de índices dos eventos e alarmes de disjuntores;

D_j é o conjunto de índices dos diagnósticos associados ao evento j ;

E_i é o conjunto de índices dos eventos e alarmes de disjuntores associados ao diagnóstico i .

Parâmetros

$$e_j = \begin{cases} 1, & \text{se o evento } j \text{ é escolhido} \\ 0, & \text{caso contrário} \end{cases}$$

M_i é um número suficiente grande, no caso, $M_i = |E_i|$;

w_1, w_2, w_3 são os pesos da FO.

Variáveis

$$e_i = \begin{cases} 1, & \text{se o evento } i \text{ é escolhido para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$s_j = \begin{cases} 1, & \text{se o evento } j \text{ é falso} \\ 0, & \text{caso contrário} \end{cases}$$

$$f_j = \begin{cases} 1, & \text{se o evento } j \text{ é falho} \\ 0, & \text{caso contrário} \end{cases}$$

$vd_i \geq 0$, é o número de eventos falhos do diagnóstico d_i .

Modelo

$$\min w_1 \sum_{j \in J} s_j + w_2 \sum_{i \in I} vd_i + w_3 \sum_{i \in I} d_i \quad (4.11)$$

sujeito a

$$s_j + \sum_{i \in D_j} d_i \geq e_j \quad \forall j \in J \quad (4.12)$$

$$d_i \leq f_j \quad \forall i \in I, \forall j \in \{E_i : e_j = 0\} \quad (4.13)$$

$$M_i(d_i - 1) + \sum_{j \in E_i} f_j \leq vd_i \quad \forall i \in I \quad (4.14)$$

$$d_i \in \{0,1\} \quad \forall i \in I \quad (4.15)$$

$$s_j, f_j \in \{0,1\} \quad \forall j \in J \quad (4.16)$$

$$vd_i \geq 0 \quad \forall i \in I \quad (4.17)$$

A eq. (4.11) é a FO do modelo, em que $w_1 \geq w_2 \geq w_3$ são os pesos empregados para refletir a importância relativa de cada variável de decisão e, desta forma, atender ao princípio da parcimônia. Observe que devido à configuração dos pesos, a solução ótima do modelo apresenta o menor número de diagnósticos, eventos falsos e eventos falhos associados a um diagnóstico d_i . A restrição (4.12) determina que um evento deva estar associado a um diagnóstico ao menos, caso contrário, o evento é considerado falso. A lógica dessa restrição é igual à utilizada na restrição (4.2), no entanto, com diferentes parâmetros e variáveis. A restrição (4.13) determina se um diagnóstico é caracterizado por um evento e este não é reportado, então o evento é considerado falho. As restrições (4.15), (4.16) e (4.17) são restrições de domínio das variáveis de decisão.

O diferencial deste modelo em relação ao modelo BIP encontra-se na restrição (4.14), cujas variáveis vd_i indicam o número de eventos falhos presentes no diagnóstico d_i escolhido para compor a solução. Essa restrição torna mais difícil encontrar soluções em que eventos falhos estejam associados a mais de um diagnóstico. Essa restrição possui um *Big-M* com tamanho definido, $M_i = |E_i|$.

Observe que as variáveis vd_i assumem valores inteiros na solução ótima devido ao conjunto de restrições (4.14-4.17). Observe também que os valores vd_i na solução ótima indicam o quanto um diagnóstico d_i se difere do padrão. Em soluções com múltiplos diagnósticos, os valores vd_i podem ser utilizados para fornecer uma ordenação de diagnósticos aos operadores do COS.

Se o sistema de proteção funcionar corretamente, todos os alarmes reportados devem ser suficientes para descrever a falta. Neste caso, o modelo do método AD fica reduzido a um problema SCP e não há identificação de alarmes falhos. Quando a proteção principal não opera corretamente, é necessário ajustar os valores dos pesos na FO (4.1), de forma a discriminar os alarmes falsos dos falhos. É comumente aceito que alarmes falsos são mais raros que alarmes falhos, cuja suposição resulta em $w_1 \geq w_2$. Neste trabalho, os valores dos pesos são obtidos de maneira heurística para cada sistema elétrico de potência.

4.5.3 Método ED2

O método ED2 incorpora outra variação do modelo BIP proposto por Fritzen et al. (2012). Neste caso, o modelo proposto é capaz de entregar o mesmo tipo de resposta do modelo formulado na metodologia AD, ou seja, é capaz de estimar a seção em falta, identificar alarmes falsos e falhos, identificar subestações com falha na comunicação ou falta CC, e restringir alarmes falhos até um limiar ajustado. A seguir são apresentados os conjuntos, parâmetros e variáveis utilizados no modelo formulado para o método ED2.

Conjuntos

B é o conjunto de índices das subestações sem alarmes reportados;

I é o conjunto de índices dos diagnósticos;

J é o conjunto de índices dos alarmes;

D_j é o conjunto de índices dos diagnósticos associados ao evento j ;

E_i é o conjunto de índices dos eventos associados ao diagnóstico i .

Parâmetros

$$b_j = \begin{cases} 1, & \text{se o evento } j \in B \\ 0, & \text{caso contrário} \end{cases}$$

$$c_j = \begin{cases} 2, & \text{se as duas SEs do evento } j \text{ não possuem eventos reportados} \\ 1, & \text{se uma SE do evento } j \text{ não possui eventos reportados} \\ 0, & \text{caso contrário} \end{cases}$$

$$e_j = \begin{cases} 1, & \text{se o evento } j \text{ é acionado} \\ 0, & \text{caso contrário} \end{cases}$$

M_i é um número suficientemente grande, no caso, $M_i = |E_i|$;

w_1, w_2, w_3 são os pesos da FO;

w_4 é limite percentual de alarmes falhos de um diagnóstico.

Variáveis

$$bf_j = \begin{cases} 1, & \text{se o evento } j \text{ é inexistente} \\ 0, & \text{caso contrário} \end{cases}$$

$$cf1_j = \begin{cases} 1, & \text{se o evento } j \text{ é inexistente} \\ 0, & \text{caso contrário} \end{cases}$$

$$cf2_j = \begin{cases} 1, & \text{se o evento } j \text{ é inexistente} \\ 0, & \text{caso contrário} \end{cases}$$

$$d_i = \begin{cases} 1, & \text{se o diagnóstico } i \text{ é escolhido para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$s_j = \begin{cases} 1, & \text{se o evento } j \text{ é falso} \\ 0, & \text{caso contrário} \end{cases}$$

$$f_j = \begin{cases} 1, & \text{se o evento } j \text{ é falho} \\ 0, & \text{caso contrário} \end{cases}$$

Modelo

$$\min w_1 \sum_{j \in J} s_j + w_2 \sum_{j \in J} f_j + w_3 \left\{ \sum_{i \in I} d_i + \sum_{j \in J} (bf_j + cf1_j + cf2_j) \right\} \quad (4.18)$$

sujeito a

(4.12)

$$d_i \leq bf_j b_j + (1 - b_j) \left\{ f_j \left(\frac{2 - c_j}{2} \right) (1 - c_j) + cf1_j c_j (2 - c_j) + cf2_j \frac{c_j}{2} (c_j - 1) \right\} \quad \forall i \in I, \forall j \in \{E_i : e_j = 0\} \quad (4.19)$$

$$\sum_{j \in E_i | b_j = 0} (f_j + bf_j + cf1_j + cf2_j) \leq w_4 |d_i| + M_i (1 - d_i) \quad \forall i \in I \quad (4.20)$$

$$d_i \in \{0, 1\} \quad \forall i \in I \quad (4.21)$$

$$bf_j, cf1_j, cf2_j, s_j, f_j \in \{0, 1\} \quad \forall j \in J \quad (4.22)$$

A eq. (4.18) é a FO do modelo e segue a mesma formulação adotada no modelo do método AD, em que $w_1 \geq w_2 \geq w_3$ são os pesos empregados para refletir a importância relativa de cada variável de decisão e atender ao princípio da parcimônia. A solução ótima do modelo é aquela que apresentar o menor número de diagnósticos, eventos falsos, eventos falhos e eventos inexistentes. O evento bf_j é definido como inexistente, pois pertence a uma subestação com suspeita de falha de comunicação ou falta CC, e pode estar associado a uma classificação de falta em equipamentos de subestações ou a um alarme de disjuntor. O evento $cf1_j$ está associado a eventos de LTs que contenham uma subestação com falha de comunicação ou falta CC. O evento $cf2_j$ está associado a eventos de LTs que contenham duas subestações com falha de comunicação ou falta CC.

A restrição (4.12) do modelo anterior, também é empregada neste modelo e determina que um evento deva estar associado à um diagnóstico ao menos, caso contrário o evento é considerado falso. A restrição (4.19) tem o mesmo princípio de funcionamento das restrições (4.3) e (4.13), ou seja, determina se para um diagnóstico i , o evento j é falho ou não. Se o evento j não é reportado existem quatro possibilidades do evento j ser considerado falho ou inexistente:

- Se $b_j = 1$ então o evento j é considerado inexistente ($bf_j = 1$);
- Se $b_j = 0$ e $c_j = 0$, então o evento j é considerado falho ($f_j = 1$);

- Se $b_j = 0$ e $c_j = 1$, então o evento j é considerado inexistente ($cf1_j = 1$);
- Se $b_j = 0$ e $c_j = 2$, então o evento j é considerado inexistente ($cf2_j = 1$).

A restrição (4.20) possui o mesmo princípio de funcionamento da restrição (4.4) do modelo do método AD, ou seja, determina que o número de eventos falhos deva ser menor do que o número de eventos reportados do diagnóstico i . Essa restrição possui um *Big-M* com tamanho definido, $M_i = |E_i|$. O valor percentual de eventos falhos (w_4) é obtido heurísticamente e deve estar contido no intervalo $0 \leq w_4 \leq 1$. As restrições (4.21) e (4.22) são restrições de domínio das variáveis de decisão.

4.5.3.1 Exemplo numérico da restrição (4.19)

Esse exemplo ilustra matematicamente como a restrição (5.19) é interpretada. Considere $E_1 = \{1,2,3,4,5,6\}$, $e = \{1,1,0,0,0,0\}$, $b = \{0,0,0,1,0,0\}$, $c = \{0,0,0,0,1,2\}$. A restrição (4.19) é válida nos eventos $e_3 = e_4 = e_5 = e_6 = 0$, ou seja,

$$d_1 \leq bf_3b_3 + (1-b_3) \left\{ f_3 \left(\frac{2-c_3}{2} \right) (1-c_3) + cf1_3c_3(2-c_3) + cf2_3 \frac{c_3}{2} (c_3-1) \right\} \quad (4.23)$$

$$d_1 \leq bf_4b_4 + (1-b_4) \left\{ f_4 \left(\frac{2-c_4}{2} \right) (1-c_4) + cf1_4c_4(2-c_4) + cf2_4 \frac{c_4}{2} (c_4-1) \right\} \quad (4.24)$$

$$d_1 \leq bf_5b_5 + (1-b_5) \left\{ f_5 \left(\frac{2-c_5}{2} \right) (1-c_5) + cf1_5c_5(2-c_5) + cf2_5 \frac{c_5}{2} (c_5-1) \right\} \quad (4.25)$$

$$d_1 \leq bf_6b_6 + (1-b_6) \left\{ f_6 \left(\frac{2-c_6}{2} \right) (1-c_6) + cf1_6c_6(2-c_6) + cf2_6 \frac{c_6}{2} (c_6-1) \right\}. \quad (4.26)$$

Para e_3 , substituindo $b_3 = 0$ e $c_3 = 0$ na restrição (4.23), obtêm-se:

$$d_1 \leq bf_3 \cdot 0 + (1-0) \left\{ f_3 \left(\frac{2-0}{2} \right) (1-0) + cf1_3 \cdot 0(2-0) + cf2_3 \frac{0}{2} (0-1) \right\}$$

$$d_1 \leq f_3.$$

Dessa forma, se d_1 compor a solução ótima, então o evento e_3 é considerado evento falho.

Para e_4 , substituindo $b_4 = 1$ e $c_4 = 0$ na restrição (4.24), obtêm-se:

$$d_1 \leq bf_4 \cdot 1 + (1-1) \left\{ f_4 \left(\frac{2-0}{2} \right) (1-0) + cf1_4 \cdot 0(2-0) + cf2_4 \frac{0}{2} (0-1) \right\}$$

$$d_1 \leq bf_4.$$

Dessa forma, se d_1 compor a solução ótima, então o evento e_4 é considerado inexistente.

Para e_5 , substituindo $b_5 = 0$ e $c_4 = 1$ na restrição (4.25), obtêm-se:

$$d_1 \leq bf_5 \cdot 0 + (1-0) \left\{ f_5 \left(\frac{2-1}{2} \right) (1-1) + cf1_5 \cdot 1(2-1) + cf2_5 \frac{1}{2} (1-1) \right\}$$

$$d_1 \leq cf1_5.$$

Dessa forma, se d_1 compor a solução ótima, então o evento e_5 é considerado inexistente.

Para e_6 , substituindo $b_5 = 0$ e $c_4 = 2$ na restrição (4.26), obtêm-se:

$$d_1 \leq bf_6 \cdot 0 + (1-0) \left\{ f_6 \left(\frac{2-2}{2} \right) (1-2) + cf1_6 \cdot 2(2-2) + cf2_6 \frac{2}{2} (2-1) \right\}$$

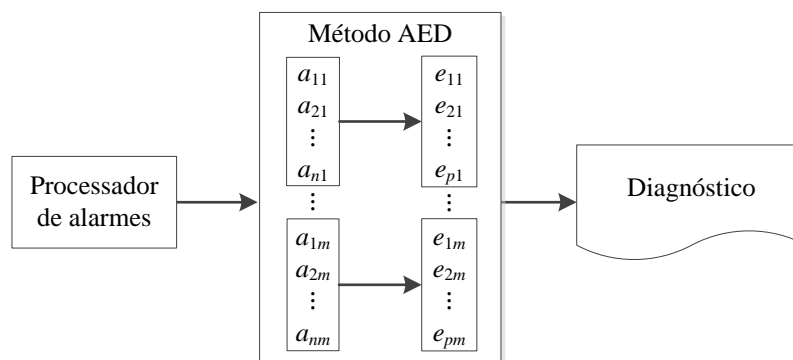
$$d_1 \leq cf2_6.$$

Dessa forma, se d_1 compor a solução ótima, então o evento e_6 é considerado inexistente.

4.6 Método AED

A última metodologia de diagnóstico considerada neste trabalho é a metodologia AED, a qual se assemelha à metodologia ED. A diferença principal reside na resolução integrada do problema, ou seja, o método AED realiza o diagnóstico nos níveis de equipamento e de sistema de forma simultânea. Dessa forma, espera-se que a solução encontrada pelo método AED contenha a melhor explicação dos alarmes reportados. O fluxograma do problema modelado AED é mostrado na Figura 4.5.

Figura 4.5 – Fluxograma da metodologia AED



O processamento de alarmes para o método AED deve conter a mesma informação que seria utilizada pela metodologia ED, ou seja, identificação dos alarmes $\{[a_{11}, \dots, a_{n1}], \dots, [a_{1m}, \dots, a_{nm}]\}$ e $\{[cb_{11}, \dots, cb_{q1}], \dots, [cb_{1m}, \dots, cb_{qm}]\}$ dos m equipamentos com proteções sensibilizadas. O diagnóstico corresponde à solução do problema e é formado pelas seções em falta e pelos dispositivos de proteção com atuação indevida, bem como os eventos escolhidos para classificar a falta em nível de equipamento $\{[e_1, e_2, \dots, e_{p1}], \dots, [e_1, e_2, \dots, e_{pm}]\}$.

O método AED incorpora um modelo formalizado para estimar a seção em falta e classificar eventos em nível de equipamento. Além disso, o modelo permite identificar alarmes falsos e falhos e restringir soluções que contenham um número de alarmes indevidos maior do que um limiar ajustado em cada evento. O modelo AED é descrito a seguir:

Conjuntos

A é o conjunto de índices dos alarmes;

D é o conjunto de índices dos diagnósticos;

E é o conjunto de índices dos eventos;

Q é o conjunto de índices dos equipamentos;

R é o conjunto de índices das regras de proteção;

DE_j é o conjunto de índices dos diagnósticos associados ao evento j ;

ED_i é o conjunto de índices dos eventos associados ao diagnóstico i ;

RE_j é o conjunto de índices das regras associadas ao evento j ;

ER_h é o conjunto de índices dos eventos associados à regra h ;

RA_g é o conjunto de índices das regras associadas ao alarme g ;

AR_h é o conjunto de índices dos alarmes associados à regra h ;

AQq é o conjunto de índices dos alarmes do equipamento q ;

RQq é o conjunto de índices das regras do equipamento q .

Parâmetros

$$a_g = \begin{cases} 1, & \text{se o alarme } g \text{ é acionado} \\ 0, & \text{caso contrário} \end{cases}$$

$w_1, w_2, w_3, w_4, w_5, w_6$ são os pesos da FO;

w_7 é limite percentual de alarmes falhos e falsos de uma regra de proteção.

Variáveis

$$d_i = \begin{cases} 1, & \text{se o diagnóstico } i \text{ é escolhido para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$e_j = \begin{cases} 1, & \text{se o evento } j \text{ é utilizado para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$f_j = \begin{cases} 1, & \text{se o evento } j \text{ é falho} \\ 0, & \text{caso contrário} \end{cases}$$

$$s_j = \begin{cases} 1, & \text{se o evento } j \text{ é falso} \\ 0, & \text{caso contrário} \end{cases}$$

$$r_h = \begin{cases} 1, & \text{se a regra } h \text{ é utilizada para explicar a falta} \\ 0, & \text{caso contrário} \end{cases}$$

$$ff_g = \begin{cases} 1, & \text{se o alarme } g \text{ é falho} \\ 0, & \text{caso contrário} \end{cases}$$

$$ss_g = \begin{cases} 1, & \text{se o alarme } g \text{ é falso} \\ 0, & \text{caso contrário} \end{cases}$$

Modelo

$$\min w_1 \sum_{j \in J} s_j + w_2 \sum_{j \in J} f_j + w_3 \sum_{i \in I} d_i + w_4 \sum_{g \in G} ss_g + w_5 \sum_{g \in G} ff_g + w_6 \sum_{h \in H} r_h \quad (4.27)$$

sujeito a

$$s_j + \sum_{i \in DE_j} d_i \geq e_j \quad \forall j \in E \quad (4.28)$$

$$d_i \leq e_j + f_j \quad \forall i \in D, \forall j \in ED_i \quad (4.29)$$

$$ss_g + \sum_{h \in RA_g} r_h \geq a_g \quad \forall g \in A \quad (4.30)$$

$$r_h \leq ff_g \quad \forall h \in R, \forall g \in \{AR_h : a_g = 0\} \quad (4.31)$$

$$e_j \geq r_h \quad \forall h \in R, \forall j \in ER_h \quad (4.32)$$

$$e_j \leq \sum_{h \in RE_j} r_h \quad \forall j \in E \quad (4.33)$$

$$\sum_{h \in RQ_q} r_h \geq w_7 \sum_{g \in AQ_q} ss_g \quad \forall q \in Q \quad (4.34)$$

$$d_i \in \{0,1\} \quad \forall i \in D \quad (4.35)$$

$$e_j, s_j, f_j \in \{0,1\} \quad \forall j \in E \quad (4.36)$$

$$r_h \in \{0,1\} \quad \forall h \in R \quad (4.37)$$

$$ss_g, ff_g \in \{0,1\} \quad \forall g \in A \quad (4.38)$$

A equação (4.27) é a FO do modelo AED, em que $w_1 \geq w_2 \geq w_3$ e $w_4 \geq w_5 \geq w_6$ são os pesos empregados para refletir a importância relativa de cada variável de decisão e atender ao princípio da parcimônia. A solução ótima do modelo é aquela que apresentar o menor número de diagnósticos, eventos falsos, eventos falhos, regras, alarmes falsos e falhos. As variáveis d_i , s_j e f_j são equivalentes às variáveis dos modelos dos métodos ED e correspondem ao diagnóstico em nível de sistema. As variáveis r_h , ss_g e ff_g são as variáveis de decisão utilizadas para classificar eventos em nível de equipamento.

As restrições (4.28) e (4.29) são empregadas para o diagnóstico em nível de sistema. De acordo com a restrição (4.28), um evento j deve estar associado a um diagnóstico i ao menos, caso contrário o evento j é considerado falso. De acordo com a restrição (4.29), se um evento j não é escolhido, então o evento j é considerado falho para o diagnóstico i .

As restrições (4.30) e (4.31) são empregadas para o diagnóstico em nível local. De acordo com a restrição (4.30), um alarme g deve estar associado à uma regra da proteção h ao

menos, caso contrário o alarme g é considerado falso. De acordo com a restrição (4.31), se um alarme g não é reportado, então o alarme g é considerado falho para uma regra h .

A restrição (4.32) determina que um evento j somente pode ser escolhido se uma regra h for escolhida na análise local. O oposto desta condição também é verdade e é realizada na restrição (4.33). Essas restrições foram formuladas porque existe a possibilidade de um conjunto de regras de proteção representar o mesmo evento em nível de sistema. Em LTs com proteção duplicada, é comum que a proteção principal seja realizada por duas funções de proteção distintas, por exemplo, 87L e zona 1 do 21. No entanto, a atuação de qualquer um destes relés permite a mesma conclusão: a LT está em falta.

A restrição (4.34) determina que se um determinado número de alarmes monitorados em um equipamento q é recebido, então estes alarmes não podem ser considerados falsos. Ou seja, ao menos uma regra r_h deve ser escolhida para explicar os alarmes reportados no equipamento q . Neste trabalho, o limiar w_7 é ajustado em 0,5. As equações (4.35-4.38) são restrições de domínio das variáveis de decisão.

4.7 Considerações finais

Nesse capítulo foram descritos as metodologias adotadas no trabalho para o diagnóstico de faltas em sistemas de potência. Três metodologias foram consideradas: um método que analisa alarmes e gera diagnósticos (AD); um método que analisa alarmes e gera eventos combinado com um método que analisa eventos e gera diagnósticos (ED); e um método que analisa alarmes e gera eventos e diagnósticos (AED).

O método AD incorpora um modelo de otimização que determina a seção em falta, os dispositivos de proteção com atuação indevida, e os alarmes falhos em subestações com falha na comunicação ou falta CC. Dois métodos foram propostos seguindo a metodologia ED, ED1 e ED2, e utilizam uma heurística construtiva baseada no teorema de Bayes para classificação de eventos em nível de equipamento. O método ED1 incorpora um modelo para determinar a seção em falta e os dispositivos de proteção com atuação indevida, com restrição de eventos falhos em dois diagnósticos escolhidos para compor a solução ótima. O modelo do método ED2 permite obter soluções semelhantes às obtidas no modelo do método AD com as vantagens do diagnóstico em dois níveis. Por fim, foi apresentado um modelo baseado na metodologia AED, cujo método engloba as funções formuladas nos modelos anteriores e combina as vantagens dos métodos AD (garantia da solução ótima do problema modelado) e ED (utiliza menor base de padrões).

5 RESULTADOS DO PROCESSADOR DE ALARMES E DISCUSSÕES

5.1 Considerações gerais

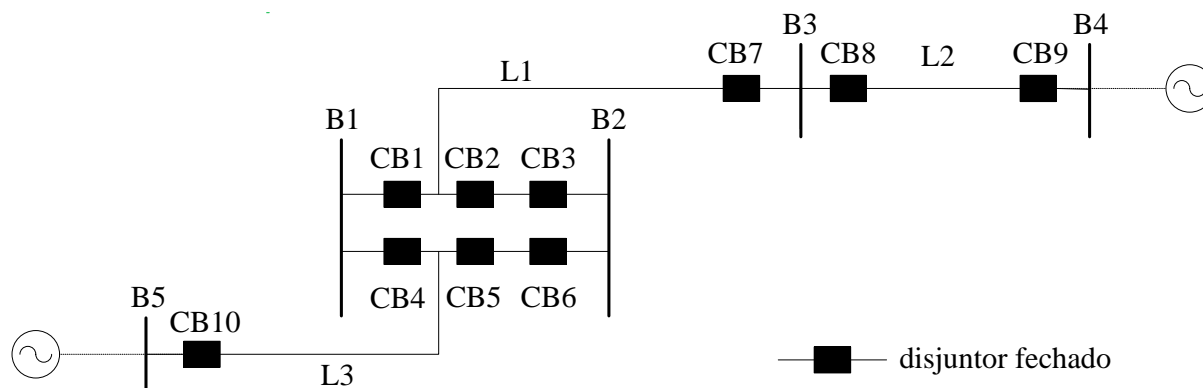
Os resultados experimentais da metodologia proposta desta tese foram divididos em dois capítulos: testes envolvendo funções do processador de alarmes, e simulações de falta com análise dos métodos de diagnóstico. Neste capítulo são apresentados os principais resultados obtidos pelo processador de alarmes em testes computacionais envolvendo diferentes porções de um sistema elétrico de potência de grande porte. As rotinas foram implementadas no *software* Matlab[®] e os resultados foram obtidos utilizando um computador Intel Core i7-2600, 3.4 GHz, 8 GB RAM e sistema operacional Windows 7 de 64 bits. Os testes computacionais foram divididos em três grupos:

- Avaliação do método de reordenação cronológica de alarmes baseado em máquinas de estados;
- Análise do mapeamento de eventos e do processador topológico;
- Avaliação do algoritmo para geração de padrões de funcionamento da proteção.

5.2 Reordenação cronológica dos alarmes

O sistema elétrico mostrado na Figura 5.1 é utilizado para avaliar o impacto no diagnóstico em virtude de erros cronológicos de alarmes reportados.

Figura 5.1 – Topologia pré falta do sistema teste 1



O sistema faz parte do sistema de transmissão sob concessão da CEEE-GT. O sistema é composto de cinco barras, três LTs e dez disjuntores. Os geradores simbolizam a existência

A coluna “Ordem” corresponde à ordem de chegada do alarme; “Hora” corresponde ao instante de disparo do alarme; “Seção” é a seção monitorada pelo alarme; “Proteção” é o código identificador da proteção; “Status” é o estado de disjuntores (1, aberto; 0, fechado) e relés (1, operou; 0, não operou); e “Descrição” é a característica do alarme. A lista dos alarmes reportados apresentam diversos erros cronológicos, como:

- atraso no recebimento de alarmes;
- abertura de disjuntores antes do recebimento de *trip*;
- fechamento de disjuntores antes do religamento automático;
- *reset* de relés antes do religamento automático (Não é um erro, mas essa ação de proteção impacta no mapeamento de eventos).

A Tabela 5.2 apresenta os diagnósticos obtidos pelo método ED1 para a ordem original de alarmes.

Tabela 5.2 – Diagnóstico obtido a partir dos dados da Tabela 5.1

Evento	Seção	Alarme	Status	Classificação	Diagnóstico
1	L1	21-1	0	Normal	Falta em L1 e falha no disjuntor CB7 Eventos falhos: → “Falta em L1”; → “Falta externa na direção de B3 vista por relés de L2”.
		CB1	1		
	CB2	1			
2	L2	21-2	0	Normal	
		CB9	1		
1	L3	21-3	1	Falta externa	
	L1	CB1	0	Normal	
		CB2	0		
2	L2	CB9	0	Normal	Evento falso: → “Falta externa na direção de B1 vista por relés de L3”.

A coluna “Evento” corresponde aos eventos detectados durante a etapa de mapeamento de eventos. A coluna “Seção” contém as seções cujas proteções foram sensibilizadas. As colunas ‘Alarme’ e ‘Status’ contém o dispositivo de proteção e o estado considerado. As colunas ‘Classificação’ e ‘Diagnóstico’ correspondem aos diagnósticos obtidos nos níveis de equipamento e de sistema, respectivamente.

Com a cronologia original de alarmes, foi possível identificar apenas dois eventos na janela de dados. O primeiro evento é caracterizado por alarmes em três componentes (L1, L2

e L3) reportados no período anterior ao instante de religamento da linha L2. O evento associado à linha L3 foi classificado como falta externa, enquanto os demais equipamentos (L1 e L2) foram classificados como “normal” (não há falta). A classificação errada dos eventos está associada às sinalizações de *reset* do relé, que ocorreram antes do alarme 79.

O método ED1 identificou corretamente a origem da falta (linha L1) e o disjuntor falho (CB7). Por outro lado, devido aos erros na classificação, dois eventos foram identificados como falhos. Quanto maior o número de alarmes indevidos ou falhos, mais eventos deverão ser combinados pelo método de diagnóstico para explicar os alarmes reportados.

A Tabela 5.3 apresenta a lista dos alarmes reordenados após aplicação da máquina de estados desenvolvida para a proteção de linhas, conforme visto na Figura 3.6. Note que os alarmes foram agrupados por equipamento monitorado seguindo a sequência original de alarmes reportados, ou seja, na ordem L1, L2 e L3.

Tabela 5.3 – Lista de alarmes após uso das máquinas de estado

Ordem	Hora	Seção	Proteção	Status	Descrição
3	10:03:21	L1	21-1	1	<i>trip</i>
1	10:03:21	L1	CB1	1	abertura
2	10:03:21	L1	CB2	1	abertura
13	10:03:22	L1	79	1	religamento
6	10:03:22	L1	21-1	0	<i>reset</i>
11	10:03:22	L1	CB1	0	fechamento
12	10:03:22	L1	CB2	0	fechamento
7	10:03:22	L2	21-2	1	<i>trip</i>
4	10:03:22	L2	CB9	1	abertura
9	10:03:22	L2	79	1	religamento
8	10:03:22	L2	21-2	0	<i>reset</i>
10	10:03:22	L2	CB9	0	fechamento
5	10:03:22	L3	21-3	1	partida

A Tabela 5.4 mostra os diagnósticos obtidos para a sequência cronológica dos alarmes acima. O reposicionamento dos alarmes 79 permitiu mapear três eventos na janela de dados. Os diagnósticos obtidos mostram que apenas a reordenação por máquinas de estado não fornece a informação requerida pelos métodos, visto que as soluções foram deterioradas.

Tabela 5.4 – Diagnóstico obtido a partir dos dados da Tabela 5.3

Evento	Seção	Alarme	Status	Classificação	Diagnóstico
1	L1	21-1	1	Falta	Alarmes falsos: →CB1 e CB2 Eventos falsos → “Falta em L1”
		CB1	1		
		CB2	1		
2	L1	21-1	0	Normal	Alarmes falsos: → ”Abertura do disjuntor CB9” → ”Falta externa vista por L2”
		CB1	0		
	L2	21-2	1	Falta externa	
		CB9	1		
3	L2	21-2	0	Normal	Evento falso: → ”Falta externa vista por relés de L3”.
		CB9	0		
	L3	21-3	1	Falta externa	

A Tabela 5.5 apresenta a ordenação dos alarmes após uso do critério de tempo de religamento. Note que os alarmes de relés de L2 e L3 foram movidos para antes do alarme 79.

Tabela 5.5 – Lista de alarmes após uso do critério de tempo

Ordem	Hora	Seção	Proteção	Status	Descrição
3	10:03:21	L1	21-1	1	<i>trip</i>
1	10:03:21	L1	CB1	1	abertura
2	10:03:21	L1	CB2	1	abertura
7	10:03:22	L2	21-2	1	<i>trip</i>
4	10:03:22	L2	CB9	1	abertura
5	10:03:22	L3	21-3	1	partida
13	10:03:22	L1	79	1	religamento
6	10:03:22	L1	21-1	0	<i>reset</i>
11	10:03:22	L1	CB1	0	fechamento
12	10:03:22	L1	CB2	0	fechamento
9	10:03:22	L2	79	1	religamento
8	10:03:22	L2	21-2	0	<i>reset</i>
10	10:03:22	L2	CB9	0	fechamento

A Tabela 5.6 contém os resultados obtidos após o sequenciamento de dados.

Tabela 5.6 - Diagnóstico obtido a partir dos dados da Tabela 5.5

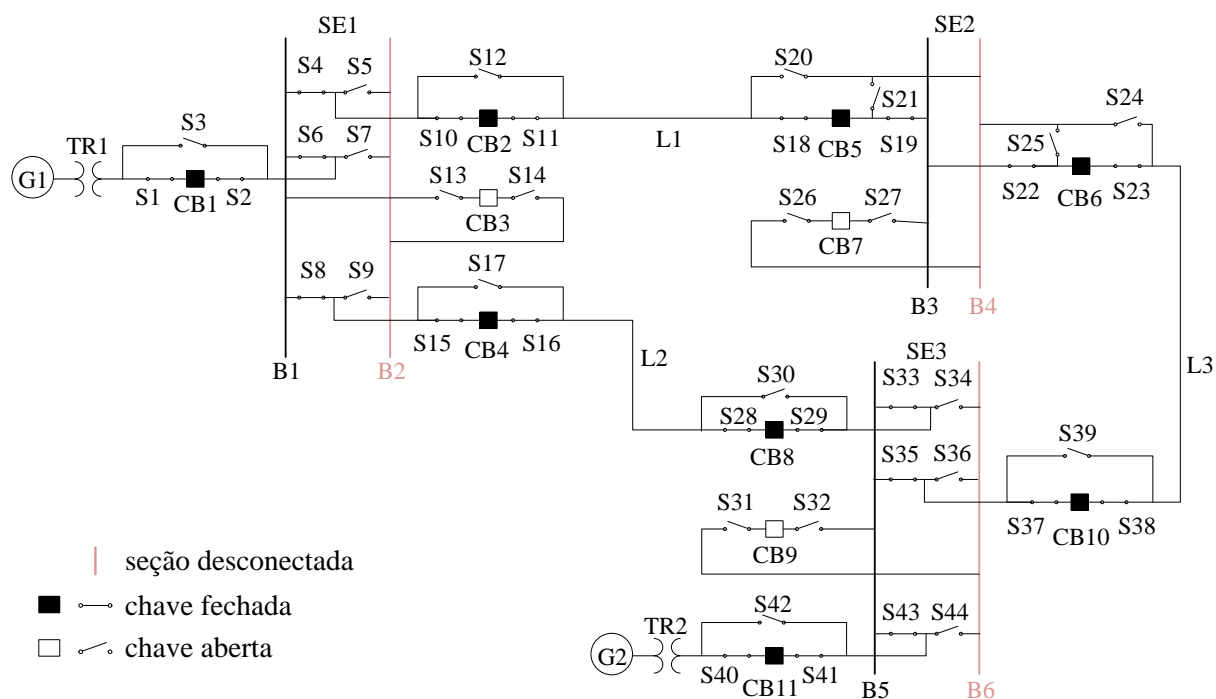
Evento	Seção	Alarme	Status	Classificação	Diagnóstico
1	L1	21-1	1	Falta	Falta em L1 e falha no disjuntor CB7
		CB1	1		
		CB2	1		
L2	21-2	1	Falta externa		
	CB9	1			
L3	21-3	1	Falta externa		
2	L1	21-1	0	Normal	Alarmes falsos: → CB9. Eventos falsos: → "Falta externa vista por L2"; → "Falta externa vista por L3".
		CB1	0		
		CB2	0		
3	L2	21-2	0	Normal	Evento falso: → "Falta externa vista por L3"
		CB9	0		

Note que o diagnóstico do primeiro evento foi preciso e sem inconsistência de alarmes. O evento 2 engloba os pontos do sistema modificados pela ação da função 79 da linha L1, enquanto o evento 3 engloba os pontos modificados pela ação da função 79 da linha L2. Em ambos os eventos, o diagnóstico é de operação normal sem falta.

5.3 Mapeamento dos eventos e identificação da topologia da rede

O sistema elétrico ilustrado na Figura 5.3 corresponde a uma pequena porção do SEP da CEEE-GT e é empregado para validar as funções do processador de alarmes inerentes ao mapeamento de eventos e à identificação topológica da rede. O sistema abrange 11 disjuntores (CB1-CB11), 44 chaves seccionadoras (S1-S44), duas unidades geradoras (G1-G2), dois transformadores (TR1-TR2), três linhas de transmissão (L1-L3) e seis barras (B1-B6). O grafo correspondente contém 13 vértices, 45 DSs (arestas), 55 dispositivos de chaveamento e 248 alarmes de relés. A estrutura de dados relativa ao sistema é apresentada no Apêndice A.

Figura 5.3 – Sistema teste 2



Considere a topologia da Figura 5.3 como sendo a topologia inicial dos testes. Com exceção de disjuntores e chaves, todos os relés estão ativos e em estado não operativo, ou seja, *status* igual à zero.

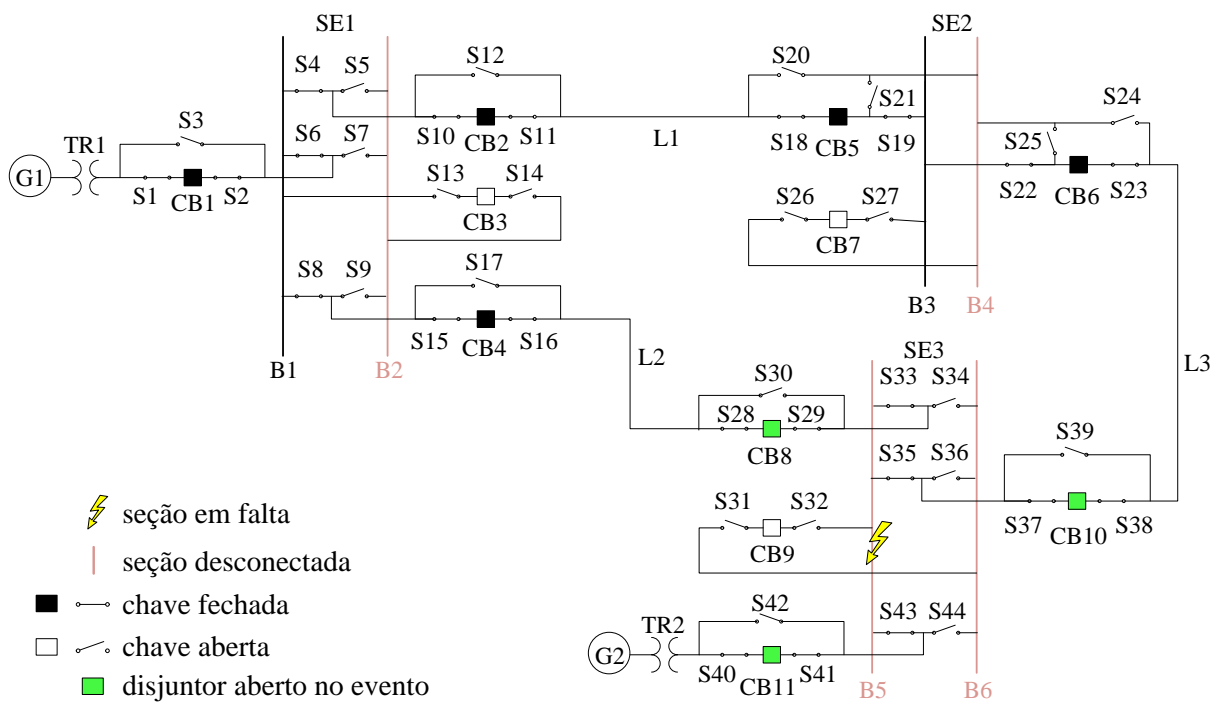
Abaixo seguem outras premissas adotadas nos testes:

- A notação <sigla da tabela><índice do elemento> é utilizado para representar os elementos de cada tabela da estrutura de dados. Por exemplo, o elemento 88 da tabela de alarmes é representado por TAL₈₈;
- Barras B2, B4 e B6 estão desenergizadas inicialmente, ou seja, *status* na tabela TEQ igual à zero;
- Não há registros na tabela TED;
- O método baseado no Teorema de Bayes é utilizado para a classificação de eventos nos estudos de caso 1 e 3.

5.3.1 Estudo de caso 1 – Falta na barra B5

O presente estudo de caso decorre de um erro humano, no qual o técnico esqueceu a haste de aterramento conectada à barra após uma manutenção de rotina. A operação nas três fases do relé diferencial 87 habilitou o relé de bloqueio 86, que por sua vez, realizou o *trip* dos disjuntores CB8, CB10 e CB11, conforme é mostrado na Figura 5.4.

Figura 5.4 – Topologia da rede após a falta na barra B5



Os dados de disparo dos disjuntores foram armazenados nas linhas 40, 49 e 55 da tabela TDC. A lista correspondente, $L = \{40, 49, 55\}$, é criada a fim de iniciar a rotina de verificação dos estados dos DSs (Figura 3.9). As linhas dos disjuntores em TDC são acessadas e o valor de *status* modificado para 0. O conjunto *EO* é montado a partir dos índices dos DSs armazenados no campo ‘Arestas’, ou seja, $EO = \{22, 24, 33, 35, 41, 43\}$. Dessa forma, os *status* destas arestas são atualizados para o estado aberto. Neste exemplo, o conjunto *EV* permanece vazio porque todos os disjuntores no conjunto *L* estão abertos.

Em termos de estrutura de dados, a abertura dos disjuntores causou o isolamento elétrico da barra B5 por meio das arestas TDS_{22} , TDS_{33} e TDS_{41} . Note que o transformador TR2 e o gerador G2 permanecem operando, mesmo que eletricamente isolados do resto do sistema. A Figura 5.5 mostra as mudanças na estrutura de dados ocorridas após o evento.

Figura 5.5 – Modificações na estrutura após caso 1

TEQ			
i de vi	Nomes	Arestas	status
10	B5	22 23 33 34 37 38 39 40 41 42	0
12	TR2	41 42 43 44 45	1
13	G2	45	1

TDS				
k de ek	v _i	v _j	Chaves	status
22	6	10	35 37 38 40	0
33	9	10	44 46 47 49	0
41	10	12	50 51 53 55	0

TAL			
h de ah	Nome	Vertice	status
245	B5 230kV-(87)-A-Trip	10	1
246	B5 230kV-(87)-B-Trip	10	1
247	B5 230kV-(87)-C-Trip	10	1
248	B5 230kV-(86)-Trip	10	1

TDC			
l de dl	Nome	Arestas	status
40	CB8	22 24	0
49	CB10	33 35	0
55	CB11	41 43	0

TED						
m de em	Seção	Alarmes {TAL}	CBs {TDC}	Evento	Tempo	Diagnóstico
1	B5	245 246 247 248	40 49 55	1	22:47:31	Falta

Os campos não modificados da Figura 5.5 foram omitidos para facilitar a leitura dos dados. Somente a barra B5 foi desconectada da rede em virtude do distúrbio e incluída na tabela TED para posterior análise. A instância utilizada para diagnóstico é formada pelos alarmes de relés e disjuntores reportados durante o evento. Evidentemente, o método ED1 não encontrou dificuldades e confirmou que a origem da falta está localizada na barra B5.

5.3.2 Estudo de caso 2 – Recomposição da subestação SE3

Após o diagnóstico da falta ocorrida no caso anterior, o operador, ou um sistema de auto-restabelecimento se disponível, é capaz de tomar as decisões necessárias para recompor a subestação SE3. A abertura das chaves S33, S36 e S43, juntamente com o fechamento das chaves S34, S36 e S44, permite a reconexão da unidade geradora G2 através da barra B6. O fechamento dos disjuntores CB8, CB10 e CB11 ativa as arestas TDS₂₄, TDS₃₅ e TDS₄₃.

O circuito equivalente e as modificações realizadas na estrutura de dados são apresentados na Figura 5.6

Figura 5.6 e na

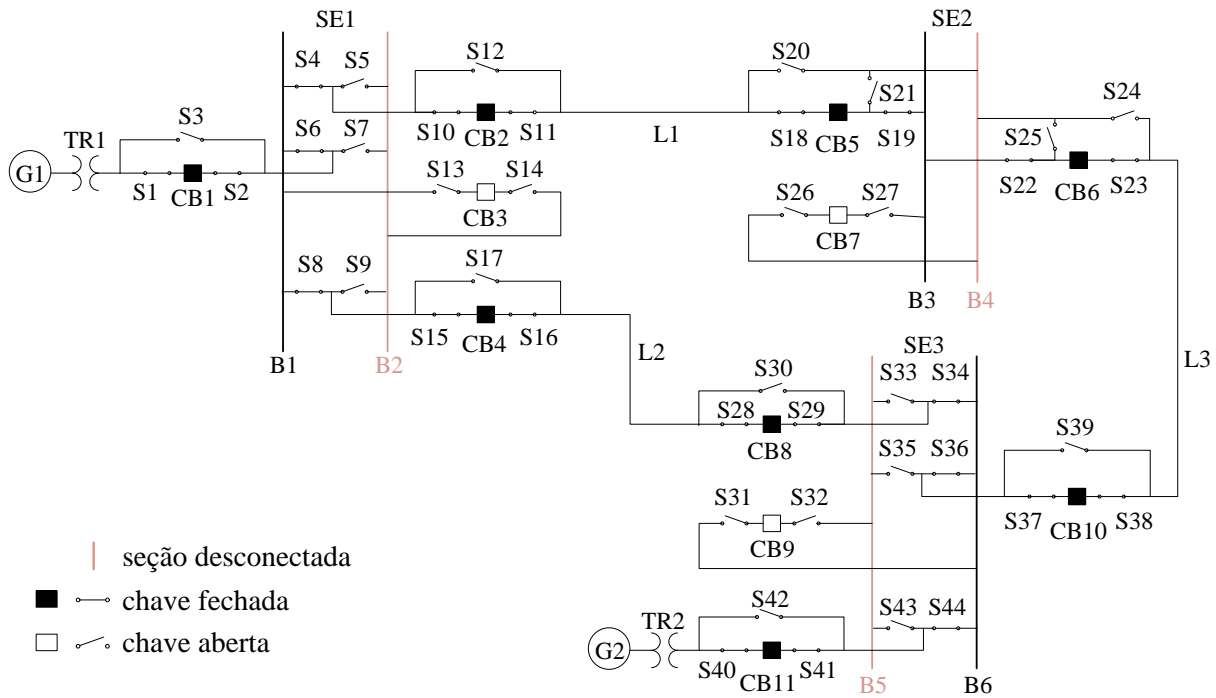


Figura 5.7, respectivamente. Durante esse ciclo, não houve desconexão de equipamentos, logo a tabela TED permanece inalterada.

Figura 5.6 – Topologia de rede após recomposição da SE3

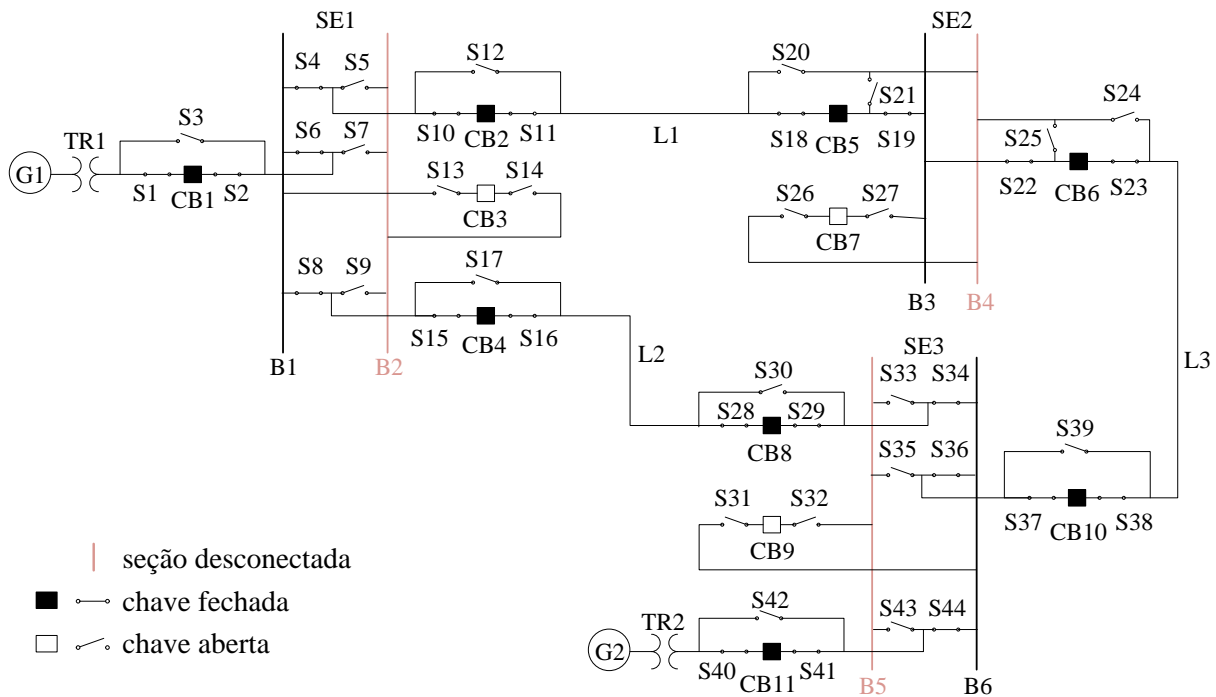


Figura 5.7 – Modificações na estrutura após caso 2

TEQ				TDC					
i de vi	Nome	Arestas		status	I de di	Nome	Arestas		status
11	B6	24 25 35 36 37 38 39 40 43 44		1	35	S33	22 23 37		0
					36	S34	24 25 37		1
					40	CB8	22 24		1
					44	S35	33 34 38		0
					45	S36	35 36 38		1
					49	CB10	33 35		1
					53	S43	40 41 42		0
					54	S44	40 43 44		1
					55	CB11	41 43		1

TDS					
k de ex	v _i	v _j	Chaves		status
24	6	11	36 37 38 40		1
35	9	11	45 46 47 49		1
43	11	12	50 51 54 55		1

5.3.3 Estudo de caso 3 – Falta temporária na linha L2

Esse caso compreende uma falta temporária monofásica na fase A da linha L2. A

Tabela 5.7 lista os alarmes reportados com respectivos instantes de tempo. A abertura dos disjuntores CB4 e CB8 causa a abertura dos dispositivos lógicos seccionadores TDS₁₂ e TDS₂₄, apesar das chaves que formam essas arestas permanecerem fechadas.

Tabela 5.7 – Alarmes reportados no caso 3

Hora	Índice	Descrição
09:03:03	TAL1	SE1 L2 230kV-(21)-Zone 1-A-Trip
09:03:03	TAL88	SE3 L2 230kV-(21)-Zone1-A-Trip
09:03:05	TSD4	CB4 (abertura)
09:03:05	TSD40	CB8 (abertura)
09:03:33	TAL101	SE1 L2 230kV-Recloser(79)-Trip
09:03:33	TAL102	SE L2 230kV-Recloser(79)-Trip
09:03:34	TSD4	CB4 (fechamento)
09:03:34	TSD40	CB8 (fechamento)

Neste caso foram identificados dois eventos durante a etapa de mapeamento de eventos. O primeiro evento contém os alarmes disparados antes do sinal de religamento automático da linha L2, enquanto o segundo evento contém os alarmes subsequentes. Como não há seções desconectadas no segundo evento, este evento é classificado como normal. A

topologia e a estrutura de dados pós-falta são mostrados na Figura 5.8 e na Figura 5.9, respectivamente.

Figura 5.8 – Topologia pós-falta na linha L2

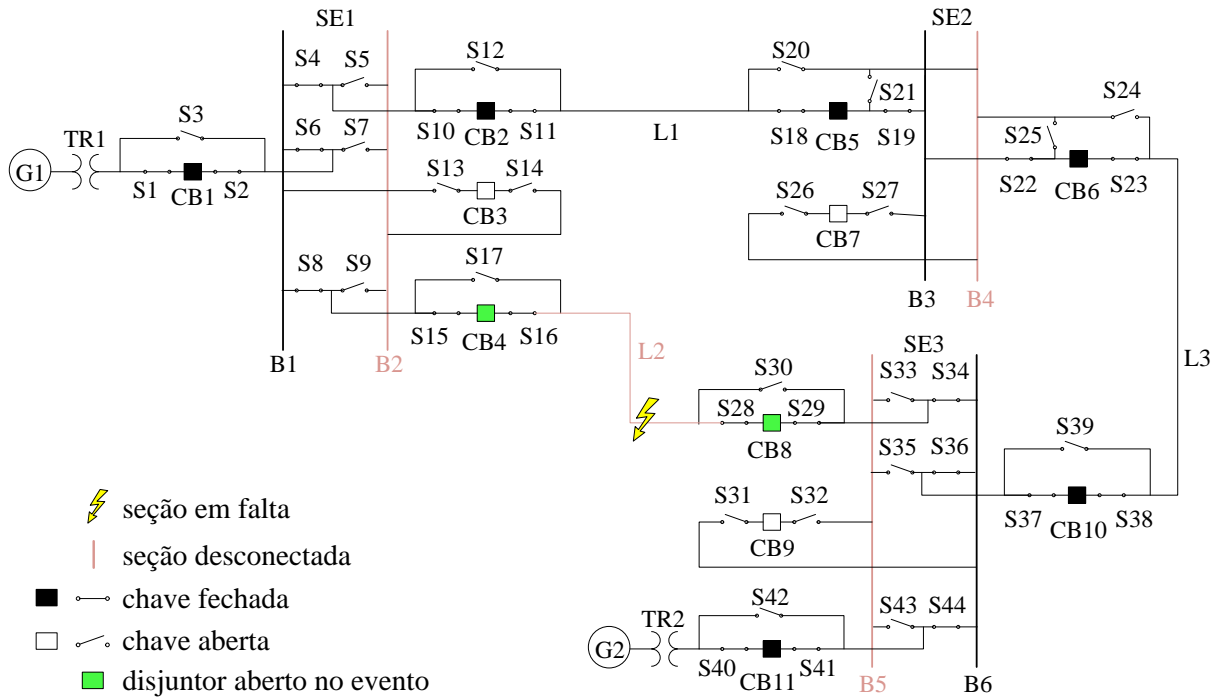


Figura 5.9 – Modificações na estrutura pós-falta do caso 3

TEQ			
i de v _i	Nome	Arestas	status
6	L2	12 13 16 17 22 23 24 25	0

TDS				
k de ex	v _i	v _j	Chaves	status
12	3	6	16 18 19 21	0
24	6	11	36 37 38 40	0

TAL			
h de an	Nome	Vertice	status
1	SS1 L2 230kV-(21)-Zone1-A-Trip	6	1
88	SS3 L2 230kV-(21)-Zone1-A-Trip	6	1
101	SS1 L2 230kV-Recloser(79)-Trip	6	1
102	SS3 L2 230kV-Recloser(79)-Trip	6	1

TDC			
l de di	Nome	Arestas	status
21	CB4	12 16	0
40	CB8	22 24	0

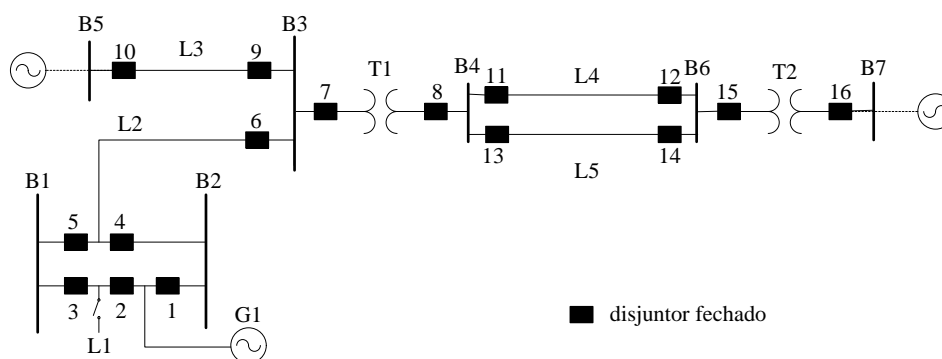
TED						
m de em	Seção	Alarmes {TAL}	CBs {TDC}	Evento	Tempo	Diagnóstico
2	L2	1 88	4 40	2	09:03:03	Falta

No evento 1, a linha L2 está desenergizada e pertence a lista de suspeitos, logo o seu vértice é movido para a tabela TED. A instância analisada na classificação do evento é formada pelos sinais de *trip* dos relés de distância e de abertura dos disjuntores. Tanto o diagnóstico em nível local, quanto em nível de sistema estimaram L2 como seção em falta.

5.4 Geração de padrões de eventos

O sistema de potência mostrado na Figura 5.10 é utilizado para validar o algoritmo proposto para geração de padrões de funcionamento da proteção em nível de sistema.

Figura 5.10 – Sistema teste 3



O sistema considerado é composto de 15 equipamentos: um gerador (G1), sete barras (B1-B7), um terminal de linha (L1), quatro linhas de transmissão (L2-L5) e um transformador T1. O sistema de proteção é composto de 16 disjuntores (CB1-CB16) e dos esquemas de proteção apresentados na seção 3.7.1 deste trabalho. A Tabela 5.8 apresenta os dados de entrada necessários para execução do algoritmo de geração de padrões.

Tabela 5.8 – Dados das arestas do grafo referente ao sistema teste 3

Dispositivo lógico seccionador j	Equipamentos conectados pelo DS j (V_j)	Disjuntores do DS j (B_j)
DS1	G1 e B1	CB2 e CB3
DS2	G1 e B2	CB1
DS3	G1 e L1-terminal	CB2
DS4	B1 e B2	CB1, CB2 e CB3
DS5	B1 e B2	CB4 e CB5
DS6	B1 e L1-terminal	CB3

Dispositivo lógico seccionador j	Equipamentos conectados pelo DS j (V_j)	Disjuntores do DS j (B_j)
DS7	B1 e L2	CB5
DS8	B2 e L1-terminal	CB1 e CB2
DS9	B2 e L2	CB4
DS10	B3 e L2	CB6
DS11	B3 e T1	CB7
DS12	T1 e B4	CB8
DS13	B3 e L3	CB9
DS14	B5 e L3	CB10
DS15	B4 e L4	CB11
DS16	B4 e L5	CB13
DS17	L4 e B6	CB12
DS18	L5 e B6	CB14
DS19	B6 e T2	CB15
DS20	T2 e B7	CB16

O sistema teste 3 é mais complexo em relação ao exemplo numérico apresentado na seção 3.7.2.6, e apresenta resultados utilizando todas as rotinas desenvolvidas no gerador de padrões. Esse sistema se diferencia por conter um gerador, transformadores, linhas em paralelo, arranjo de barras disjuntor e meio, e terminal de linha desenergizada protegida pela função *stub bus*. A Tabela 5.9 descreve os padrões de funcionamento da proteção.

Tabela 5.9 – Padrões de eventos gerados

Padrão	Seção em falta	CB falho	Disjuntores abertos	Eventos esperados
1	G1	[]	CB1 CB2	G1FI L2FD→B1
2	B1	[]	CB3 CB5	B1FI L2FD→B1
3	B2	[]	CB1 CB4	B2FI L2FD→B1
4	B7	[]	CB16	B7FI
5	B3	[]	CB6 CB7 CB9	B3FI L2FD→B3 L3FD→B3
6	L2	[]	CB4 CB5 CB6	L2FI L3FD→B3

Padrão	Seção em falta	CB falho	Disjuntores abertos	Eventos esperados
7	T1	[]	CB7 CB8	L2FD→B3 T1FI L3FD→B3 L4FD→B4 L5FD→B4
8	B4	[]	CB8 CB11 CB13	B4FI L4FD→B4 L5FD→B4
9	B5	[]	CB10	B5FI L3FD→B5
10	L3	[]	CB9 CB10	L2FD→B3 L3FI
11	L4	[]	CB11 CB12	L4FI
12	L5	[]	CB13 CB14	L5FI
13	B6	[]	CB12 CB14 CB15	L4FD→B6 L5FD→B6 B6FI
14	T2	[]	CB15 CB16	L4FD→B6 L5FD→B6 T2FI
15	L1-term	[]	CB2 CB3	L1FI L2FD→B1
16	G1	CB1	CB2 CB6	G1FI L2FD→B1
17	G1	CB2	CB1 CB6	G1FI L2FD→B1
18	B1	CB3	CB1 CB2 CB5 CB6	G1FE B1FI L2FD→B1
19	B1	CB5	CB1 CB2 CB3 CB6	G1FE B1FI L2FD→B1
20	B2	CB1	CB2 CB4 CB6	G1FE B2FI L2FD→B1
21	B2	CB4	CB1 CB2 CB6	G1FE B2FI L2FD→B1
22	B7	CB16	CB15	B7FI T2FD→B7
23	B3	CB6	CB4 CB5 CB7 CB9	B3FI L2FD→B3 L3FD→B3
24	B3	CB7	CB6 CB8 CB9	B3FI L2FD→B3 T1FD→B3 L3FD→B3
25	B3	CB9	CB6 CB7 CB10	B3FI L2FD→B3 L3FD→B3
26	L2	CB4	CB1 CB2 CB5 CB6	G1FE L2FI L3FD→B3
27	L2	CB5	CB1 CB2 CB4 CB6	G1FE L2FI L3FD→B3
28	L2	CB6	CB4 CB5 CB7 CB10	L2FI T1FD→B3 L3FD→B3
29	T1	CB7	CB4 CB5 CB8 CB10	L2FD→B3 T1FI L3FD→B3 L4FD→B4 L5FD→B4
30	T1	CB8	CB7 CB12 CB14	L2FD→B3 T1FI L3FD→B3 L4FD→B4 L5FD→B4
31	B4	CB8	CB7 CB11 CB13	T1FD→B4 B4FI L4FD→B4 L5FD→B4
32	B4	CB11	CB8 CB12 CB13	B4FI L4FD→B4 L5FD→B4

Padrão	Seção em falta	CB falho	Disjuntores abertos	Eventos esperados
33	B4	CB13	CB8 CB11 CB14	B4FI L4FD→B4 L5FD→B4
34	B5	CB10	CB9	B5FI L3FD→B5
35	L3	CB9	CB4 CB5 CB7 CB10	L2FD→B3 T1FD→B3 L3FI
36	L3	CB10	CB9	L2FD→B3 L3FI
37	L4	CB11	CB8 CB12 CB14	T1FD→B4 L4FI L5FD→B4
38	L4	CB12	CB11 CB13 CB15	L4FI T2FD→B6 L5FD→B6
39	L5	CB13	CB8 CB12 CB14	T1FD→B4 L4FD→B4 L5FI
40	L5	CB14	CB11 CB13 CB15	L4FD→B6 L5FI T2FD→B6
41	B6	CB12	CB11 CB14 CB15	L4FD→B6 L5FD→B6 B6FI
42	B6	CB14	CB12 CB13 CB15	L4FD→B6 L5FD→B6 B6FI
43	B6	CB15	CB12 CB14 CB16	L4FD→B6 L5FD→B6 B6FI T2FD→B6
44	T2	CB15	CB11 CB13 CB16	L4FD→B6 L5FD→B6 T2FI
45	T2	CB16	CB15	L4FD→B6 L5FD→B6 T2FI
46	L1-term	CB2	CB1 CB3 CB4	B2FE G1FE L1FI L2FD→B1
47	L1-term	CB3	CB1 CB5	B1FE L1FI L2FD→B1
48	G1	CB1	CB2 CB4	G1FI B2FE L2FD→B1
49	G1	CB2	CB1 CB3 CB5	G1FI B1FE L2FD→B1
50	L2	CB4	CB1 CB5 CB6	B2FE L2FI L3FD→B3
51	L2	CB5	CB3 CB4 CB6	B1FE L2FI L3FD→B3
52	L2	CB6	CB4 CB5 CB7 CB9	B3FE L2FI L3FD→B3
53	T1	CB7	CB6 CB8 CB9	B3FE L2FD→B3 T1FI L3FD→B3 L4FD→B4 L5FD→B4
54	T1	CB8	CB7 CB11 CB13	L2FD→B3 T1FI B4FE L3FD→B3 L4FD→B4 L5FD→B4
55	L3	CB9	CB6 CB7 CB10	B3FE L2FD→B3 L3FI
56	L3	CB10	CB9	L2FD→B3 B5FE L3FI
57	L4	CB11	CB8 CB12 CB13	B4FE L4FI
58	L4	CB12	CB11 CB14 CB15	L4FI B6FE
59	L5	CB13	CB8 CB11 CB14	B4FE L5FI
60	L5	CB14	CB12 CB13 CB15	L5FI B6FE

Padrão	Seção em falta	CB falho	Disjuntores abertos	Eventos esperados
61	T2	CB15	CB12 CB14 CB16	L4FD→B6 L5FD→B6 B6FE T2FI
62	T2	CB16	CB15	B7FE L4FD→B6 L5FD→B6 T2F
63	L1-term	CB2	CB1 CB3 CB6	G1FE L1FI L2FD→B1
64	L1-term	CB3	CB1 CB2 CB6	G1FE L1FI L2FD→B1

Códigos: FI é sigla de falta interna; FE é falta externa; FD→B1 é falta na direção da barra B1; FD→B2 é falta na direção da barra B2; FD→B3 é falta na direção da barra B3; FD→B4 é falta na direção da barra B4; FD→B5 é falta na direção da barra B5; FD→B6 é falta na direção da barra B6; e FD→B7 é falta na direção da barra B7.

Os padrões gerados são combinações lógicas de 52 sinais lógicos, sendo 16 alarmes de disjuntores (CB1-CB16) e 35 eventos. Dentre os eventos, foram considerados 15 classificações de falta interna, 8 classificações de falta externa e 12 classificações de faltas externas com direção. Cada equipamento possui um evento caracterizado como “operação normal” que não é utilizado nos padrões da proteção.

Com esses dados, foram gerados 64 padrões de funcionamento da proteção, sendo 15 padrões associados à atuação da proteção principal, 32 padrões associados à atuação da proteção de retaguarda remota e 17 padrões associados à operação da proteção de retaguarda local.

O conjunto de padrões no intervalo 1-15 corresponde à operação esperada da proteção principal com sucesso na abertura de todos os disjuntores que devem receber *trip*. Os demais padrões consideram a operação conjunta da proteção principal e de retaguarda em decorrência da falha na abertura de um disjuntor (coluna disjuntor falho). O conjunto de padrões no intervalo 16-47 representam as possibilidades de operação da proteção de retaguarda remota, enquanto o intervalo 48-64 representa as possibilidades de operação da retaguarda local.

Os padrões são gerados após uma mudança topológica da rede e utilizados como “guia” dos modelos de programação matemática para diagnóstico de faltas. O tempo de processamento total da rotina para o sistema teste 3 é desprezível, na ordem dos milissegundos.

5.5 Considerações finais

Este capítulo apresentou os resultados experimentais oriundos da aplicação do processador de alarmes proposto. A metodologia de testes englobou três tipos de testes

computacionais: no primeiro, é avaliado o impacto no diagnóstico a partir de uma determinada ordem cronológica de alarmes; no segundo é analisado o mapeamento de eventos de acordo com mudanças topológicas; e por último, são mostrados os padrões de funcionamento da proteção gerados para um pequeno sistema teste.

O primeiro teste confirmou que, de fato, existe uma relação entre a ordem de recebimentos dos alarmes e a exatidão de um diagnóstico, que justifica o uso de lógicas adicionais para a reordenação cronológica de alarmes. O segundo teste permitiu averiguar que o mapeamento de eventos é fundamental para a aplicação de metodologias de diagnóstico divididas em duas etapas.

O terceiro teste mostra que o algoritmo de geração de padrões consegue encontrar um conjunto de padrões suficiente para a aplicação de métodos de diagnóstico, tendo como base os requisitos técnicos de proteção estabelecidos pelo ONS. O algoritmo de geração de padrões é uma forma viável para facilitar a implantação de técnicas de diagnóstico em sistemas reais, uma vez que a rotina reconhece as funções de proteção de acordo com a topologia da rede e gera os eventos em intervalos de tempo desprezíveis.

6 RESULTADOS DE MÉTODOS DE DIAGNÓSTICO E DISCUSSÕES

6.1 Considerações gerais

Este capítulo apresenta os resultados experimentais dos métodos propostos para diagnósticos de faltas. Os métodos foram implementados no *software* Matlab[®], e os modelos de programação matemática foram resolvidos utilizando o *solver* comercial CPLEX 12.4 com configurações *default*. O computador utilizado é um Intel Core i7-2600, 3.4 GHz, 8 GB RAM e sistema operacional Windows 7 de 64 bits. Os testes computacionais foram divididos em quatro tipos de experimentos:

- Análise dos métodos HC+BIP e ED1, considerando padrões com e sem eventos “não falta”;
- Análise comparativa de métodos de diagnóstico divididos em dois níveis, considerando instâncias com inserção de bits aleatórios;
- Análise comparativa de métodos de diagnóstico em um sistema de transmissão radial e malhado;
- Análise comparativa dos modelos de programação matemática em um sistema de potência de grande porte.

Os dados dos padrões de funcionamento da proteção de cada sistema teste estão disponibilizados no endereço <https://github.com/aceiooliveira/tese>. O sistema proposto por Wen e Han (1995) e o sistema da AES-Sul possuem arquivos que relacionam alarmes, eventos e diagnósticos. Os sistemas da Eletrosul e da CEEE-GT contém arquivos que relacionam alarmes, regras da proteção, eventos e diagnósticos.

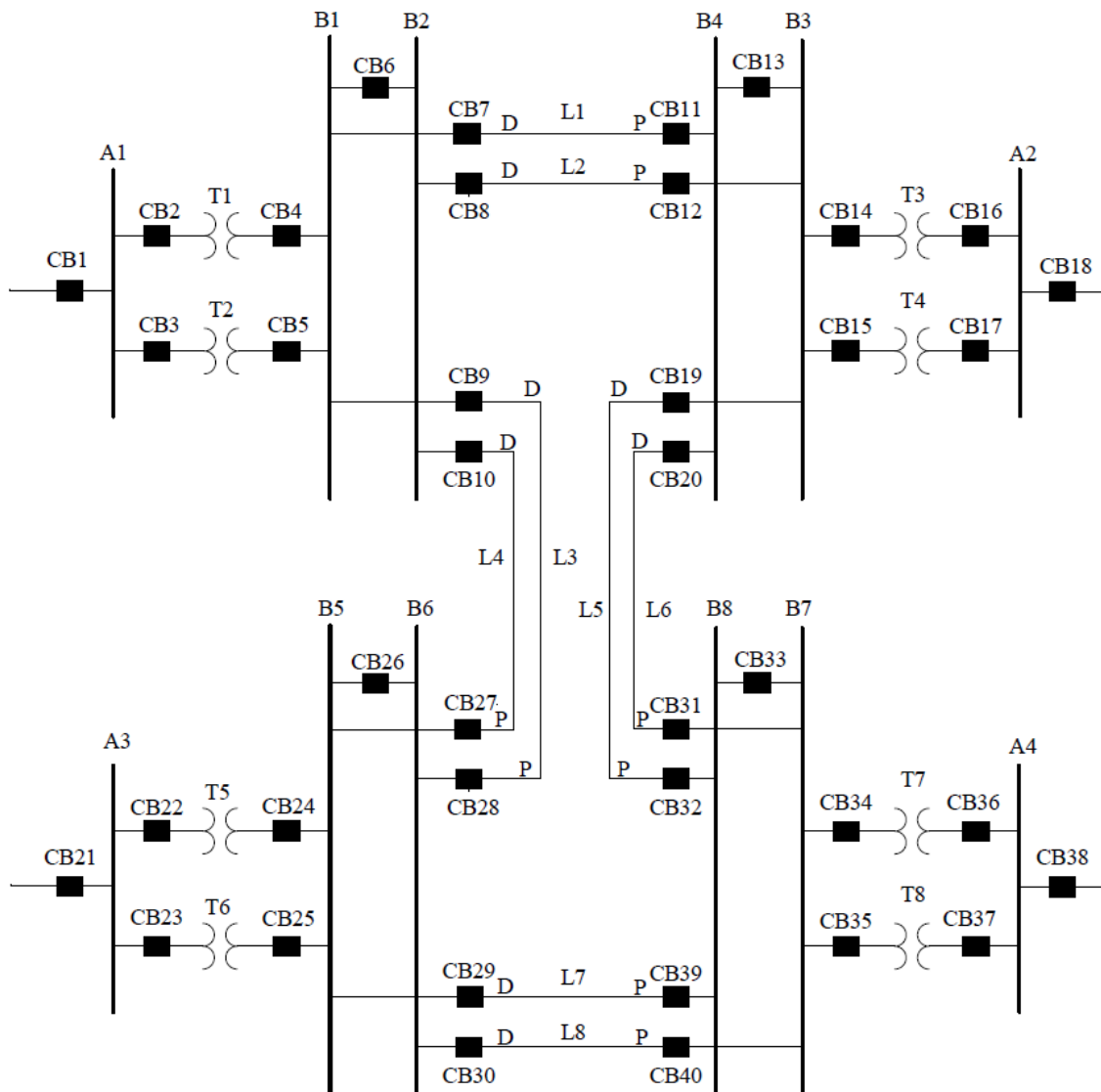
6.2 Efeito no diagnóstico do uso de padrões contendo eventos “não falta”

O objetivo deste teste é avaliar o impacto gerado no diagnóstico pelo uso de padrões que contenham, ou não, eventos de “não falta” (“normal”). Esse evento denota que o equipamento não está em falta apesar dos alarmes reportados. Os métodos HC+BIP e ED1 são considerados nos testes por serem baseados na metodologia de diagnóstico em dois níveis.

O SEP apresentado por Wen e Han (1995) é utilizado para realizar os estudos comparativos. O diagrama unifilar do sistema é mostrado na Figura 6.1 e é composto de 28

seções e 40 disjuntores. Os padrões e instâncias apresentados por Fritzen et al. (2012) são considerados no estudo e consideram eventos “não falta” em todo e qualquer equipamento do SEP não afetado pela falta. O uso desses eventos implica em maior tempo de processamento, uma vez que todos os equipamentos do sistema devem ser analisados para cada novo conjunto de alarmes reportados.

Figura 6.1 – Sistema teste proposto por Wen e Han (1995)



Os resultados mostram que o método ED1 obteve os mesmos diagnósticos utilizando padrões com ou sem eventos “não falta”. Por outro lado, a resolução por meio do modelo BIP modificou a solução em 20% dos casos testados após a retirada de eventos “não falta” dos padrões. A Tabela 6.1 mostra as instâncias cujas soluções foram modificadas.

Tabela 6.1 – Instâncias de Fritzen et al. (2012) sem alarmes “não falta”

#	Diagnóstico	Alarmes	Eventos
5	Falta em T1 T2NF falho	CB2 CB4	L1FD L2FD L3FD L4FD T1F
12	Falta em B1 L3FP falso L4FP falso	CB4 CB5 CB6 CB7 CB9	B1F L1FD T1FP L2FD L3FD L4FD L3FP L4FP T2FP
15	Falta em T1 Falta em A1 Falta em B1 CB1 falho CB7 falho	CB2 CB3 CB4 CB5 CB6 CB7 CB9 CB11	L1FD L2FD L3FD L4FD T1FP T1F L1F B1F T2FP T3FD T4FD T1FP T2FP T1FD T2FD

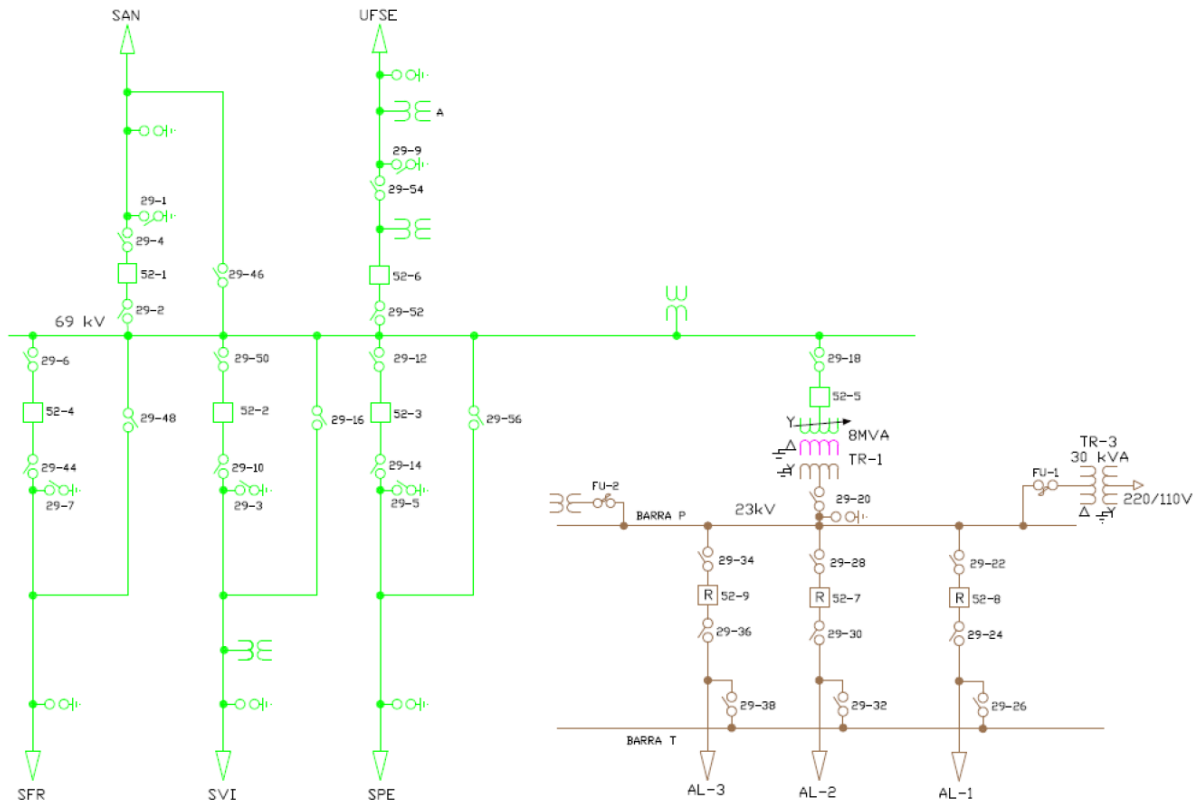
Códigos: FD é sigla de “falta no lado D”, FP é sigla de “falta no lado P”, F é sigla de “falta interna” e NF é sigla de “não-falta”.

O teste 12 é o caso que melhor exemplifica a queda de desempenho do método de Fritzen et al. (2012) , cuja solução original estimou a barra B1 em falta e identificou dois eventos indevidos: falta no lado “P” da linha L3 (L3FP) e falta no lado “P” da linha (L4FP). A nova solução encontrada pelo modelo BIP é formada por dois eventos simultâneos: faltas em B1 e em T6. Além disso, cinco alarmes foram identificados como falhos (CB23, CB25, L7FD, L8FD e T6F). Em termos de velocidade de processamento, a retirada destes eventos dos padrões acelera o diagnóstico em ambos os métodos.

6.3 Análise dos métodos de dois níveis

Para este estudo comparativo são utilizados dados reais da subestação JAG 179 69/23 kV da AES-Sul (Distribuidora Gaúcha de Energia S.A.), localizada no Município de Jaguari/RS. A Figura 6.2 mostra o diagrama unifilar da SE JAG 179.

Figura 6.2 – Diagrama unifilar da SE JAG 179



Fonte: Toller (2011).

O sistema possui 10 equipamentos, sendo cinco linhas, uma barra, um transformador e 3 alimentadores. A barra de 23 kV não é considerada na análise, pois não possui esquema de proteção próprio. A SE possui duas fontes de energia: a fonte principal é proveniente da LT SVI, conectada com a SE abaixadora 230/69 kV de propriedade da CEEE (Companhia Estadual de Energia Elétrica); a fonte secundária é proveniente da LT UFSE, conectada a usina hidroelétrica de Furnas do Segredo. O levantamento dos dados e estudo da lógica da operação da proteção da SE JAG 179 foi realizada por Toller (2011).

6.3.1 Metodologia de testes

A metodologia de testes abrange um conjunto de instâncias geradas a partir dos padrões da proteção e da inserção de ruídos aleatórios. Para cada diagnóstico, são criadas 200 amostras aleatórias com ruídos, sendo 100 instâncias com 1 alarme aleatório e 100 instâncias com 2 alarmes aleatórios. O total de instâncias geradas é igual a $(200 \text{ amostras} \cdot 100 \text{ diagnósticos}) = 20.000$ instâncias.

Considere que cada diagnóstico i é formado por ne_i eventos e cada evento j é composto na_j alarmes. O ruído no diagnóstico i decorrente da inserção de alarmes aleatórios ($ruído_i$) é calculado da seguinte forma:

$$ruído_i = \left\{ \sum_{s=1}^{ns} \frac{bit \cdot ne_i}{\max(\sum_{j=1}^{ne_i} \sum_{k=1}^{na_j} a_k^s, na_{diag})} \right\} \div ns \tag{6.1}$$

em que,

- bit é o número de alarmes aleatórios inseridos em cada amostra j ;
- a_k^s é o estado do alarme k na instância s (1, reportado; 0, não reportado);
- na_{diag} é o número de alarmes do diagnóstico-padrão;
- ns é o número de instâncias geradas aleatoriamente;
- \max é uma função que escolhe o valor do maior argumento.

Os diagnósticos foram divididos em quatro grupos com base no número de eventos que caracteriza cada diagnóstico. No total, 6800 diagnósticos contém 1 evento apenas, 8000 diagnósticos possuem 2 eventos, 2000 diagnósticos possuem 3 eventos e 3200 diagnósticos possuem 4 eventos. Os ruídos amostrais médios gerados pela inserção de 1 ou 2 alarmes aleatórios são mostrados na Figura 6.3 e na Figura 6.4, respectivamente.

Figura 6.3 – Ruído amostral médio após inserção de 1 alarme aleatório

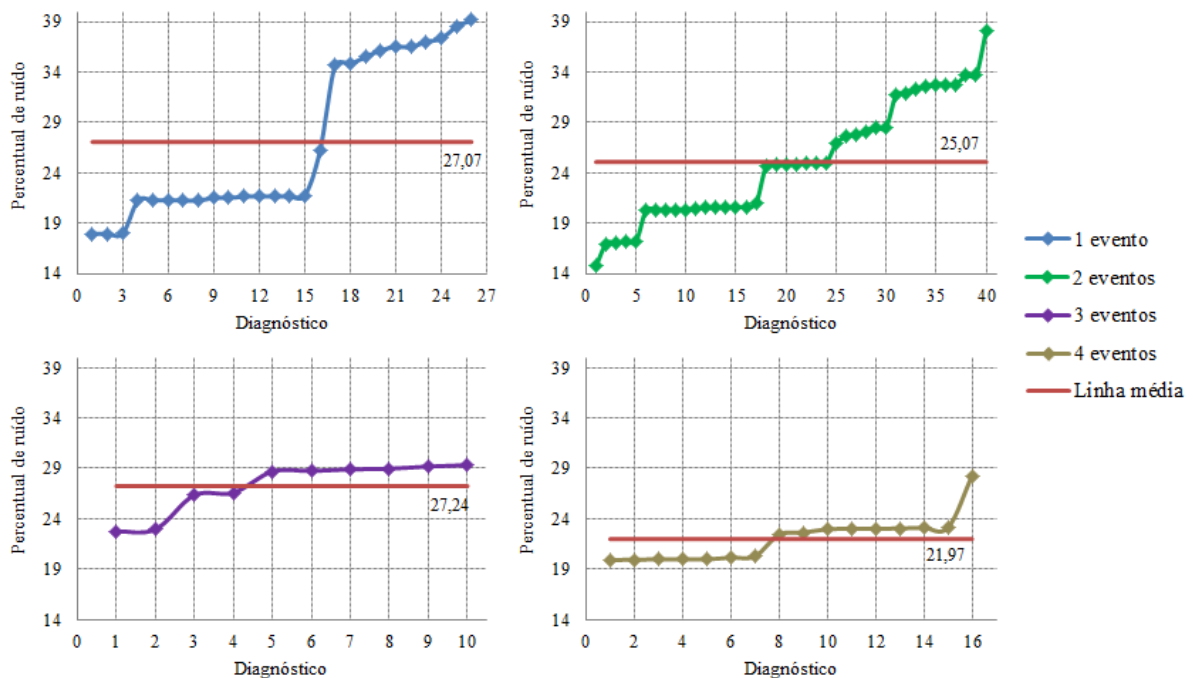
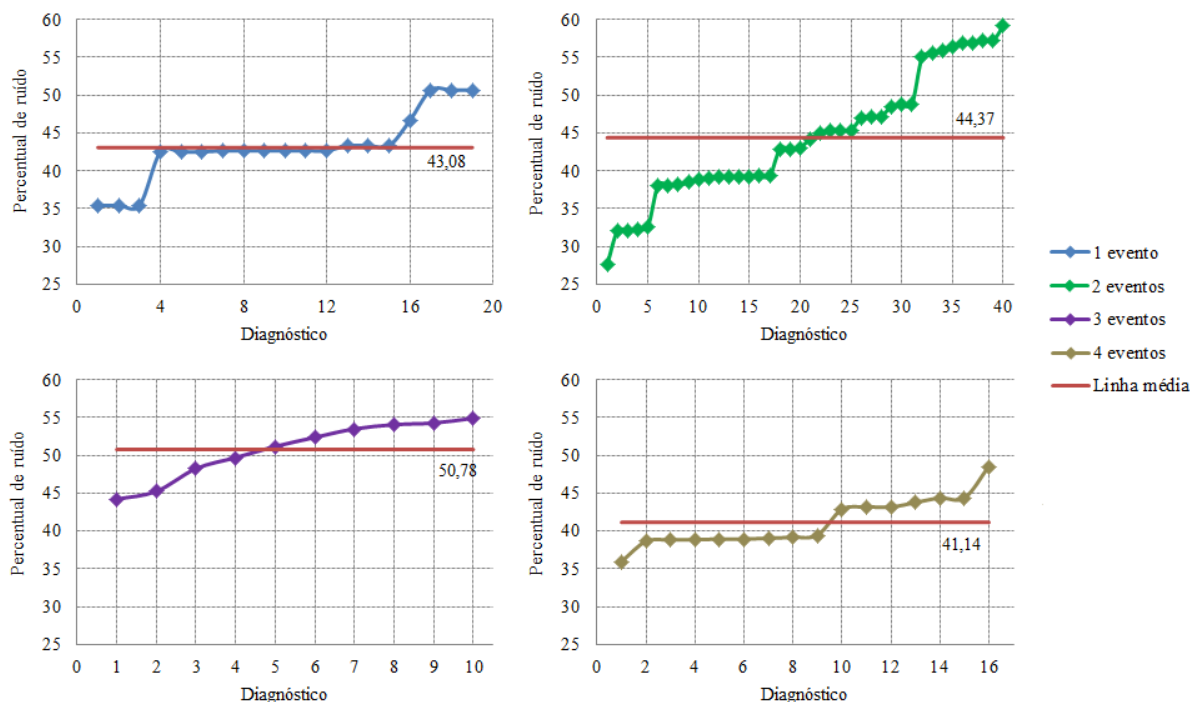


Figura 6.4 – Ruído amostral médio após inserção de 2 alarmes aleatórios



Dos 200 grupos de instâncias, 27 grupos foram desconsiderados dos testes computacionais devido ao ruído ser maior que a informação, sendo 8 grupos de instâncias gerados com um alarme de ruído, e 15 grupos de instâncias gerados com dois alarmes de ruídos. No total, foram consideradas 17.300 instâncias nas simulações. As instâncias geradas a partir da inserção de um alarme aleatório apresenta um ruído médio de 25,33%, enquanto as instâncias geradas a partir da inserção de dois alarmes aleatórios apresenta um ruído médio de 44,23%. Observe que as instâncias que sofrem maior ruído são aquelas cujos eventos associados possuem o menor número de alarmes.

Com as instâncias geradas, pretende-se avaliar o desempenho de métodos de diagnóstico em dois níveis. Os métodos considerados nos testes comparativos são:

- Método GRNN+AG: rede GRNN empregada por Cardoso Jr., Rolim e Zurn (2004) combinada com AG empregado por Wen e Han (1995);
- Método HC+BIP proposto por Fritzen et al. (2012);
- Métodos ED1 e AED propostos neste trabalho.

Os métodos IA, proposto por Leão, Pereira e Mantovani (2010), método AD e método ED2 não são considerados nas simulações por não serem compatíveis com os dados do sistema. Além disso, foi considerado um quinto método que incorpora o modelo de

programação matemática relativo ao problema de otimização resolvido com um AG em Wen e Han (1995). Uma vez que esse modelo é resolvido na otimalidade, é de se esperar que os resultados sejam melhores ou iguais àqueles obtidos com o AG. Desta forma, será possível avaliar se a metodologia proposta por Wen e Han (1995) condiz com o problema real. O modelo deste método, chamado de MAG, é semelhante ao modelo BIP proposto por Frizen et al. (2012), distinguindo-se apenas em relação ao número de pesos adotados na FO: no modelo MAG há um ajuste para alarmes falsos e falhos, enquanto no modelo BIP há um ajuste específico para cada tipo de alarme.

Os parâmetros dos métodos utilizados nos testes são os seguintes:

- GRNN: número de neurônios da camada padrão é igual ao número de alarmes do equipamento; número de neurônios da camada linear é igual ao número de eventos do equipamento; $spread = 0,40$;
- HC: não possui parâmetros;
- Bayes: $pc = 0,82$; $pi = 0,12$; $pf = 0,06$;
- AG: $w_1 = 1000$; $w_2 = 3$; $w_3 = 2$; $P_c = 0,9$; $P_m = 0,001$; $n = 1000$; $nse = 25$;
- MAG: $w_1 = 3$; $w_2 = 2$;
- BIP: $w_1 = 3$; $w_2 = 3$; $w_3 = 1$;
- ED1: $w_1 = 6$; $w_2 = 3$; $w_3 = 1$;
- AED: $w_1 = 9$; $w_2 = 9$; $w_3 = 3$; $w_4 = 3$; $w_5 = 3$; $w_6 = 1$; $w_7 = 0,5$.

O percentual total de acertos dos métodos é igual à média do percentual de acertos obtidos nos grupos de diagnóstico. O percentual de acertos dos grupos de diagnósticos é igual à média do percentual de acertos de cada instância com ruído. O percentual de diagnósticos corretos é utilizado para avaliar os métodos em nível de sistema, enquanto o percentual de eventos corretos é utilizado para avaliar os métodos em nível de equipamento.

6.3.2 Resultados obtidos

Os percentuais médios de acerto dos métodos em nível de equipamento (local) após inserção de um e dois alarmes aleatórios são mostrados na Figura 6.5 e na Figura 6.6, respectivamente. A linha média representa o percentual global de acertos dos métodos, enquanto as colunas representam a média percentual de acertos por grupo de diagnósticos. Observe que os resultados da GRNN são utilizados para alimentar os métodos AG e MAG.

Figura 6.5 – Desempenho de métodos com erro em 1 alarme em nível local

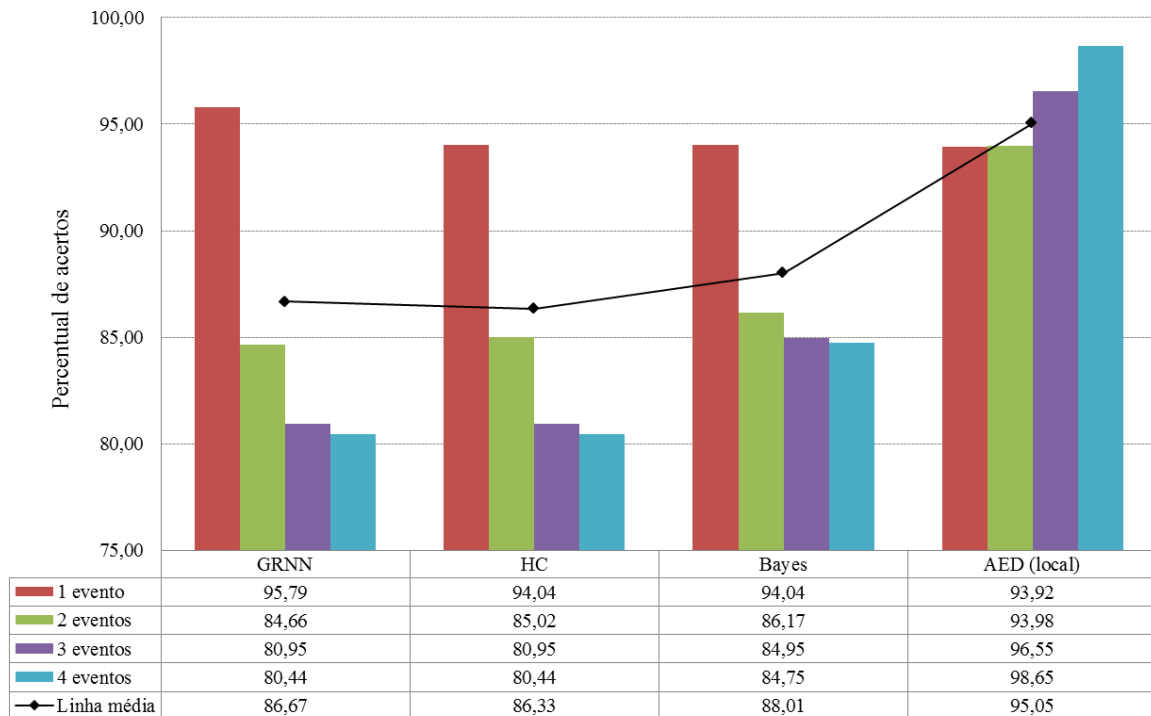
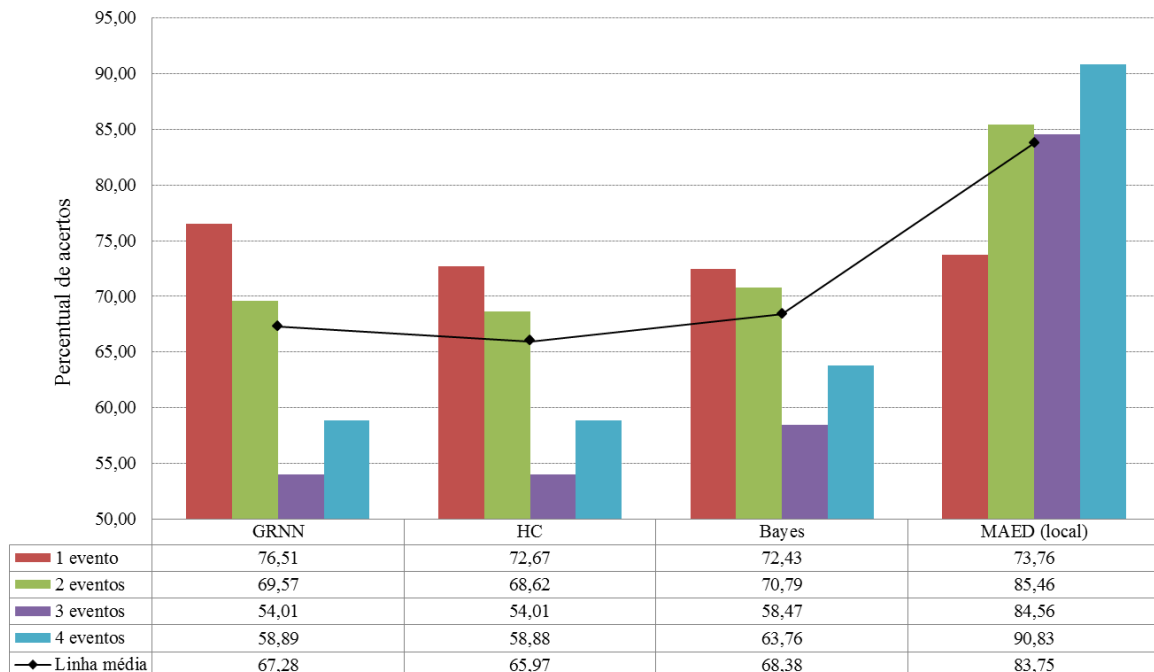


Figura 6.6 – Desempenho de métodos com erro em 2 alarmes em nível local



Os resultados em nível de equipamento mostram que o método AED consegue acertar 8,00% e 22,47% mais eventos que o segundo melhor, a heurística baseada no teorema de Bayes, nos testes envolvendo instâncias com um e dois alarmes aleatórios, respectivamente. Esse ganho de desempenho se deve, principalmente, ao fato de que o modelo AED é o único que avalia os alarmes reportados juntamente com os eventos que compõem um diagnóstico.

O método AED apresenta desempenho superior aos demais em todos os grupos de instâncias, exceto o grupo de instâncias com apenas um evento. O desempenho inferior (2% e 3,7% em relação à GRNN) está associado ao fato da instância ser extremamente pequena. Por critério de decisão, o método AED opta por considerar muitas dessas instâncias como alarmes falsos, dada a incapacidade do método em escolher um ou outro evento.

Outro detalhe que deve chamar a atenção do leitor é a capacidade do modelo do método AED em melhorar o desempenho de acertos conforme aumenta a complexidade da instância analisada, em sentido oposto ao que ocorrem nos demais métodos. Esse resultado sugere que o método AED é o mais viável para ser aplicado em SEPs de grande porte.

Os percentuais médios de acerto dos métodos em nível de sistema após inserção de um e dois alarmes aleatórios é mostrado na Figura 6.7 e na Figura 6.8, respectivamente.

Figura 6.7 – Desempenho de métodos com 1 alarme de ruído em nível de sistema

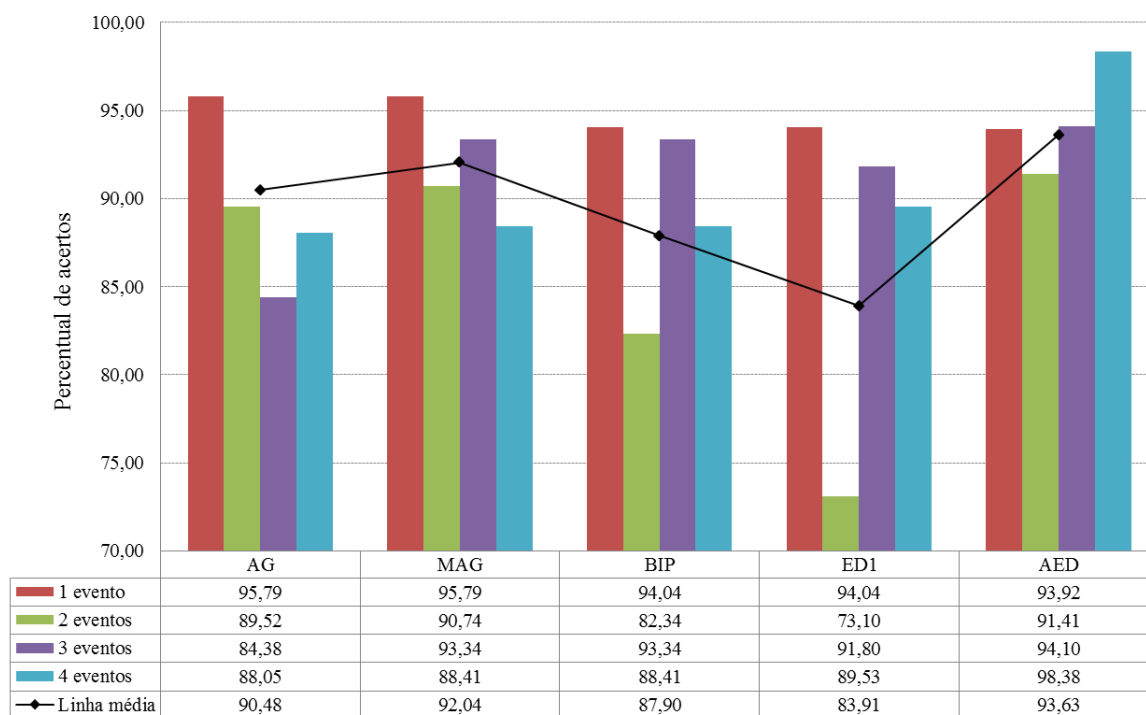
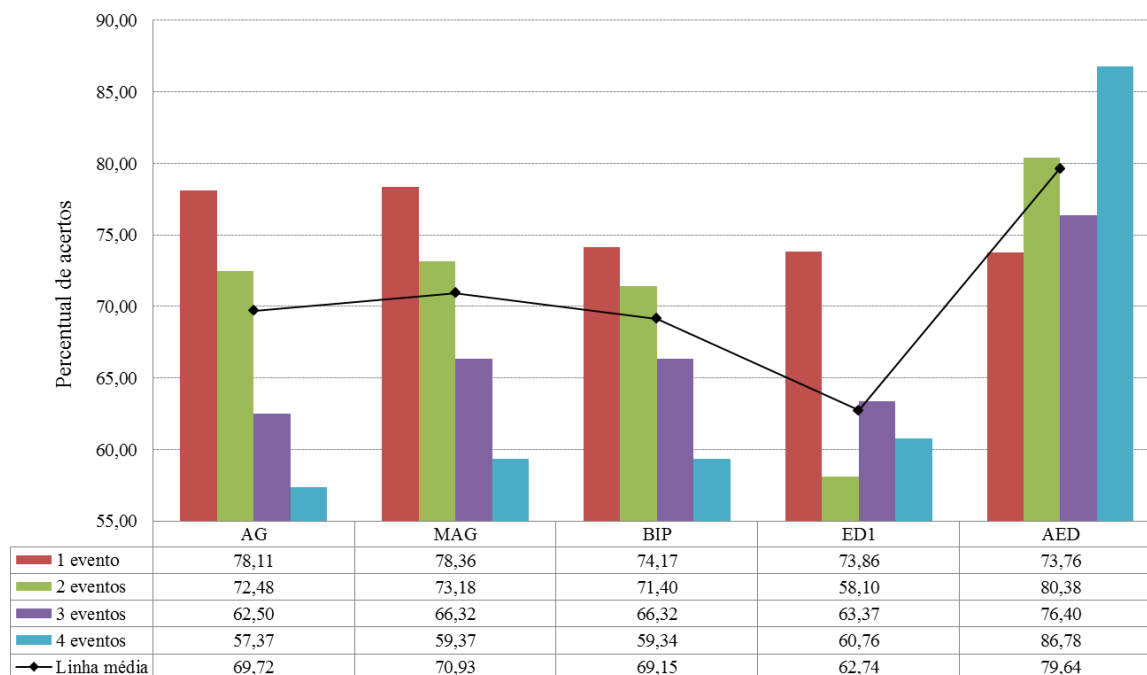


Figura 6.8 – Desempenho de métodos com 2 alarmes de ruído em nível de sistema



Os quadros contendo os resultados detalhados das simulações são mostrados no Apêndice C. Os resultados em nível de sistema mostram que o método AED consegue acertar 1,73% e 12,28% mais diagnósticos que o segundo melhor, o método MAG, nos testes envolvendo instâncias com um e dois alarmes aleatórios, respectivamente. Da mesma forma que ocorreu no nível local, o método AED possui desempenho inferior em instâncias com um único evento (1,93% e 5,57% em relação ao método MAG). Nos demais grupos de instâncias, o desempenho do AED continua superior aos demais e com o mesmo padrão de desempenho, melhora conforme aumenta a complexidade da instância.

Note que a solução do método ED1 foi degradada consideravelmente em relação ao desempenho obtido pela heurística baseada no teorema de Bayes. A principal razão da redução de acertos é devido ao número de eventos classificados em nível local ser menor do que o número encontrado pela GRNN e HC.

6.4 Análise dos métodos em um sistema de transmissão radial e malhado

Esse teste tem como objetivo principal comparar o desempenho dos métodos propostos neste trabalho para diagnóstico de faltas com o método proposto com Leão, Pereira e Mantovani (2010). Essa metodologia é baseada em um modelo UBP resolvida por

algoritmos artificiais imunológicos e é um dos diversos trabalhos que focam na aplicação de metaheurísticas bioinspiradas no problema de diagnóstico.

O sistema de potência considerado faz parte do sistema da Eletrosul e foi utilizado para obtenção de resultados por Leão, Pereira e Mantovani (2010). Na validação dos resultados, os autores consideraram o sistema de potência completamente malhado, inclusive nos barramentos de 69 e 138 kV. Para confirmar que a implementação do método IA estava correta, os dados das instâncias originais (SEP malhado) foram utilizados para obter os resultados apresentados no artigo original. Após validação do método IA, optou-se em modificar o sistema teste apresentado em Leão, Pereira e Mantovani (2010), uma vez que os sistemas de 69 e 138 kV são sistemas radiais. O diagrama unifilar do sistema da Eletrosul é mostrado na Figura 6.9.

Nos testes foram considerados que a rede de 525 kV não está conectada diretamente à área monitorada, que a rede de 230 kV é um sistema malhado e que as redes de 69 e 138 kV são sistemas radiais. O sistema monitorado é composto de cinco subestações: Curitiba (CT), Joinville (JV), Blumenau (BL), Palhoça (PA) e Jorge Lacerda B (JB); e está interligado em 230 kV com a SEs Umbará (UM), Jorge Lacerda A (JA), Jorge Lacerda C (JC), São Mateus do Sul (SM) e Siderópolis (SP). As SEs BL, JV e PA possuem monitoramento nos barramentos de 69 e 138 kV. A SE JB possui duas unidades geradoras, cujos relés não são considerados nos testes. As SEs CT e PA são conectadas a fontes externas sem qualquer monitoramento de alarmes.

O sistema monitorado é composto de 32 seções, sendo 8 barras de 230 kV (C, E, F, H, I, J, K, L), 13 linhas de transmissão (L2-L14) e 11 transformadores (TF1-TF11). Além disso, existem 11 seções interligadas sem monitoramento da proteção: uma barra de 69 kV (JVA69), três barras de 138 kV (BLA138, JVA138, PAA138), 5 terminais de linha (JA, JC, SM, SP, UM) e duas unidades geradoras (JBBG1 e JBBG2).

Para esse sistema foram modelados quatro conjuntos de regras da proteção, uma para cada tipo de equipamento: transformador, barra, LT radial e LT malhada. As regras modeladas estão disponíveis no Apêndice B. De acordo com as regras, existem 62 possíveis classificações de falta, sendo 32 eventos de falta interna (um evento por seção) e 30 eventos de faltas externas. O conjunto de padrões de funcionamento da proteção é formado por 129 diagnósticos, sendo 44 diagnósticos indicando falta em barras, 32 diagnósticos indicando falta em linhas, 33 diagnósticos indicando falta em transformadores e 20 diagnósticos indicando falta externa à região monitorada.

Nos testes computacionais foram consideradas 10 instâncias de faltas. As instâncias foram elaboradas por Leão, Pereira e Mantovani (2010) e correspondem a casos de múltiplas faltas. Apesar de improvável na prática, a simulação de múltiplas faltas é importante para a validação de métodos. A Tabela 6.2 mostra os conjuntos de alarmes reportados em cada teste.

Tabela 6.2 – Alarmes reportados nos testes envolvendo o SEP da Eletrosul

Teste	Alarmes de relés	Alarmes de CBs
1	DP3	CB6
2	DP3, BP11, BP12	CB6, CB9, CB11, CB12
3	BP11, BP12	CB6, CB9, CB11, CB12
4	DP5, DP13, BP8, BP19, OR2, OR5	CB8, CB12, CB13, CB19, CB28, CB30, CB32, CB33
5	MP8, MP11, BP6, BP16, BP19, OR1, OR2, OR3, OR4	CB6, CB8, CB11, CB16, CB19, CB28, CB29, CB30, CB32
6	DP8, MP14, BP16, BP19, BP21, BP25, OR1, OR2, OR3, OR9, OR10	CB16, CB19, CB21, CB25, CB28, CB29, CB30, CB37, CB38, CB41, CB42
7	DP6, DP11, DP18, DP20, MP20, MP27, BP14, BP20, BP21	CB14, CB16, CB17, CB21, CB24, CB26, CB27, CB37, CB38, CB40, CB41, CB43, CB53
8	DP22, MP22, BP21, BP25, OR9, OR10, OR11, OR12	CB21, CB22, CB25, CB37, CB38, CB41, CB42, CB49, CB51
9	DP10, DP22, MP20, MP21, MP22, OR19	CB20, CB52
10	DP13, MP6, MP9, BP6, BP9, BP12, BP16, BP19, OR2, OR5	CB9, CB16, CB19, CB28, CB29, CB32, CB33

Fonte: Leão, Pereira e Mantovani (2010).

Os parâmetros dos métodos utilizados nos testes são os seguintes:

- IA: $w_1 = 1000$; $w_2 = 3$; $w_3 = 2$; $P_c = 0,9$; $P_m = 0,001$; $n = 1000$; $nse = 25$;
- AD: $w_1 = 9$; $w_2 = 3$; $w_3 = 1$; $w_4 = 0,5$;
- Bayes: $pc = 0,82$; $pi = 0,12$; $pf = 0,06$;
- ED1: $w_1 = 9$; $w_2 = 3$; $w_3 = 1$;
- ED2: $w_1 = 9$; $w_2 = 3$; $w_3 = 1$; $w_4 = 0,5$;
- AED: $w_1 = 3$; $w_2 = 3$; $w_3 = 1$; $w_4 = 9$; $w_5 = 9$; $w_6 = 1$; $w_7 = 0,5$.

A topologia pós-falta de cada instância é mostrada no Apêndice D. Os diagnósticos obtidos nos testes computacionais são apresentados na Tabela 6.3.

Tabela 6.3 – Diagnósticos obtidos nas simulações de falta no SEP da Eletrosul

Teste	IA ¹	Solução esperada	IA	AD	Bayes ED1	Bayes ED2	AED
1	C JV	alarmes falsos	C JV BL JB	C	alarmes falsos	C	alarmes falsos
2	C L5	C/L3	C L3	C	C L3	C L2	C
3	C L5 CT	Qualquer seção de CT	C L10 CT BL PA	C	L3	L2 L5	L2
4	E TF1 TF2	E TF1 JVA138	E TF1 TF3	E TF1 TF2/TF3 JVA138	E TF1 JVA138	E TF1 JVA138	E TF1 JVA138
5	E L4 TF1	L4 TF2/TF3 TF4/TF5 JVA69	L4 TF1 TF2 TF4	L4 TF1 TF2/TF3 TF4/TF5 JVA69	L4 TF2 TF3 TF4 TF5 JVA69	L4 TF1 TF2 TF3 TF4 TF5 JVA69	L4 TF1 TF3 TF5 JVA69
6	E H L7 CT	F/H L7 TF1 TF2/TF3 TF4/TF5 TF8 TF9 CT	H L7 TF1 TF2 TF4 TF8 TF9 CT	H L7 TF1 TF2/TF3 TF4/TF5 TF8 TF9 CT (4a)	F H TF1 TF2 TF3 TF4 TF5 TF8 TF9	F H TF1 TF2 TF3 TF4 TF5 TF8 TF9 CT (4a)	F H L7 TF1 TF3 TF5 TF8 TF9
7	F K L9 L14 TF6 TF8	F K L9 L14 TF6 TF8	F K L9 L14 TF6 TF8	F K L9 L14 TF6 TF8	F K L14 TF6 TF8	F K L9 L14 TF6 TF8	F K L9 L14 TF6 TF8

Teste	IA ¹	Solução esperada	IA	AD	Bayes ED1	Bayes ED2	AED
8	F	L10	L10	L10	L10	L10	L10
	L10	TF6	TF6	TF6	TF6	TF6	TF6
	TF10	TF7	TF7	TF7	TF7	TF7	TF7
	JV	TF8	TF8	TF8	TF8	TF8	TF8
		TF9	TF9	TF9	TF9	TF9	TF9
		TF10	TF10	TF10	TF10	TF10	TF10
		JV (4a)	JV	JV (4a)		JV(4a)	
9	J	L9	J	I	I	I	I
	L9		L9	L9	J	J	J
	L10		L10	L10	L9	L9	L9
	TF10		TF10	TF10		L10	
			PAA138	PAA138			
10	L2	L2	L2	L2	L2	L2	L2
	L5	L5	L5	L5	TF1	TF1	L5
	TF1	TF1	TF1	TF1	TF3	TF3	TF1
	TF2	TF2	TF2	TF2	JVA138	JVA138	TF2
		JVA138		TF2/TF3			JVA138
				UMB			
			JVA138				

A coluna IA¹ corresponde ao resultado obtido pela metodologia proposta por Leão, Pereira e Mantovani (2010), considerando o sistema completamente malhado. A coluna “Solução esperada” corresponde à solução mais plausível de ser encontrada pelos métodos de diagnóstico, considerado o sistema radial e malhado. As demais colunas correspondem aos diagnósticos obtidos pelos métodos analisados.

Comparando os resultados do método IA¹ com a solução esperada é possível notar que houve mudança de solução em 9 das 10 instâncias devido a consideração de radicalidade nos componentes de 69 e 138 kV. Por exemplo, observe o impacto gerado na instância #8. Como os relés de sobrecorrente somente são sensibilizados para faltas a jusante, apenas o transformadores TF6-TF9 são candidatos à seção em falta, diferentemente da barra F, situada a montante dos relés de sobrecorrente.

No teste 1, os métodos que encontraram a solução ótima do problema foram os métodos ED1 e AED, que identificaram todos alarmes reportados como falsos. Observe que os demais métodos estimaram a barra C como sendo a seção em falta, mas essa hipótese é pouco plausível, visto que a falta continua sendo alimentada após atuação da proteção.

A solução esperada no teste 2 indica que falta pode estar localizada em duas seções: barra C ou linha L3. Os métodos AD e AED estimaram apenas a barra C em falta, enquanto

os métodos IA e ED1 estimaram ambas as seções como estando em falta. Esse resultado mostra que o diagnóstico por alarmes requer dados adicionais de tensão e corrente para distinguir o local da falta.

No teste 3, qualquer componente da SE CT pode ser considerada como sendo a seção em falta. Apenas os métodos AD, ED1 e AED identificaram seções da SE CT como estando em falta. Observe que todos os métodos obtiveram soluções distintas, o que permite concluir que o diagnóstico por meio de alarmes é limitado e requer informações adicionais para estimar corretamente a seção em falta.

Os métodos ED1, ED2 e AED estimaram corretamente as seções em falta no teste 4. Observe que uma das respostas corresponde a falta na barra de 138 kV da SE JV (JVA138), cuja proteção não é monitorada. O método IA não foi capaz de identificar essa seção, devido ao equacionamento utilizado para calcular os estados esperados de relés a partir dos alarmes de dispositivos de proteção. Seções em falta externas dificilmente serão identificadas pelo método IA, uma vez que as equações necessitam de dados monitorados no sistema.

O teste 5 possui uma falta na barra de 69 kV da SE JV (JVA69) que somente não é identificada pelo método IA. Como os transformadores TF2 e TF3 compartilham a proteção de sobrecorrente, a identificação da seção em falta somente pode ser obtida utilizando outras fontes de dados do sistema. O mesmo ocorre para os transformadores TF4/TF5. O método que obteve melhor desempenho é método ED1.

O teste 6 considera uma falha na comunicação de dados da SE CT. Os métodos IA, AD e ED2 conseguiram identificar a SE com falta CC, pois são os únicos modelos formulados que consideram essa possibilidade de falta. Em adição a essa formulação, o modelo dos métodos AD e ED2 permitem não apenas a identificação da SE com defeito, mas também a identificação dos alarmes que deveriam ter reportados na SE (4 alarmes no caso). Neste teste, considera-se que os métodos IA e AD obtiveram os melhores resultados.

No teste 7, apenas o método ED1 não encontrou uma das seções em falta (linha L9). O teste 8, existe uma falha no canal de comunicação de dados entre a SE JV e o COS. Apesar de todos os métodos diagnosticarem corretamente as faltas, apenas os métodos IA, AD e ED2 identificaram a falha no canal de comunicação.

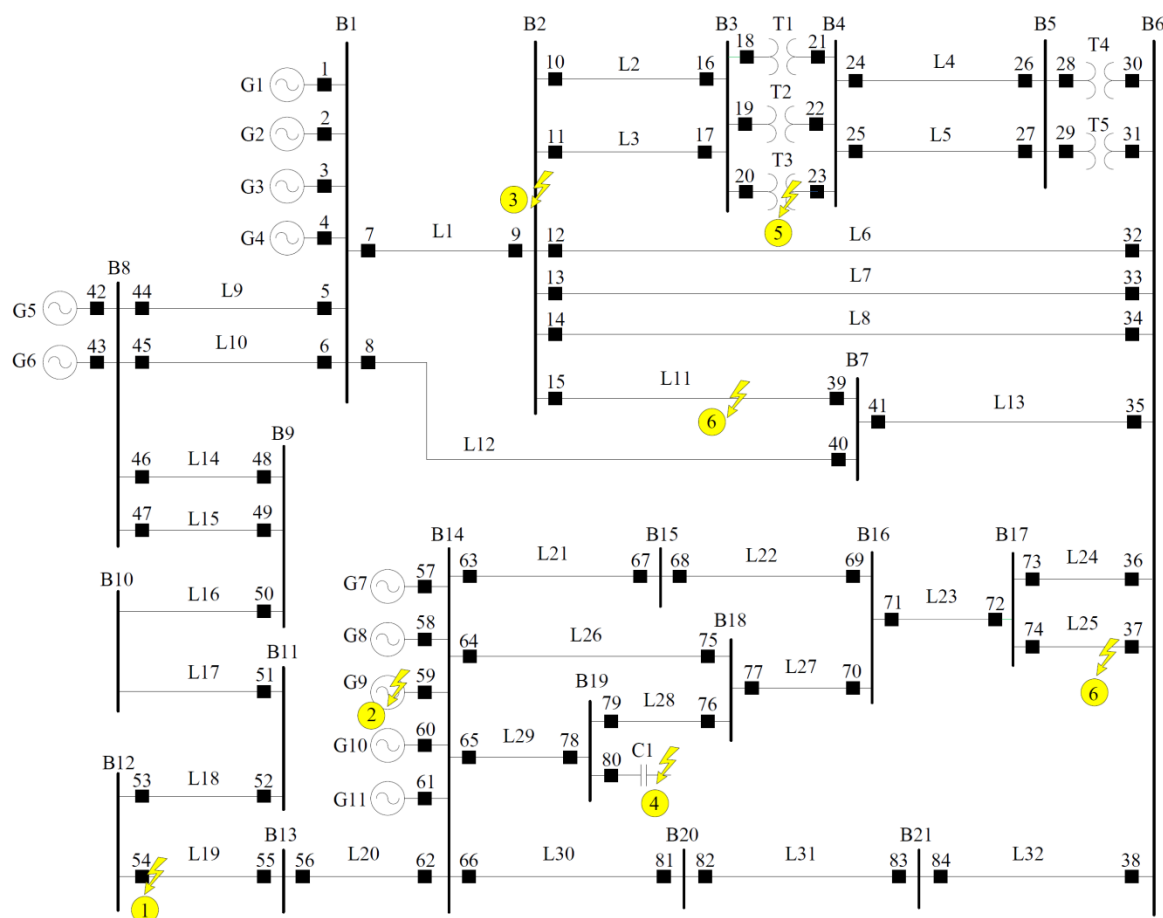
O teste 9 considera atuações da proteção principal de diversos componentes da SE PA, mas sem a devida abertura de disjuntores, um cenário extremamente improvável. As melhores soluções foram obtidas pelos métodos ED1 e AED, cujos diagnósticos são os mais parcimoniosos. No último teste, apenas o método AED diagnosticou corretamente as faltas.

Os resultados mostram que o método AED teve a melhor solução em 7 das 10 instâncias. O método AED não encontrou a melhor solução em dois casos: falhas no canal de comunicação entre SEs e o COS; e faltas em seções que compartilham o sistema de proteção. Para o primeiro caso, a melhor forma de resolver o problema é incluir a restrição ao modelo para lidar com SEs com falta CC ou falha na comunicação de dados. Já no segundo caso, o problema pode ser resolvido modelando um padrão específico para os componentes com proteção compartilhada ou desenvolvendo uma rotina de pós-processamento.

6.5 Testes computacionais em um SEP de grande porte

Diversas simulações foram realizadas em parte do sistema de 138/230 kV da CEEE-GT para validar e comparar as metodologias ED1 e AED. O método AD não foi considerado no teste por não ser uma metodologia de dois níveis. O método IA não foi considerado porque não é aplicável em SEPs que possuam esquemas de proteção com dois estágios de retaguarda.

Figura 6.10 – Diagrama unifilar do sistema de 138/230 kV da CEEE-GT



O sistema da CEEE-GT considerado é composto de 70 seções: 21 barras (B1-B21), 32 linhas de transmissão (L1-L32), 11 unidades geradoras (G1-G11), 5 transformadores (T1-T5), um banco de capacitores (C1) e protegidos por 84 disjuntores (CB1-CB84). As regras da proteção dos equipamentos foram apresentadas na seção 3.7.1. Todos os equipamentos de mesmo tipo possuem os mesmos esquemas de proteção, com exceção da barra B10 (não possui retaguarda local) e das linhas L16 e L17, que são linhas radiais. A Figura 6.10 mostra o diagrama unifilar do sistema CEEE-GT.

O total de alarmes monitorados no sistema são 398 alarmes, sendo 84 alarmes de estado de disjuntores e 314 alarmes de partida ou operação de relés. Observe que um alarme de relé corresponde a qualquer função de proteção pertencente ao esquema de proteção que possua a mesma finalidade de proteção como, por exemplo, as funções 87L e zona 1 do 21 que são consideradas como o alarme de proteção seletiva em linhas.

O sistema teste é composto de 1024 regras de proteção e de 174 eventos. Os possíveis eventos no sistema são:

- 21 eventos de falta interna em barras;
- 20 eventos de falta externa vista por barras;
- 32 eventos de falta interna em linhas;
- 62 eventos de falta externa direcional vista por linhas;
- 11 eventos de falta interna em unidades geradoras;
- 11 eventos de falta externa vista por unidades geradoras;
- 1 evento de falta interna em banco de capacitores;
- 1 evento de falta externa vista por banco de capacitores;
- 5 eventos de falta interna em transformadores;
- 10 eventos de falta externa direcional vista por transformadores.

Com base nos dados de topologia e de esquemas de proteção, o gerador de padrões encontrou 324 padrões para compor a base de conhecimento dos modelos de otimização. Os padrões consideram o possível funcionamento de sistema proteção principal, retaguarda local e retaguarda remota dos equipamentos.

Dados históricos do SCADA da concessionária referente a eventos ocorridos durante o mês de janeiro de 2011 foram utilizados para os testes computacionais. No entanto, as instâncias reais se mostraram fáceis de resolver devido à pequena extensão de distúrbios. Desta forma, foram gerados cenários de falta mais complexos incluindo a má operação de

sistemas de proteção e faltas múltiplas. Os estudos de caso estão enumerados na Figura 6.10, cujas descrições dos eventos são as seguintes:

- Evento 1 – Defeito no disjuntor CB54;
- Evento 2 – Desligamento completo da geração na barra B14;
- Evento 3 – Falta na barra B2;
- Evento 4 – Falta no banco de capacitores C1;
- Evento 5 – Falta no transformador T3;
- Evento 6 – Faltas simultâneas nas linhas L11 e L25.

Os parâmetros de simulação de cada método são os seguintes:

- Bayes: $p_c = 0,82$; $p_i = 0,12$; $p_f = 0,06$;
- ED1: $w_1 = 9$; $w_2 = 3$; $w_3 = 1$;
- AED: $w_1 = 3$; $w_2 = 3$; $w_3 = 1$; $w_4 = 9$; $w_5 = 9$; $w_6 = 1$; $w_7 = 0,5$.

A Tabela 6.4 mostra os alarmes reportados em cada estudo de caso e os diagnósticos obtidos utilizando o método ED1. A Tabela 6.5 mostra os resultados obtidos utilizando o método AED.

Tabela 6.4 – Testes computacionais e diagnósticos obtidos pelo método ED1

Teste	Seção	Alarmes reportados no SCADA			Classificação do evento			Solução do modelo				Diagnóstico	
		CBs	Relés	Barra	Prob.	Regra	Classificação	<i>f</i>	<i>s</i>	<i>ve</i>	FO	Seção em falta	CB falho ou indevido
1	-	-	CB54-baixa pressão	-	57,23%	1	Defeito em CB54	-	-	-	-	-	-
2	L20	-	21-3s	B13	84,88%	18	Falta na direção de B14	2	1	6	28	G9	
	L21	-	21-3s	B15	84,88%	13	Falta na direção de B14						
	L26	-	21-3s	B18	84,88%	13	Falta na direção de B14						
	L29	-	21-3s	B19	84,88%	13	Falta na direção de B14						
	B14	CB57 CB58 CB59 CB60 CB61	-	-	95,60%	9	Normal						
	G7	CB57	86 59	-	39,97%	7	Falta externa						
	G8	CB58	86 59	-	39,97%	7	Falta externa						
	G9	CB59	86 87	-	44,36%	3	Falta						
	G10	CB60	86 21G	-	39,97%	7	Falta externa						
	G11	CB61	86 59	-	39,97%	7	Falta externa						
3	B2	CB9 CB10 CB12 CB13 CB14 CB15	86 87 86BF	-	39,94%	5	Falta	-	-	-	1	B2	CB11 (falho)
	B3	CB17	-	-	95,60%	9	Normal						
	L1	CB9	21-2s 21-3s	B1	84,11%	19	Falta na direção de B2						
	L2	CB10	21-2s 21-3s	B3	84,11%	14	Falta na direção de B2						
	L3	CB17	21-2s 21-2t 21-3s	B3	82,19%	11	Falta na direção de B2						
	L6	CB12	21-2s 21-3s	B6	84,11%	14	Falta na direção de B2						

Teste	Seção	Alarmes reportados no SCADA			Classificação do evento			Solução do modelo				Diagnóstico	
		CBs	Relés	Barra	Prob.	Regra	Classificação	<i>f</i>	<i>s</i>	<i>ve</i>	FO	Seção em falta	CB falho ou indevido
3	L7	CB13	21-2s 21-3s	B6	84,11%	14	Falta na direção de B2						
	L8	CB14	21-2s 21-3s	B6	84,11%	14	Falta na direção de B2						
	L11	CB15	21-2s 21-3s	B7	84,11%	14	Falta na direção de B2						
4	B19	CB80	-	-	95,60%	9	Normal						
	C1	CB80	61 61N 86	-	39,72%	3	Falta	1	-	3	10	C1	-
	L29	-	21-3s	B18	84,88%	18	Falta na direção de B19						
5	B3	CB20	-	-	95,60%	9	Normal						
	B4	CB21 CB22 CB24 CB25	86BF	-	58,44%	7	Falta externa						
	B5	CB28 CB29	-	-	95,60%	9	Normal						
	L2	-	21-3s	B2	84,88%	18	Falta na direção de B3						CB23 (falho)
	L3	-	21-3s	B2	84,88%	18	Falta na direção de B3						CB28 (indevido)
	L4	CB24	21-3s	B5	84,11%	19	Falta na direção de B4	4	4	12	73	T3	CB29 (indevido)
	L5	CB25	21-3s	B5	84,11%	19	Falta na direção de B4						
	T1	CB21	-	-	57,40%	21	Normal						
	T2	CB22	-	-	57,40%	21	Normal						
	T3	CB20	86 87	-	53,45%	7	Falta						
	T4	CB28	51	B5	34,65%	15	Falta externa em 138 kV						
T5	CB29	51	B5	34,65%	15	Falta externa em 138 kV							

Teste	Seção	Alarmes reportados no SCADA			Classificação do evento			Solução do modelo				Diagnóstico	
		CBs	Relés	Barra	Prob.	Regra	Classificação	<i>f</i>	<i>s</i>	<i>ve</i>	FO	Seção em falta	CB falho ou indevido
6	B2	CB15	-	-	95,60%	9	Normal						
	B6	CB36 CB37	-	-	95,60%	9	Normal						
	B7	CB39	-	-	95,60%	9	Normal						
	B17	CB74	-	-	95,60%	9	Normal						
	L1	-	21-3s	B1	84,88%	18	Falta na direção de B2						
	L6	-	21-3s/21-3s	B2/B6	44,06%	13 18	Falta externa						
	L7	-	21-3s/21-3s	B2/B6	44,06%	13 18	Falta externa						
	L8	-	21-3s/21-3s	B2/B6	44,06%	13 18	Falta externa			9			
	L11	CB15 CB39	21-1 21-2s 21-3s	B2	86,39%	2	Falta	5	1	6	56	L11 L25	CB36 (indevido)
			21-1 21-2s 21-3s	B7						(2 eventos)			
	L12	-	21-2s 21-3s	B1	84,88%	18	Falta na direção de B7						
	L23	-	21-3s	B16	84,88%	13	Falta na direção de B17						
	L24	CB36	21-2s 21-2t 21-3s	B6	82,19%	11	Falta na direção de B17						
	L25	CB37 CB74	21-2s 21-3s 87L	B6	86,39%	2	Falta						
			21-2s 21-3s 87L	B17									
L32	-	21-2s 21-3s	B21	84,88%	13	Falta na direção de B6							

Tabela 6.5 - Testes computacionais e diagnósticos obtidos pelo método AED

Teste	FO	Eventos	Diagnóstico	Alarmes falhos
2	32	G7FI, G8FE, G9FI, G10FE, G11FE, L20→B14, L21→B14, L26→B14, L29→B14	Falta em G9	59 de G9
3	12	B2FI, L1→B2, L2→B2, L3→B2, L6→B2, L7→B2, L8→B2, L11→B2	Falta em B2	CB11
4	6	C1FI, L29→B19	Falta em C1	
5	27	B4FE, L2→B3, L3→B3, L4→B4, L5→B4, T3FI, T4→B5, T5→B5	Faltas em L4 e T3	CB26 e CB23
6	43	L1→B2, L6→B2, L6→B6, L7→B2, L7→B6, L8→B2, L8→B6, L11FI, L12→B7, L23→B17, L24→B17, L25FI, L32→B6	Falta em L11 e L25	zona 2 do 21 da linha L7

Códigos: FI é sigla de falta interna; FE é falta externa; → é falta na direção de uma barra.

Na Tabela 6.4, a coluna “Classificação do evento” se refere às soluções obtidas pela heurística baseada no teorema de Bayes em nível de equipamento. A coluna “Solução do modelo” contém as soluções ótimas encontradas pelo método ED1 para cada um dos testes. São apresentadas as seguintes informações: número de alarmes falhos (f), número de alarmes falsos (s), a contribuição do evento na FO (ve) e o valor alcançado da FO. A coluna “Diagnóstico” mostra a explicação semântica do evento, contendo as seções em falta e os dispositivos de proteção com atuação indevida.

Na Tabela 6.5, a coluna “Evento” contém as classificações escolhidas em nível de equipamento para justificar a falta. A coluna “Diagnóstico” contém a solução encontrada pelo método AED. A coluna “Alarmes falhos” contém os alarmes de relés e disjuntores que falharam.

O primeiro estudo de caso simula um defeito no compressor de gás do disjuntor CB54. Aplicando o método de Bayes, a probabilidade do evento estar relacionado a um defeito interno no disjuntor é de 57,23%. Como não há seções associados com o alarme disparado, o

módulo de otimização não é acionado. O mesmo ocorre com o método AED, cujo pré-processamento resolve a instância. Nesse caso, o diagnóstico sugere visita técnica em campo para realização dos reparos necessários.

O caso 2 consiste de um curto-circuito nos enrolamentos do estator do gerador síncrono G9 com posterior queda de tensão por sobrecarga e desligamento completo da geração conectada junto à barra B14. Neste cenário, 19 alarmes foram reportados e 10 equipamentos foram identificados por meio do mapeamento de eventos incluindo uma barra, quatro linhas e cinco unidades geradoras. Observe que todas as linhas perceberam a existência de uma falta em direção à barra B14, embora a proteção da barra tenha interpretado o distúrbio como normal. Ambos os métodos identificaram a unidade geradora G9 como originadora do distúrbio.

O terceiro caso está associado a uma falta na barra B2, que consiste de 26 alarmes reportados e 9 seções envolvidas. Todas as linhas vizinhas à falta identificaram uma falta em direção a B2, enquanto a barra B2 é classificada como estando em falta. A FO encontrada pelo modelo ED1 é igual a 1, visto que apenas um evento é necessário para explicar os alarmes recebidos (falta em B2 e falha na abertura de CB11). O método AED encontrou a mesma solução, porém com um valor de FO maior, como é de se esperar pelo método ser integrado nos dois níveis de análise.

O teste 4 considera uma falta em uma célula do banco de capacitores C1, o qual resultou em 6 alarmes disparados. A operação do relé de desbalanço de neutro (61N) e consequente abertura de CB80 são suficientes para caracterizar uma falta em C1. Ambos os métodos diagnosticaram corretamente a falta.

O quinto caso apresenta um efeito em cascata devido a uma falta mal isolada no transformador T3. O relé diferencial de T3 atuou corretamente, mas CB23 não operou corretamente. A falha de CB23 resultou na operação da proteção 86BF que “limpou” a barra B4, tirando de serviço dois transformadores e duas linhas de 138 kV. Por fim, houve sobrecarga nos transformadores T4 e T5 que ocasionou na operação do relé de sobrecorrente.

De acordo com a solução do modelo do método ED1, o transformador T3 é o único equipamento classificado como falta interna com probabilidade de 53,45%. Apesar da abertura dos disjuntores no lado de baixa tensão dos transformadores T1 e T2, ambos os esquemas de proteção não identificaram anormalidades na rede. O método estimou T3 como a seção em falta com FO igual 73, resultado da soma das seguintes contribuições: 1 de um evento (falta em T3 com falha de CB23); 36 da variável ve_i ($4 \times 3 = 12$), composta de quatro alarmes falhos (falta externa vista por T1 e T2); e 36 de quatro alarmes falsos (CB28, CB29,

falta externa na direção de B5 vista por T4 e T5). Os alarmes falsos são consequência da sobrecarga e caso os padrões considerassem esquemas de alívio de carga, provavelmente esses alarmes não seriam identificados como falsos.

O método AED encontrou uma solução múltipla: faltas na linha L4 e no transformador T3. Apesar da solução obtida pelo método ED1 possuir apenas uma seção em falta, a solução encontrada pelo método AED é mais parcimoniosa, pois utiliza dados dos dois níveis e encontra menos alarmes falhos para explicar a falta.

O último estudo de caso consiste de faltas simultâneas em duas linhas de transmissão, cujo evento resultou em 33 alarmes reportados e 14 seções afetadas. É possível averiguar na Tabela 6.4 a existência de um conflito de classificações do evento obtidas pelas linhas conectando as barras B2 e B6. A razão principal é pela baixa probabilidade dos eventos escolhidos (15,24%) devido ao fato destas linhas estarem localizadas entre as duas faltas. Ambos os métodos encontraram a diagnóstico correto.

6.6 Considerações finais

O presente capítulo apresentou os testes computacionais realizados para validação dos métodos de diagnóstico propostos na tese. Os testes compreendem diversos cenários de faltas em diferentes sistemas de potência de grande porte. Além da validação, foi analisado o desempenho obtido dos métodos propostos com métodos existentes na literatura especializada. Os métodos ED1 e AED foram os que obtiveram os melhores resultados de desempenho e que estiveram mais próximos das soluções esperadas em cada instância.

7 CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS

Nesta tese foram propostos um processador inteligente de alarmes e modelos de programação matemática para diagnóstico de faltas em sistemas elétricos de potência. Em um primeiro momento, foi realizada a revisão da literatura a fim de identificar o estado-da-arte no assunto. A revisão permitiu identificar a tendência do uso de metaheurísticas bioinspiradas na resolução de modelos de otimização para a estimação da seção em falta. Além disso, notou-se necessidade de desenvolver lógicas avançadas de gerenciamento de alarmes para viabilizar a implementação prática dos métodos de diagnóstico. Em um segundo momento, o problema de diagnóstico de faltas foi definindo, incluindo as funções esperadas tanto por um processador de alarmes quanto por um método de diagnóstico.

Com base nisso, foi desenvolvido um processador inteligente de alarmes que realiza a reordenação cronológica de alarmes reportados, mapeamento de eventos e a geração de padrões de funcionamento do sistema de proteção de acordo com a topologia da rede. O sistema de proteção considerado no desenvolvimento do gerador de padrões atende aos requisitos técnicos e de proteção estabelecidos nos procedimentos de rede do Operador Nacional do Sistema (ONS).

O problema de diagnóstico de faltas foi tratado dentro de três óticas distintas: a metodologia AD se refere ao método que gera diagnósticos a partir dos alarmes reportados no SCADA; a metodologia ED contém dois métodos que analisam, separadamente e de forma sequencial, os eventos gerados a partir dos alarmes reportados em nível de equipamento e os diagnósticos gerados a partir dos eventos; e a metodologia AED que consiste um único método que analisa a falta em dois níveis de forma integrada.

A partir das metodologias de diagnóstico, foram formulados quatro modelos de programação inteira para estimação da seção em falta considerando o critério da parcimônia e baseados no problema de recobrimento de conjuntos. O método AD incorpora um modelo com restrições adicionais que limita o número de alarmes falhos e identifica os alarmes de subestações com falha na comunicação de dados ou falta na alimentação de relés. Os métodos ED empregam uma heurística baseada no teorema de Bayes para a classificação de eventos em nível de equipamento. O método ED1 incorpora um modelo com restrição adicional que limita o uso de alarmes falhos em diagnósticos distintos. O método ED2 incorpora um modelo com as mesmas restrições do modelo do método AD. O método AED incorpora um modelo para diagnosticar faltas nos dois níveis de forma integrada. Além disso, o modelo do método AED limita o uso de alarmes falsos para cada equipamento sensibilizado pela falta.

Foram realizados testes computacionais para avaliar o desempenho obtido pelo processador de alarmes em relação aos seguintes itens: impacto no diagnóstico gerado pela reordenação cronológica de alarmes; mapeamento de eventos para métodos de diagnóstico em dois níveis; e geração de padrões de eventos. Além disso, foram realizadas simulações de faltas em diversos sistemas de potência para avaliar o desempenho obtido dos métodos propostos na tese em relação ao desempenho obtido por outras técnicas da literatura. Os testes computacionais foram divididos em quatro tipos de experimentos: análise de desempenho de métodos considerando padrões com e sem eventos “não falta”; comparação de métodos considerando instâncias com inserção de alarmes aleatórios; comparação de métodos de diagnóstico em um sistema de transmissão radial e malhado; comparação de métodos em um sistema elétrico de potência de grande porte.

Nos testes envolvendo as rotinas desenvolvidas para o processamento de alarmes, foi possível concluir que as lógicas avançadas de gerenciamento de alarmes são fundamentais para a implantação dos métodos de diagnóstico em sistemas supervisórios reais. No teste envolvendo a ordem cronológica de alarmes, notou-se melhoria na exatidão dos diagnósticos obtidos após a aplicação das máquinas de estados e do critério de tempo. Nos testes envolvendo operações do processador de alarmes, foi possível averiguar que o mapeamento de eventos permite a detecção de múltiplos eventos na mesma janela de dados. O terceiro teste mostrou que o algoritmo de geração de padrões permite encontrar um conjunto de padrões suficiente para o diagnóstico de faltas. Em todos os testes em que o gerador de padrões foi utilizado, o tempo de processamento ficou na casa dos milissegundos.

A exclusão dos eventos “não falta” dos padrões utilizados por Fritzen et al. (2012) não alterou o diagnóstico obtido pelos métodos propostos nesta tese. A exclusão desses eventos reduz o tempo de processamento total do diagnóstico, uma vez que não é requerida a classificação de eventos em todos os equipamentos.

Os resultados oriundos de testes computacionais com inserção de ruídos aleatórios mostram que o método AED apresenta o percentual médio de acertos de diagnósticos superior aos métodos comparados em instâncias com 2, 3 e 4 eventos. Além disso, notou-se que quanto maior a complexidade da instância analisada (maior número de eventos), melhor o desempenho do método AED. Essa relação é verdadeira apenas para o método AED e possui relação inversa para os demais métodos, ou seja, o desempenho cai com o aumento da complexidade da instância.

Os resultados oriundos de simulações de falta no sistema da Eletrosul mostram que o método AED teve a melhor o melhor desempenho, e apenas não encontrou a solução ótima

em dois tipos de instâncias: com falhas no canal de comunicação de dados e faltas em seções que compartilham o sistema de proteção. Por outro lado, os modelos dos métodos AD e ED2 foram capazes de identificar os alarmes que deveriam ter sido reportados na SE com falha no canal de comunicação de dados.

O último teste considera uma porção do sistema sob concessão da CEEE-GT e contém esquemas de proteção semelhantes aos esquemas reais de proteção. O método proposto por Leão, Pereira e Mantovani (2010) não foi considerado no teste porque a equação modelada para o funcionamento esperado de relés não prevê o uso de inúmeras funções de proteção existentes em esquemas reais de proteção e diferentes estágios de operação da proteção de retaguarda. Os resultados deste teste mostram que os métodos ED1 e AED conseguem obter soluções robustas para cenários complexos de falta, múltiplas faltas e com atuação indevida de dispositivos de proteção.

De forma geral, foi possível concluir que o método AED obteve os melhores resultados em relação aos seguintes itens: resolução integrada do problema de diagnóstico em dois níveis, uso de base de conhecimentos menores e possibilidade de encontrar a solução ótima do problema modelado devido ao uso de métodos exatos pelo *solver CPLEX 12.4* com configurações *default*. Como desvantagem do modelo AED, pode-se citar a ausência de restrição para lidar com SEs com falha no canal de comunicação ou falta CC.

7.1 Sugestões para trabalhos futuros

Para trabalhos futuros na área, são apresentadas as seguintes sugestões:

- analisar a sensibilidade dos pesos empregados nos modelos de otimização;
- desenvolver um sistema multi-agente que combine os dados de alarmes com dados de RDPs e PMUs;
- incluir restrição no modelo do método AED para detecção de faltas CC em SEs;
- incluir rotinas que detectem esquemas de alívio de carga e oscilação de potência;
- incorporar procedimentos de manobra para o reestabelecimento automático do SEP no PIA;
- validar o processador inteligente de alarmes no COS em tempo real.

REFERÊNCIAS

ALSTOM. **Network Protection & Automation Guide**. 1. ed., may 2011.

ANDERSON, P. M. **Power System Protection**. Nova York: McGraw-Hill, 1999. 1307 p.

ANSI/ISA-18.2. **Management of Alarm Systems for the Process Industries**. International Society of Automation, USA, 2009.

ARAÚJO, E. V. **Gerenciamento de Alarmes em Plantas Industriais: Conceitos, Normas e Estudo de Caso em um Forno de Reaquecimento de Blocos**. 2010. 101 p. Dissertação (Mestrado em Engenharia Elétrica), Universidade Federal de Minas Gerais, Belo Horizonte, 2010.

ATKINS, W. T. J. An Oscillograph for the Automatic Recording of Disturbances on Electric Supply Systems. **Proceedings of the IEE – Part II: Power Engineering**, v. 96, n. 50, p. 276-281, abr. 1949.

BAUER, A. et al. Alarm processing with model-based diagnosis of event discrete systems. **Proceedings of the AI for an Intelligent Planet**, p. 1–8, 2011.

BEDEKAR, P. P.; BHIDE, S. R.; KALE, V. S. Fault Section Estimation in Power System Using Hebb's Rule and Continuous Genetic Algorithm. **International Journal of Electrical Power & Energy Systems**, v. 33, n. 3, p. 457–465, mar. 2011.

BI, T.; LI, Q. Multi-layer Disturbance Processing System based on Multiple Information Sources. **Proceedings of the IEEE Power Engineering Society General Meeting**, p. 1-4, jun. 2007.

BROWN, D. C. Alarm System Performance – One Size Fits All? **Measurement + Control**, v. 36/4, p. 120-123, maio 2003.

CAPRARA, A.; TOTH, P. Algorithms for the Set Covering Problem. **Annals of Operations Research**, v. 98, p. 353-371, 2000.

CARDOSO JR., G. **Estimação da Seção em Falta em Sistemas Elétricos de Potência via Redes Neurais e Sistemas Especialistas Realizada em Nível de Centro de Controle**. 2003. 162 p. Tese (Doutorado em Engenharia Elétrica), Universidade Federal de Santa Catarina, Florianópolis, 2003.

CARDOSO JR., G.; ROLIM, J. G.; ZURN, H. H. Application of Neural-Network Modules to Electric Power System Fault Section Estimation. **IEEE Transactions on Power Delivery**, v. 19, n. 3, p. 1034–1041, jul. 2004.

CHEN, W. Fault Section Estimation Using Fuzzy Matrix-Based Reasoning Methods, **IEEE Transactions on Power Delivery**, v.26, n. 1, p. 205–213, jan. 2011.

CHEN, W. H.; TSAI, S. H.; LIN, H. I. Fault Section Estimation for Power Networks Using Logic Cause-Effect Models. **IEEE Transactions on Power Delivery**, v. 26, n. 2, p. 963–971, abr. 2011.

DAVIDSON, E. M. et al. Applying Multi-Agent System Technology in Practice: Automated Management and Analysis of SCADA and Digital Fault Recorder Data. **IEEE Transactions on Power Systems**, v. 21, n. 2, p. 559–567, maio 2006.

DIJKSTRA, E.W. A Note on Two Problems in Connexion with Graphs, **Numerische Mathematik**, v. 1, p. 269-271, jun. 1959.

DOBAKSHARI, A. S.; RANJBAR A. M. Application of synchronized phasor measurements to wide-area fault diagnosis and location, **IET Generation, Transmission & Distribution**, v. 8, n. 4, p. 716-729, abr. 2014.

EDWARDS, C. J. et al. Flexible Model-Based Alarm Processing for Protection Performance Assessment and Incident Identification. **IEEE Transactions on Power Delivery**, v. 28, n. 3, p. 2584–2591, ago. 2013.

EEMUA 191, Engineering Equipment Materials Users' Association. Alarm Systems A Guide to Design, Management and Procurement. **EEMUA Publication 191**, second edition, London, 2007.

EPRI - Electric Power Research Institute. **Human Factors Review of Electric Power Dispatch Control Centers**, v. 1-6, EL-1960, Palo Alto, CA, 1960.

FONSECA, W. A. S. et al. Simultaneous Fault Section Estimation and Protective Device Failure Detection Using Percentage Values of the Protective Devices Alarms. **IEEE Transactions on Power Systems**, v. 28, n. 1, p. 170-180, fev. 2013.

FRITZEN, P. C. et al. Hybrid System Based on Constructive Heuristic and Integer Programming for the Solution of Problems of Fault Section Estimation and Alarm Processing in Power Systems. **Electric Power Systems Research**, v. 90, p. 55–66, set. 2012.

FUKUI, C.; KAWAKAMI, J. An expert system for fault section estimation using information from protective relays and circuit breakers. **IEEE Transactions on Power Delivery**, v. PWRD-1, n. 4, out. 1986.

GHAINANI, A. T.; MOHD ZIN, A. A.; ISMAIL, N. A. M. Fuzzy timing Petri net for fault diagnosis in power system. **Mathematical Problems in Engineering**, v. 2012, p. 1-12, jun. 2012.

GUAN, Y.; KEZUNOVIC, M. Implementing Intelligent Techniques for the Advanced Alarm Processing. **15th International Conference on Intelligent System Applications to Power Systems**, p. 1–6, 2009.

GUO, W. et al. An Analytic Model for Fault Diagnosis in Power Systems Considering Malfunctions of Protective Relays and Circuit Breakers. **IEEE Transactions on Power Delivery**, v. 25, n. 3, p. 1393–1401, jul. 2010.

GUO, W. et al. An Analytic Model-Based Approach for Power System Alarm Processing Employing Temporal Constraint Network. **IEEE Transactions on Power Delivery**, v. 25, n. 4, p. 2435–2447, out. 2010.

- HE, Z. et al. Fault Section Estimation in Power Systems Based on Improved Optimization Model and Binary Particle Swarm Optimization. **IEEE Power & Energy Society General Meeting**, p. 1–8, 2009.
- HERTZ, A; FAUQUEMBERGUE, P. Fault Diagnosis at Substations Based on Sequential Event Recorders. **Proceedings of the IEEE**, v. 80, n. 5, p. 684–688, maio 1992.
- HOSSACK, J. A. et al. A Multiagent Architecture for Protection Engineering Diagnostic Assistance. **IEEE Transactions on Power Systems**, v. 18, n. 2, p. 639–647, maio 2003.
- HUANG, S. J.; LIU, X. Z. Application of Artificial Bee Colony-Based Optimization for Fault Section Estimation in Power Systems. **International Journal of Electrical Power & Energy Systems**, v. 44, n. 1, p. 210–218, jan. 2013.
- HUANG, S. et al. Application of Enhanced Honey-Bee Mating Optimization Algorithm to Fault Section Estimation in Power Systems. **IEEE Transactions on Power Delivery**, v. 28, n. 3, p. 1944–1951, jul. 2013.
- HUANG, S. J.; LIU X. Z. Fault Section Estimation in Distribution Systems using Biogeography-Based Optimization Approaches. **International Transactions on Electrical Energy Systems**, v. 5, n. 1, p. 155–168, jan. 2015.
- IBRAHIM, M. A. **Disturbance Analysis for Power Systems**. New York: Wiley-IEEE Press, 2011, 736 p.
- IEEE. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Std. C37.2: IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations**, New York: IEEE, 3 out. 2008. 48 p.
- JUNG, J. et al. Multiple Hypotheses and Their Credibility in On-Line. **IEEE Transactions on Power Delivery**, v. 16, n. 2, p. 225–230, abr. 2001.
- KIRSCHEN, D.S.; WOLLENBERG, B.F. Intelligent alarm processing in power systems, **Proceedings of the IEEE**, v. 80, n. 5, p. 663–672, maio 1992.
- LARMAN, C. **Applying UML and patterns: an introduction to object-oriented analysis and design the Unified Process**. Upper Saddle River, NJ:Prentice Hall, 2002. 627 p.
- LEÃO, F. B. **Metodologia para Análise e Interpretação de Alarmes em Tempo Real de Sistemas de Distribuição de Energia Elétrica**. 2011. 345 p. Tese (Doutorado em Engenharia Elétrica), Universidade Estadual Paulista, Ilha Solteira, 2011.
- LEÃO, F. B.; PEREIRA, R. A. F.; MANTOVANI, J. R. S. Fault Section Estimation in Electric Power Systems Using an Optimization Immune Algorithm. **Electric Power Systems Research**, v. 80, n. 11, p. 1341–1352, nov. 2010.
- LEÃO, F. B.; PEREIRA, R. A. F.; MANTOVANI, J. R. S. Fast fault section estimation in distribution control centers using adaptive genetic algorithm. **International Journal of Electrical Power & Energy Systems**, v. 63, p. 787–805, jul. 2014.

- LIN, X. et al. A Fault Diagnosis Method of Power Systems Based on Improved Objective Function and Genetic Algorithm-Tabu Search. **IEEE Transactions on Power Delivery**, v. 25, n. 3, p. 1268–1274, jul. 2011.
- LUO, X.; KEZUNOVIC, M. Implementing Fuzzy Reasoning Petri-Nets for Fault Section Estimation. **IEEE Transactions on Power Delivery**, v. 23, n. 2, p. 676–685, abr. 2008.
- MALHEIRO, N. et al. On-Line Fault Diagnosis with Incomplete Information in a Power Transmission Network. **Proceedings of the 13th International Conference on Intelligent System Applications to Power Systems**, p. 169–174, nov. 2005.
- MORETO, M.; ROLIM, J. G. Using phasor data records and sequence of events to automate the classification of disturbances of power generating units. **Electric Power Systems Research**, v. 81, n. 7, p. 1266-1273, jul. 2011.
- MU, J. et al. An Online Intelligent Alarm-Processing System Based on Abductive Reasoning Network. **IEEE Power and Energy Society General Meeting**, p. 1–5, jul. 2012.
- OLIVEIRA, A. L. et al. A mixed integer programming model for optimal fault section estimation in power systems. **International Journal of Electrical Power & Energy Systems**, p. 372-384, n. 77, maio 2016.
- ONS. Operador Nacional do Sistema Elétrico. **Procedimentos de Rede - Submódulo 2.6. Estabelece os requisitos mínimos para os sistemas de proteção e de telecomunicações**. Agência Nacional de Energia Elétrica, Brasília, DF, 16 set. 2010, revisão 1.1, p. 1-22.
- PENG, Y.; REGGIA, J. A. Plausibility of Diagnostic Hypotheses: The Nature of Simplicity. **Proceedings of the 5th National Conference on AI (AAAI-86)**, p. 140-145, 1986.
- PIRES, S. S. **Descoberta de Causa-raiz em Ocorrências de Sistemas Elétricos**. 2010. 89 p. Dissertação (Mestrado em Ciências da Computação), Universidade Federal de Campina Grande, Campina Grande, 2010.
- POPOVIC, T.; KEZUNOVIC, M. Measures of Value: Data Analytics for Automated Fault Analysis. **IEEE Power and Energy Magazine**, v. 10, n. 5, p. 58-69, out. 2012.
- PSRC. POWER SYSTEM RELAYING COMMITTEE. **PSRC WG D6: Power Swing and Out-of-Step Considerations on Transmission Lines**, New York: IEEE, jul. 2005
- PSRC. POWER SYSTEM RELAYING COMMITTEE. **Considerations for Use of Disturbance Recorders**. New York: IEEE, 27 dez. 2006.
- RODRIGUES, M. A. M. et al. Novas Tendências Para Análise Automática De Falhas E Distúrbios Em Sistemas De Potência. **X STPC - Seminário Técnico De Proteção E Controle**, Recife, 2010.
- SÖRENSEN, K. Metaheuristics – The Exposed Metaphors Considered Harmful. **Matheuristics – 4th International Workshop on Model-Based Metaheuristics**, set. 2012.

STAHLHUT, J. W.; HEYDT, G. T.; CARDELL, J. B. Power System “Economic Alarms”. **IEEE Transactions on Power Systems**, v. 23, n. 2, p. 426–433, maio 2008.

STRINGFIELD, T. W.; MARIHART, D. J.; STEVENS, R. F. Fault Location Methods for Overhead Lines. **IEEE Transactions on Power Apparatus and Systems**, v.76, n.3, p. 518-529, ago. 1957.

TOLLER, M. B. **Proposta de um sistema híbrido composto por redes neurais artificiais e algoritmos genéticos e o diagnóstico de faltas em sistemas elétricos de potência**. 2011. 131 p. Dissertação (Mestrado em Engenharia Elétrica), Universidade Federal de Santa Maria, Santa Maria, 2011.

UNITED STATES PATENT OFFICE. Edward W. Knapp. **Electrical transmission line fault finding system**. US n. 2242956, 9 p., 20 maio 1941.

WANG, J. et al. An overview of industrial alarm systems: main causes for alarm overloading, research status, and open problems. **IEEE Transactions on Automation Science and Engineering**, v. 13, n. 2, abr. 2016.

WEI, L. et al. An Online Intelligent Alarm-Processing System for Digital Substations. **IEEE Transactions on Power Delivery**, v. 26, n. 3, p. 1615–1624, jul. 2011.

WEN, F.; CHANG, C. S. A tabu search approach to fault section estimation in power systems. **Electric Power Systems Research**, v. 40, n. 1, p. 63–73, 1997.

WEN, F. S.; CHANG, C. S.; SRINIVASAN, D. Alarm Processing in Power Systems Using a Genetic Algorithm. **IEEE International Conference on Evolutionary Computation**, p. 27–32, 1995.

WEN, F. S.; HAN, Z., Fault section estimation in power systems using a genetic algorithm. **Electric Power Systems Research**, v. 34, n. 3, p. 165-172, fev. 1995.

WOLLENBERG, B.F. Feasibility study for an energy management system intelligent alarm processor. **IEEE Transactions on Power Systems**, v. PWRS-1, n. 2, pp. 241–246, maio 1986.

XIONG, G. et al. Divisional fault diagnosis of large-scale power systems based on radial basis function neural network and fuzzy integral. **Electric Power Systems Research**, v. 105, p. 9–19, ago. 2013.

APÊNDICE A – Estrutura de dados do sistema teste 2

Figura A.1 – Dados do sistema teste 2

TEQ				TDS					TDC			
i de v	Nome	Arestas	status	k de ek	v _i	v _j	Chaves	status	de di	Nome	Arestas	status
1	G1	1	1	1	1	2	-	1	1	S1	2 4	1
2	TR1	1 2 3 4 5	1	2	2	3	1 2 4 6	1	2	S2	2 4	1
3	B1	2 3 6 7 8 9 10 11 12 13	1	3	2	3	3 4	0	3	S3	3 5	0
4	B2	4 5 6 7 8 9 14 15 16 17	0	4	2	4	1 2 5 6	0	4	S6	2 3 7	1
5	L1	10 11 14 15 18 19 20 21	1	5	2	4	3 5	0	5	S7	4 5 7	0
6	L2	12 13 16 17 22 23 24 25	1	6	3	4	10 11	0	6	CB1	2 4	1
7	B3	18 19 26 27 28 29 30	1	7	3	4	4 5	0	7	S13	9	0
8	B4	20 21 26 27 28 31 32	0	8	3	4	16 17	0	8	S14	9	0
9	L3	29 30 31 32 33 34 35 36	1	9	3	4	7 8 9	0	9	CB3	9	0
10	B5	22 23 33 34 37 38 39 40 41 42	1	10	3	5	10 12 13 15	1	10	S4	6 10 11	1
11	B6	24 25 35 36 37 38 39 40 43 44	0	11	3	5	10 14	0	11	S5	6 14 15	0
12	TR2	41 42 43 44 45	1	12	3	6	16 18 19 21	1	12	S10	10 14	1
13	G2	45	1	13	3	6	16 20	0	13	S11	10 14	1
				14	4	5	11 12 13 15	0	14	S12	11 15	0
				15	4	5	11 14	0	15	CB2	10 14	1
				16	4	6	17 18 19 21	0	16	S8	8 12 13	1
				17	4	6	17 20	0	17	S9	8 16 17	0
				18	5	7	22 24 26	1	18	S15	12 16	1
				19	5	7	22 23 25	0	19	S16	12 16	1
				20	5	8	23 24 26	0	20	S17	13 17	0
				21	5	8	25	0	21	CB4	12 16	1
				22	6	10	35 37 38 40	1	22	S19	18 19 26	1
				23	6	10	35 39	0	23	S21	19 20 26	0
				24	6	11	36 37 38 40	0	24	S18	18 20	1
				25	6	11	36 39	0	25	S20	19 21	0
				26	7	8	22 23	0	26	CB5	18 20	1
				27	7	8	30 31	0	27	S26	28	0
				28	7	8	27 28 29	0	28	S27	28	0
				29	7	9	30 32 34	1	29	CB7	28	0
				30	7	9	30 31 33	0	30	S22	27 29 30	1
				31	8	9	31 32 34	0	31	S25	27 30 31	0
				32	8	9	33	0	32	S23	29 31	1
				33	9	10	44 46 47 49	1	33	S24	30 32	0
				34	9	10	44 48	0	34	CB6	29 31	1
				35	9	11	45 46 47 49	0	35	S33	22 23 37	1
				36	9	11	45 48	0	36	S34	24 25 37	0
				37	10	11	35 36	0	37	S29	22 24	1
				38	10	11	44 45	0	38	S28	22 24	1
				39	10	11	41 42 43	0	39	S30	23 25	0
				40	10	11	53 54	0	40	CB8	22 24	1
				41	10	12	50 51 53 55	1	41	S32	39	0
				42	10	12	52 53	0	42	S31	39	0
				43	11	12	50 51 54 55	0	43	CB9	39	0
				44	11	12	52 54	0	44	S35	33 34 38	1
				45	12	13	-	1	45	S36	35 36 38	0
									46	S37	33 35	1
									47	S38	33 35	1
									48	S39	34 36	0
									49	CB10	33 35	1
									50	S40	41 43	1
									51	S41	41 43	1
									52	S42	42 44	0
									53	S43	40 41 42	1
									54	S44	40 43 44	0
									55	CB11	41 43	1

TAL			
i de di	Nome	Verice	status
1	SS1 L2 230kV-(21)-Zone 1-A-Trip	6	0
⋮	⋮	⋮	⋮
88	SS3 L2 230kV-(21)-Zone1-A-Trip	6	0
⋮	⋮	⋮	⋮
101	SS1 L2 230kV-Recloser(79)-Trip	6	0
102	SS3 L2 230kV-Recloser(79)-Trip	6	0
⋮	⋮	⋮	⋮
245	B5 230kV-(87)-A-Trip	10	0
246	B5 230kV-(87)-B-Trip	10	0
247	B5 230kV-(87)-C-Trip	10	0
248	B5 230kV-Blocking-relay(86)-Trip	10	0

TED	
lista vazia	

APÊNDICE B – Conjunto de regras da proteção do sistema Eletrosul

Tabela B.1 – Regras da proteção de barras do sistema da Eletrosul

Alarmes	Regras			
	1	2	3	4
DP	1	1	0	0
CBs (<i>and</i>)	1	0	1	0

Tabela B.2 – Disjuntores associados ao alarme “CBs” de barras

Alarmes processados	Alarmes de disjuntores
CBs_C	CB3, CB6, CB8 e CB9
CBs_E	CB11, CB12, CB13, CB14, CB28, CB29 e CB20
CBs_F	CB16, CB17, CB37, CB38 e CB40
CBs_H	CB19, CB20, CB40, CB41 e CB42
CBs_I	CB52
CBs_J	CB21, CB22, CB50, CB51 e CB52
CBs_K	CB24, CB26, CB27, CB53 e CB55
CBs_L	CB23, CB25, CB53 e CB54

Tabela B.3 – Classificações das regras das barras do sistema da Eletrosul

Classificações	Regras			
Falta interna	1	1	1	0
Normal	0	0	0	1

Tabela B.4 – Regras da proteção de linhas malhadas

Alarmes	Regras													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
MP1	1	1	0	1	0	1	1	0	0	0	0	0	0	0
MP2	1	0	1	0	1	1	1	0	0	0	0	0	0	0
BP1	0	0	1	1	1	0	1	0	0	1	1	0	0	0
BP2	0	1	0	1	1	1	0	1	1	0	0	0	0	0
CB1	1	1	1	0	1	1	0	0	0	1	0	0	1	0
CB2	1	1	1	1	0	0	1	1	0	0	0	0	0	1

Tabela B.5 – Classificações das regras de linhas malhadas do sistema da Eletrosul

Classificações	Regras													
	Falta	1	1	1	1	1	1	1	0	0	0	0	0	0
Falta→S1	0	0	0	0	0	0	0	1	1	0	0	0	0	0
Falta→S2	0	0	0	0	0	0	0	0	0	1	1	0	0	0
Normal	0	0	0	0	0	0	0	0	0	0	0	1	1	1

Tabela B.6 – Regras da proteção de linhas radiais

Alarmes	Regras							
	1	2	3	4	5	6	7	8
MP	1	1	1	1	0	0	0	0
BP	0	1	1	0	1	1	0	0
CB	1	0	1	0	1	0	0	1

Tabela B.7 – Classificação das regras de linhas radiais do sistema da Eletrosul

Classificações	Regras							
	Falta interna	1	1	1	1	0	0	0
Falta→S2	0	0	0	0	1	1	0	0
Normal	0	0	0	0	0	0	1	1

Tabela B.8 – Regras da proteção de transformadores

Alarmes	Regras								
	1	2	3	4	5	6	7	8	9
DP	1	1	1	0	0	0	0	0	0
OR1	0	1	0	1	0	1	0	0	0
OR2	0	0	0	0	1	1	0	0	0
CB1	1	0	1	1	0	1	0	1	0
CB2	1	1	0	0	1	0	0	0	1

Tabela B.9 – Classificações das regras de transformadores do sistema da Eletrosul

Classificações	Regras								
	Falta interna	1	1	1	1	0	0	0	0
Falta→S2	0	0	0	0	1	1	0	0	0
Normal	0	0	0	0	0	0	1	1	1

APÊNDICE C – Diagnósticos obtidos por métodos no sistema AES-Sul

Quadro C.1 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 1 evento e 1 alarme de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
73	e79	17,93	100,00	100,00	100,00	100,00
85	e91	17,93	100,00	100,00	100,00	100,00
97	e103	17,97	100,00	100,00	100,00	100,00
67	e86	21,25	89,50	89,50	89,50	79,00
77	e90	21,25	91,50	91,50	91,50	100,00
79	e98	21,25	89,50	89,50	89,50	79,00
89	e102	21,25	91,50	91,50	91,50	100,00
91	e110	21,25	89,50	89,50	89,50	79,00
78	e95	21,50	93,00	86,50	86,50	96,00
90	e107	21,50	93,00	86,50	86,50	96,00
66	e83	21,65	92,00	82,00	82,00	89,00
68	e87	21,65	93,00	93,00	93,00	86,00
80	e99	21,65	93,00	93,00	93,00	86,00
92	e111	21,65	93,00	93,00	93,00	86,00
65	e78	21,75	90,00	90,00	90,00	100,00
62	e71	26,17	97,00	97,00	97,00	97,00
61	e70	34,67	95,00	95,00	95,00	95,00
64	e75	34,83	100,00	100,00	100,00	100,00
49	e54	35,50	100,00	100,00	100,00	100,00
38	e43	36,17	100,00	100,00	100,00	100,00
74	e84	36,50	100,00	91,50	91,50	90,00
86	e96	36,50	100,00	91,50	91,50	90,00
10	e10	37,00	100,00	100,00	100,00	100,00
27	e32	37,33	100,00	100,00	100,00	100,00
5	e5	38,50	100,00	100,00	100,00	100,00
98	e108	39,17	100,00	94,50	94,50	94,00
	Média	27,07	95,79	94,04	94,04	93,92

Quadro C.2 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 2 eventos e 1 alarme de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
50	e25 e61	14,75	88,83	88,83	86,83	99,50
58	e25 e65	16,95	80,53	80,87	79,33	91,17
54	e25 e62	17,03	81,54	83,70	81,67	96,17
56	e26 e63	17,15	79,59	80,79	78,79	97,17
59	e26 e66	17,20	79,48	81,65	79,50	96,50
20	e26 e36	20,28	80,77	80,77	77,50	91,00
40	e26 e56	20,32	83,63	83,63	82,83	97,33
41	e25 e57	20,36	80,63	80,63	77,17	90,33
29	e26 e45	20,36	86,23	86,23	85,00	98,00
31	e26 e47	20,36	81,90	81,90	79,67	93,00
18	e26 e34	20,44	85,17	85,17	83,67	96,67
30	e25 e46	20,53	79,57	79,57	76,33	86,67
42	e26 e58	20,57	83,57	83,57	83,33	92,00
19	e25 e35	20,57	80,43	80,43	76,50	85,67
28	e25 e44	20,61	83,97	83,97	82,17	98,67
39	e25 e55	20,61	83,97	83,97	82,17	98,67
17	e25 e33	20,97	82,17	82,17	80,33	98,67
70	e77 e85	24,63	92,83	92,83	92,83	95,33
52	e25 e73	24,76	90,00	90,00	88,83	100,00
82	e77 e97	24,83	89,00	89,00	89,00	90,67
94	e77 e109	24,89	95,17	95,17	95,17	97,33
69	e76 e80	24,95	93,00	93,00	93,00	92,00
81	e76 e92	24,95	93,00	93,00	93,00	92,00
93	e76 e104	24,95	93,00	93,00	93,00	92,00
96	e77 e113	26,92	90,50	90,50	90,50	91,33
84	e77 e101	27,58	92,83	92,83	92,83	95,33
72	e77 e89	27,83	94,17	94,17	94,17	96,67
95	e76 e112	28,08	91,33	91,33	91,33	93,33
71	e76 e88	28,50	91,17	91,17	91,17	92,00
83	e76 e100	28,50	91,17	91,17	91,17	92,00

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
36	e20 e48	31,77	77,90	77,90	93,00	99,00
60	e25 e64	31,82	81,03	38,02	36,64	55,67
47	e20 e59	32,34	80,97	80,97	96,50	98,00
7	e12 e20	32,57	73,77	73,77	84,00	85,33
26	e20 e38	32,80	78,50	97,50	100,00	100,00
37	e20 e49	32,80	78,33	78,33	95,00	99,00
48	e20 e60	32,80	78,50	97,50	100,00	100,00
6	e11 e20	33,71	78,53	78,53	84,00	100,00
25	e20 e37	33,71	79,47	79,47	95,00	98,00
12	e18 e20	38,17	80,30	94,00	94,00	97,00
	Média	25,07	84,66	85,02	86,17	93,98

Quadro C.3 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 3 eventos e 1 alarme de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
14	e7 e14 e22	22,73	79,03	79,03	79,03	94,00
13	e7 e14 e21	22,94	79,35	79,35	79,35	99,00
15	e8 e15 e23	26,33	75,34	75,34	88,33	99,00
16	e8 e15 e24	26,57	76,67	76,67	89,17	98,00
8	e6 e16 e19	28,68	87,70	87,70	88,58	96,00
2	e2 e15 e27	28,73	77,50	77,50	85,33	91,00
1	e1 e15 e27	28,90	75,86	75,86	79,67	98,00
9	e6 e17 e19	28,97	87,72	87,72	88,25	96,00
3	e3 e9 e19	29,18	85,40	85,40	86,50	96,50
4	e4 e9 e19	29,32	84,97	84,97	85,25	98,00
	Média	27,24	80,95	80,95	84,95	96,55

Quadro C.4 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 4 eventos e 1 alarme de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
21	e7 e14 e23 e28	19,88	83,09	83,09	83,09	96,80
33	e7 e14 e24 e41	19,94	81,03	81,03	81,03	99,14
32	e7 e14 e23 e39	19,95	85,50	85,50	85,50	99,14
22	e7 e14 e24 e30	19,97	81,28	81,28	81,28	97,43
44	e7 e14 e24 e52	19,97	81,28	81,28	81,28	97,43
43	e7 e14 e23 e50	20,14	81,77	81,77	81,77	99,38
51	e6 e9 e23 e67	20,26	80,93	80,93	80,67	100,00
55	e6 e9 e23 e68	22,42	79,87	79,87	78,61	99,57
57	e6 e9 e24 e69	22,62	82,56	82,56	82,09	99,67
24	e8 e15 e24 e31	22,96	77,87	77,87	92,60	99,14
23	e8 e15 e23 e29	22,98	78,81	78,81	88,40	98,29
34	e8 e15 e23 e40	22,98	78,81	78,81	88,40	98,29
46	e8 e15 e24 e53	23,04	78,42	78,42	88,75	97,86
45	e8 e15 e23 e51	23,09	76,41	76,41	89,70	99,14
35	e8 e15 e24 e42	23,10	76,47	76,47	89,85	97,43
53	e6 e9 e23 e74	28,23	82,94	82,94	82,91	99,67
	Média	21,97	80,44	80,44	84,75	98,65

Quadro C.5 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 1 evento e 2 alarmes de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
73	e79	35,43	90,00	96,00	96,00	94,50
85	e91	35,43	90,00	96,00	96,00	94,50
97	e103	35,43	90,00	96,00	96,00	94,50
68	e87	42,50	72,17	70,42	70,42	61,00
80	e99	42,50	72,17	70,42	70,42	61,00
92	e111	42,50	72,17	70,42	70,42	61,00
66	e83	42,67	66,50	57,83	57,83	64,00
67	e86	42,67	68,92	68,92	68,92	70,00
78	e95	42,67	66,50	57,83	57,83	64,00

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
79	e98	42,67	68,92	68,92	68,92	70,00
90	e107	42,67	66,50	57,83	57,83	64,00
91	e110	42,67	68,92	68,92	68,92	70,00
65	e78	43,33	69,50	69,50	69,50	90,00
77	e90	43,33	69,50	69,50	69,50	90,00
89	e102	43,33	69,50	69,50	69,50	90,00
62	e71	46,67	90,00	90,00	90,00	89,00
74	e84	50,67	87,50	67,58	66,08	58,00
86	e96	50,67	87,50	67,58	66,08	58,00
98	e108	50,67	87,50	67,58	66,08	58,00
	Média	43,08	76,51	72,67	72,43	73,76

Quadro C.6 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 2 eventos e 2 alarmes de ruído

Diagnóstico	Eventos	Ruído	GRNN	HC	Bayes	AED (%)
50	e25 e61	27,65	79,30	80,07	76,17	96,50
54	e25 e62	32,04	68,12	67,26	65,05	86,17
58	e25 e65	32,09	68,74	67,88	66,40	86,17
59	e26 e66	32,25	68,52	67,57	65,67	86,67
56	e26 e63	32,63	62,06	63,83	58,99	83,50
20	e26 e36	38,13	62,92	62,92	59,83	79,00
31	e26 e47	38,13	62,92	62,92	59,83	80,33
42	e26 e58	38,15	62,52	62,52	57,07	73,33
19	e25 e35	38,47	63,73	63,73	57,08	79,17
17	e25 e33	38,89	70,49	70,49	67,67	87,42
41	e25 e57	38,99	62,55	62,55	57,42	80,00
28	e25 e44	39,16	67,15	67,15	66,17	86,08
39	e25 e55	39,16	67,15	67,15	66,17	86,75
18	e26 e34	39,27	71,92	71,92	68,48	85,17
40	e26 e56	39,27	71,92	71,92	68,48	84,83
29	e26 e45	39,30	66,71	66,71	64,22	82,83
30	e25 e46	39,34	62,25	62,25	56,33	77,67

Diagnóstico	Eventos	Ruído	GRNN	HC	Bayes	AED (%)
82	e77 e97	42,89	82,55	80,68	81,35	89,75
94	e77 e109	42,89	82,55	80,68	81,35	89,75
52	e25 e73	43,07	79,40	79,40	76,67	99,67
70	e77 e85	44,25	78,40	77,85	77,60	83,83
60	e25 e64	45,03	66,39	35,89	34,00	41,08
69	e76 e80	45,40	79,08	79,08	78,50	82,67
81	e76 e92	45,40	79,08	79,08	78,50	82,67
93	e76 e104	45,40	79,08	79,08	78,50	82,67
96	e77 e113	46,93	77,23	76,40	75,00	88,17
71	e76 e88	47,23	74,73	74,73	73,67	84,25
83	e76 e100	47,23	74,73	74,73	73,67	84,25
95	e76 e112	48,53	74,38	74,38	72,33	82,67
72	e77 e89	48,73	77,13	76,13	74,00	89,00
84	e77 e101	48,73	77,13	76,13	74,00	89,00
37	e20 e49	55,03	65,77	65,77	89,67	94,00
6	e11 e20	55,54	50,68	50,68	57,17	83,67
36	e20 e48	55,92	66,02	66,02	89,67	92,33
7	e12 e20	56,38	53,47	53,47	61,83	91,00
25	e20 e37	56,89	65,68	65,68	87,00	93,33
47	e20 e59	56,89	65,68	65,68	87,00	92,33
26	e20 e38	57,24	65,87	65,87	87,00	90,33
48	e20 e60	57,24	65,87	65,87	87,00	90,33
12	e18 e20	59,17	62,87	62,87	74,92	100,00
	Média	44,37	69,57	68,62	70,79	85,46

Quadro C.7 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 3 eventos e 2 alarmes de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
14	e7 e14 e22	44,21	56,26	56,26	57,15	83,41
13	e7 e14 e21	45,26	54,10	54,10	54,66	87,73
16	e8 e15 e24	48,26	48,45	48,45	60,65	85,43
15	e8 e15 e23	49,71	45,69	45,69	60,08	77,23

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
2	e2 e15 e27	51,19	52,21	52,21	55,32	79,08
1	e1 e15 e27	52,38	46,30	46,30	47,00	75,67
4	e4 e9 e19	53,51	55,76	55,76	58,12	87,29
9	e6 e17 e19	54,07	61,60	61,60	65,65	94,89
8	e6 e16 e19	54,29	61,26	61,26	65,47	88,89
3	e3 e9 e19	54,92	58,44	58,44	60,63	86,00
	Média	50,78	54,01	54,01	58,47	84,56

Quadro C.8 – Desempenho médio de métodos em nível de equipamento considerando instâncias com 4 eventos e 2 alarmes de ruído

Diagnóstico	Eventos	Ruído (%)	GRNN (%)	HC (%)	Bayes (%)	AED (%)
51	e6 e9 e23 e67	35,98	64,60	64,60	64,46	98,67
21	e7 e14 e23 e28	38,65	64,25	64,25	65,40	90,53
43	e7 e14 e23 e50	38,81	65,26	65,26	65,96	92,74
32	e7 e14 e23 e39	38,88	59,86	59,86	60,82	88,01
22	e7 e14 e24 e30	38,93	60,39	60,39	62,06	88,38
44	e7 e14 e24 e52	38,93	60,39	60,39	62,06	88,38
33	e7 e14 e24 e41	39,05	61,07	61,07	62,21	90,14
57	e6 e9 e24 e69	39,18	64,75	64,75	64,23	97,29
55	e6 e9 e23 e68	39,46	61,94	61,94	62,43	96,62
45	e8 e15 e23 e51	42,88	50,65	50,65	63,22	80,98
23	e8 e15 e23 e29	43,17	53,69	53,69	66,42	90,37
34	e8 e15 e23 e40	43,17	53,69	53,69	66,42	90,37
35	e8 e15 e24 e42	43,78	55,26	55,03	64,91	86,57
24	e8 e15 e24 e31	44,38	52,86	52,86	64,12	87,91
46	e8 e15 e24 e53	44,38	52,86	52,86	64,12	87,24
53	e6 e9 e23 e74	48,56	60,70	60,70	61,37	99,14
	Média	41,14	58,89	58,88	63,76	90,83

Quadro C.9 – Desempenho médio de métodos em nível de sistema considerando instâncias com 1 evento e 1 alarme de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
73	e79	17,93	100,00	100,00	100,00	100,00	100,00
85	e91	17,93	100,00	100,00	100,00	100,00	100,00
97	e103	17,97	100,00	100,00	100,00	100,00	100,00
67	e86	21,25	89,50	89,50	89,50	89,50	79,00
77	e90	21,25	91,50	91,50	91,50	91,50	100,00
79	e98	21,25	89,50	89,50	89,50	89,50	79,00
89	e102	21,25	91,50	91,50	91,50	91,50	100,00
91	e110	21,25	89,50	89,50	89,50	89,50	79,00
78	e95	21,50	93,00	93,00	86,50	86,50	96,00
90	e107	21,50	93,00	93,00	86,50	86,50	96,00
66	e83	21,65	92,00	92,00	82,00	82,00	89,00
68	e87	21,65	93,00	93,00	93,00	93,00	86,00
80	e99	21,65	93,00	93,00	93,00	93,00	86,00
92	e111	21,65	93,00	93,00	93,00	93,00	86,00
65	e78	21,75	90,00	90,00	90,00	90,00	100,00
62	e71	26,17	97,00	97,00	97,00	97,00	97,00
61	e70	34,67	95,00	95,00	95,00	95,00	95,00
64	e75	34,83	100,00	100,00	100,00	100,00	100,00
49	e54	35,50	100,00	100,00	100,00	100,00	100,00
38	e43	36,17	100,00	100,00	100,00	100,00	100,00
74	e84	36,50	100,00	100,00	91,50	91,50	90,00
86	e96	36,50	100,00	100,00	91,50	91,50	90,00
10	e10	37,00	100,00	100,00	100,00	100,00	100,00
27	e32	37,33	100,00	100,00	100,00	100,00	100,00
5	e5	38,50	100,00	100,00	100,00	100,00	100,00
98	e108	39,17	100,00	100,00	94,50	94,50	94,00
	Média	27,07	95,79	95,79	94,04	94,04	93,92

Quadro C.10 – Desempenho médio de métodos em nível de sistema considerando instâncias com 2 eventos e 1 alarme de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
50	e25 e61	14,75	100,00	100,00	100,00	81,00	99,50
58	e25 e65	16,95	88,23	88,23	88,73	77,33	88,50
54	e25 e62	17,03	92,07	92,37	95,87	78,83	94,50
56	e26 e63	17,15	92,90	93,20	92,20	72,20	96,50
59	e26 e66	17,20	93,70	93,70	93,70	72,00	95,50
20	e26 e36	20,28	91,00	91,00	91,00	67,00	88,00
40	e26 e56	20,32	92,50	92,50	92,50	75,00	96,00
41	e25 e57	20,36	92,50	92,50	92,50	65,50	86,00
29	e26 e45	20,36	91,50	91,50	91,50	76,00	97,00
31	e26 e47	20,36	92,00	92,00	92,00	69,00	90,00
18	e26 e34	20,44	89,00	94,00	94,00	77,00	95,00
30	e25 e46	20,53	89,50	89,50	89,50	66,50	80,00
42	e26 e58	20,57	91,50	92,00	92,00	72,00	88,00
19	e25 e35	20,57	83,50	87,50	87,50	63,00	79,00
28	e25 e44	20,61	96,50	93,00	93,00	75,50	98,00
39	e25 e55	20,61	92,67	93,00	93,00	75,50	98,00
17	e25 e33	20,97	92,50	92,50	92,50	71,50	98,00
70	e77 e85	24,63	93,00	93,00	93,00	93,00	93,00
52	e25 e73	24,76	100,00	100,00	100,00	85,00	100,00
82	e77 e97	24,83	86,00	86,00	86,00	86,00	86,00
94	e77 e109	24,89	96,00	96,00	96,00	96,00	96,00
69	e76 e80	24,95	88,00	88,00	88,00	88,00	88,00
81	e76 e92	24,95	88,00	88,00	88,00	88,00	88,00
93	e76 e104	24,95	88,00	88,00	88,00	88,00	88,00
96	e77 e113	26,92	87,00	87,00	87,00	87,00	87,00
84	e77 e101	27,58	93,00	93,00	93,00	93,00	93,00
72	e77 e89	27,83	95,00	95,00	95,00	95,00	95,00
95	e76 e112	28,08	90,00	90,00	90,00	90,00	90,00
71	e76 e88	28,50	88,00	88,00	88,00	88,00	88,00
83	e76 e100	28,50	88,00	88,00	88,00	88,00	88,00

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
36	e20 e48	31,77	85,00	85,00	85,00	86,00	99,00
60	e25 e64	31,82	90,23	90,23	28,32	25,13	40,00
47	e20 e59	32,34	91,50	91,50	91,50	93,00	98,00
7	e12 e20	32,57	76,33	76,33	76,33	70,00	78,00
26	e20 e38	32,80	96,00	91,00	0,00	0,00	100,00
37	e20 e49	32,80	88,00	89,00	89,00	90,00	99,00
48	e20 e60	32,80	45,00	91,00	0,00	0,00	100,00
6	e11 e20	33,71	86,33	83,83	83,83	70,00	100,00
25	e20 e37	33,71	88,00	88,00	88,00	90,00	98,00
12	e18 e20	38,17	93,00	95,00	0,00	0,00	97,00
	Média	25,07	89,52	90,74	82,34	73,10	91,41

Quadro C.11 – Desempenho médio de métodos em nível de sistema considerando instâncias com 3 eventos e 1 alarme de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
14	e7 e14 e22	22,73	96,50	95,50	95,50	95,50	94,00
13	e7 e14 e21	22,94	98,00	97,50	97,50	97,50	99,00
15	e8 e15 e23	26,33	49,67	97,50	97,50	97,50	99,00
16	e8 e15 e24	26,57	77,33	96,50	96,50	96,50	98,00
8	e6 e16 e19	28,68	89,00	89,50	89,50	89,00	92,00
2	e2 e15 e27	28,73	88,33	88,33	88,33	80,00	82,00
1	e1 e15 e27	28,90	68,67	89,58	89,58	84,00	96,00
9	e6 e17 e19	28,97	90,50	90,50	90,50	88,00	92,00
3	e3 e9 e19	29,18	91,83	93,00	93,00	95,00	93,00
4	e4 e9 e19	29,32	94,00	95,50	95,50	95,00	96,00
	Média	27,24	84,38	93,34	93,34	91,80	94,10

Quadro C.12 – Desempenho médio de métodos em nível de sistema considerando instâncias com 4 eventos e 1 alarme de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
21	e7 e14 e23 e28	19,88	77,67	77,67	77,67	79,67	96,00
33	e7 e14 e24 e41	19,94	83,50	75,00	75,00	77,50	99,00
32	e7 e14 e23 e39	19,95	87,50	87,50	87,50	90,00	99,00
22	e7 e14 e24 e30	19,97	80,33	81,50	81,50	82,50	97,00
44	e7 e14 e24 e52	19,97	82,50	81,50	81,50	82,50	97,00
43	e7 e14 e23 e50	20,14	87,83	82,83	82,83	83,83	99,00
51	e6 e9 e23 e67	20,26	94,50	94,50	94,50	96,50	100,00
55	e6 e9 e23 e68	22,42	92,00	94,50	94,50	95,00	99,50
57	e6 e9 e24 e69	22,62	96,00	96,00	96,00	98,00	99,50
24	e8 e15 e24 e31	22,96	95,50	96,00	96,00	96,00	99,00
23	e8 e15 e23 e29	22,98	87,67	89,00	89,00	89,00	98,00
34	e8 e15 e23 e40	22,98	84,17	89,00	89,00	89,00	98,00
46	e8 e15 e24 e53	23,04	89,00	91,00	91,00	91,00	97,50
45	e8 e15 e23 e51	23,09	88,50	91,50	91,50	91,50	99,00
35	e8 e15 e24 e42	23,10	93,17	95,00	95,00	95,00	97,00
53	e6 e9 e23 e74	28,23	89,00	92,00	92,00	95,50	99,50
	Média	21,97	88,05	88,41	88,41	89,53	98,38

Quadro C.13 – Desempenho médio de métodos em nível de sistema considerando instâncias com 1 evento e 2 alarmes de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
73	e79	35,43	90,00	90,00	96,00	96,00	94,50
85	e91	35,43	90,00	90,00	96,00	96,00	94,50
97	e103	35,43	90,00	90,00	96,00	96,00	94,50
68	e87	42,50	75,50	75,50	73,67	73,67	61,00
80	e99	42,50	75,42	75,50	73,67	73,67	61,00
92	e111	42,50	75,50	75,50	73,67	73,67	61,00
66	e83	42,67	68,00	68,00	59,17	59,17	64,00
67	e86	42,67	70,08	70,08	70,08	70,08	70,00
78	e95	42,67	68,00	68,00	59,17	59,17	64,00

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
79	e98	42,67	70,42	70,08	70,08	70,08	70,00
90	e107	42,67	66,50	68,00	59,17	59,17	64,00
91	e110	42,67	69,33	70,08	70,08	70,08	70,00
65	e78	43,33	72,58	72,67	72,67	72,67	90,00
77	e90	43,33	72,17	72,67	72,67	72,67	90,00
89	e102	43,33	73,17	72,67	72,67	72,67	90,00
62	e71	46,67	90,00	90,00	90,00	90,00	89,00
74	e84	50,67	90,00	90,00	68,17	66,17	58,00
86	e96	50,67	87,50	90,00	68,17	66,17	58,00
98	e108	50,67	90,00	90,00	68,17	66,17	58,00
	Média	43,08	78,11	78,36	74,17	73,86	73,76

Quadro C.14 – Desempenho médio de métodos em nível de sistema considerando instâncias com 2 eventos e 2 alarmes de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
6	e11 e20	27,65	49,33	50,00	50,00	38,00	75,50
7	e12 e20	32,04	57,17	54,67	54,67	46,50	86,50
12	e18 e20	32,09	62,00	70,00	70,00	67,00	100,00
17	e25 e33	32,25	76,92	76,42	76,42	56,00	84,00
18	e26 e34	32,63	77,50	77,50	77,50	53,33	80,50
19	e25 e35	38,13	64,33	74,33	74,33	39,50	73,00
20	e26 e36	38,13	73,50	73,50	73,50	43,00	70,50
25	e20 e37	38,15	74,50	73,50	73,50	76,00	92,00
26	e20 e38	38,47	73,17	72,83	72,83	77,00	89,00
28	e25 e44	38,89	75,17	76,17	76,17	49,00	82,50
29	e26 e45	38,99	74,92	74,42	74,42	51,67	79,50
30	e25 e46	39,16	74,50	72,50	72,50	37,00	70,00
31	e26 e47	39,16	73,08	73,50	73,50	43,00	72,50
36	e20 e48	39,27	75,50	77,50	77,50	80,00	91,00
37	e20 e49	39,27	75,00	77,00	77,00	80,00	93,00
39	e25 e55	39,30	73,50	76,17	76,17	49,00	83,50
40	e26 e56	39,34	76,50	77,50	77,50	53,33	80,50

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
41	e25 e57	42,89	75,33	74,83	74,83	44,50	72,50
42	e26 e58	42,89	71,42	71,42	71,42	44,83	66,00
47	e20 e59	43,07	74,50	73,50	73,50	76,00	91,00
48	e20 e60	44,25	72,83	72,83	72,83	77,00	89,00
50	e25 e61	45,03	93,00	93,00	94,50	60,00	95,50
52	e25 e73	45,40	91,00	91,00	91,00	63,00	99,50
54	e25 e62	45,40	65,40	80,90	78,23	52,23	81,50
56	e26 e63	45,40	69,80	72,80	73,97	47,90	80,50
58	e25 e65	46,93	80,30	80,78	78,12	53,00	81,50
59	e26 e66	47,23	82,20	82,20	80,50	59,00	84,00
60	e25 e64	47,23	72,32	74,98	20,43	16,98	21,50
69	e76 e80	48,53	68,33	68,33	68,33	66,83	74,50
70	e77 e85	48,73	72,00	71,00	70,00	70,00	76,50
71	e76 e88	48,73	64,42	64,42	64,42	61,50	77,00
72	e77 e89	55,03	68,42	68,42	66,42	60,00	83,50
81	e76 e92	55,54	79,08	68,33	68,33	66,83	74,50
82	e77 e97	55,92	79,00	78,00	75,33	76,33	85,00
83	e76 e100	56,38	64,42	64,42	64,42	61,50	77,00
84	e77 e101	56,89	68,42	68,42	66,42	60,00	83,50
93	e76 e104	56,89	68,33	68,33	68,33	66,83	74,50
94	e77 e109	57,24	78,00	78,00	75,33	76,33	85,00
95	e76 e112	57,24	63,25	63,25	63,25	58,50	74,50
96	e77 e113	59,17	70,67	70,67	68,67	65,50	83,50
	Média	44,37	72,48	73,18	71,40	58,10	80,38

Quadro C.15 – Desempenho médio de métodos em nível de sistema considerando instâncias com 3 eventos e 2 alarmes de ruído

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
14	e7 e14 e22	44,21	70,50	71,33	71,33	70,83	77,17
13	e7 e14 e21	45,26	66,42	74,75	74,75	74,83	82,67
16	e8 e15 e24	48,26	58,45	62,42	62,42	59,50	81,67
15	e8 e15 e23	49,71	49,67	56,58	56,58	57,33	70,83

Diag.	Eventos	Ruído (%)	AG (%)	MAG (%)	BIP (%)	ED1 (%)	AED (%)
2	e2 e15 e27	51,19	55,58	63,92	63,92	44,33	67,50
1	e1 e15 e27	52,38	52,50	59,50	59,50	50,33	62,67
4	e4 e9 e19	53,51	59,33	62,33	62,33	56,50	79,50
9	e6 e17 e19	54,07	74,33	74,17	74,17	73,50	90,50
8	e6 e16 e19	54,29	73,33	73,83	73,83	79,00	78,50
3	e3 e9 e19	54,92	64,83	64,33	64,33	67,50	73,00
	Média	50,78	62,50	66,32	66,32	63,37	76,40

Quadro C.16 – Desempenho médio de métodos em nível de sistema considerando instâncias com 4 eventos e 2 alarmes de ruído

Diag.	Eventos	Ruído (%)	AG (%)	AG (%)	BIP (%)	ED1 (%)	AED (%)
51	e6 e9 e23 e67	35,98	69,75	70,75	70,58	68,00	98,00
21	e7 e14 e23 e28	38,65	56,17	57,00	57,00	59,67	87,00
43	e7 e14 e23 e50	38,81	53,92	56,00	56,00	61,67	89,83
32	e7 e14 e23 e39	38,88	52,33	55,58	55,58	58,00	82,83
22	e7 e14 e24 e30	38,93	48,62	55,70	55,70	62,67	82,83
44	e7 e14 e24 e52	38,93	47,20	56,20	56,20	63,67	82,83
33	e7 e14 e24 e41	39,05	58,17	55,50	55,50	56,83	85,33
57	e6 e9 e24 e69	39,18	69,67	68,33	68,50	67,17	96,50
55	e6 e9 e23 e68	39,46	65,00	66,00	65,50	61,00	95,50
45	e8 e15 e23 e51	42,88	49,58	51,17	51,17	54,17	75,83
23	e8 e15 e23 e29	43,17	58,87	60,17	60,17	62,50	84,50
34	e8 e15 e23 e40	43,17	58,20	60,17	60,17	62,50	84,50
35	e8 e15 e24 e42	43,78	56,50	56,75	56,75	58,08	81,00
24	e8 e15 e24 e31	44,38	54,45	56,62	56,62	57,00	82,00
46	e8 e15 e24 e53	44,38	53,20	56,62	56,62	57,00	81,00
53	e6 e9 e23 e74	48,56	66,33	67,33	67,33	62,17	99,00
	Média	41,14	57,37	59,37	59,34	60,76	86,78

APÊNDICE D – Topologias pós-falta do sistema da Eletrosul

Figura D.1 – Topologia pós-falta da instância 1 de Leão, Pereira e Mantovani (2010)

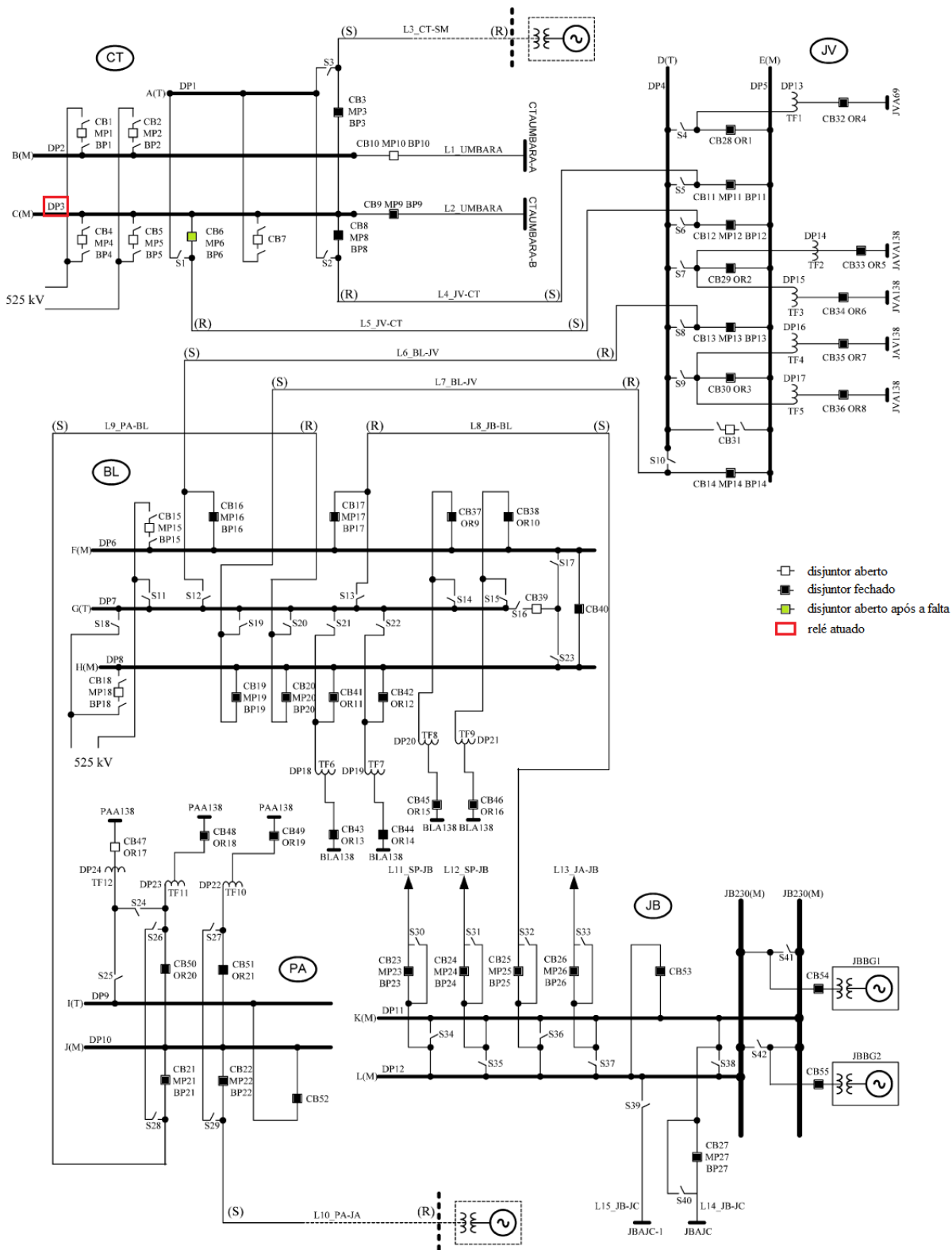


Figura D.2 – Topologia pós-falta da instância 2 de Leão, Pereira e Mantovani (2010)

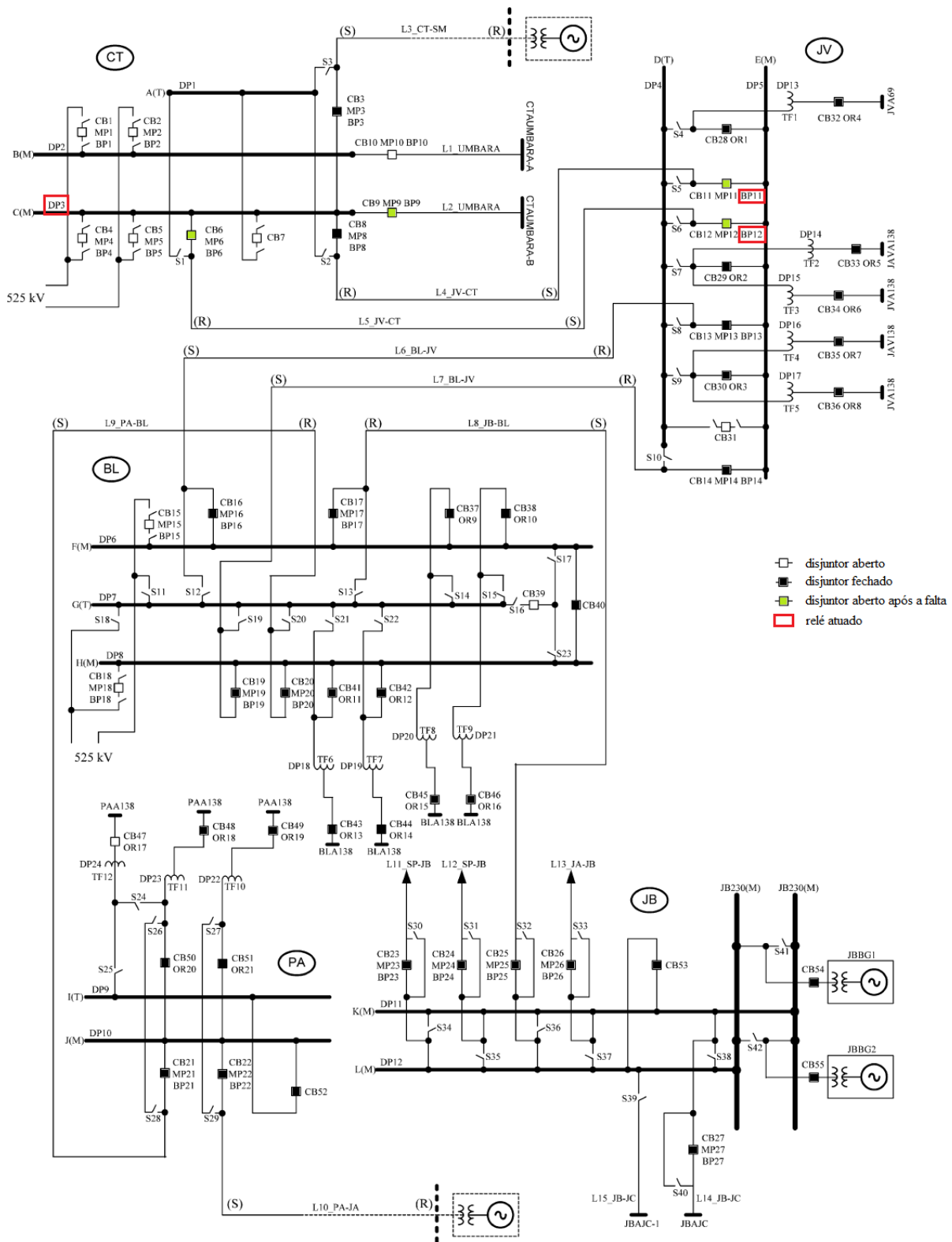


Figura D.3 – Topologia pós-falta da instância 3 de Leão, Pereira e Mantovani (2010)

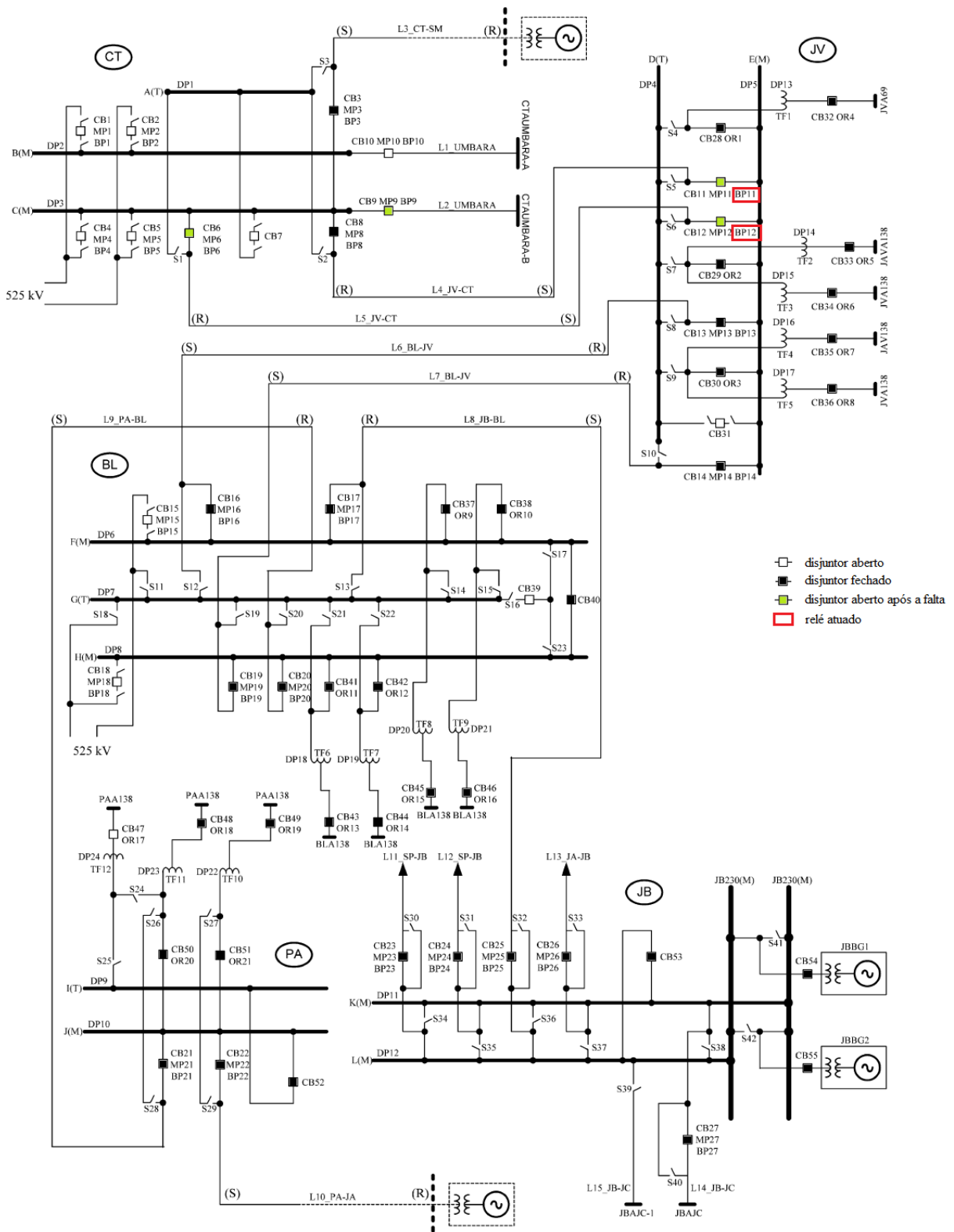


Figura D.4 – Topologia pós-falta da instância 4 de Leão, Pereira e Mantovani (2010)

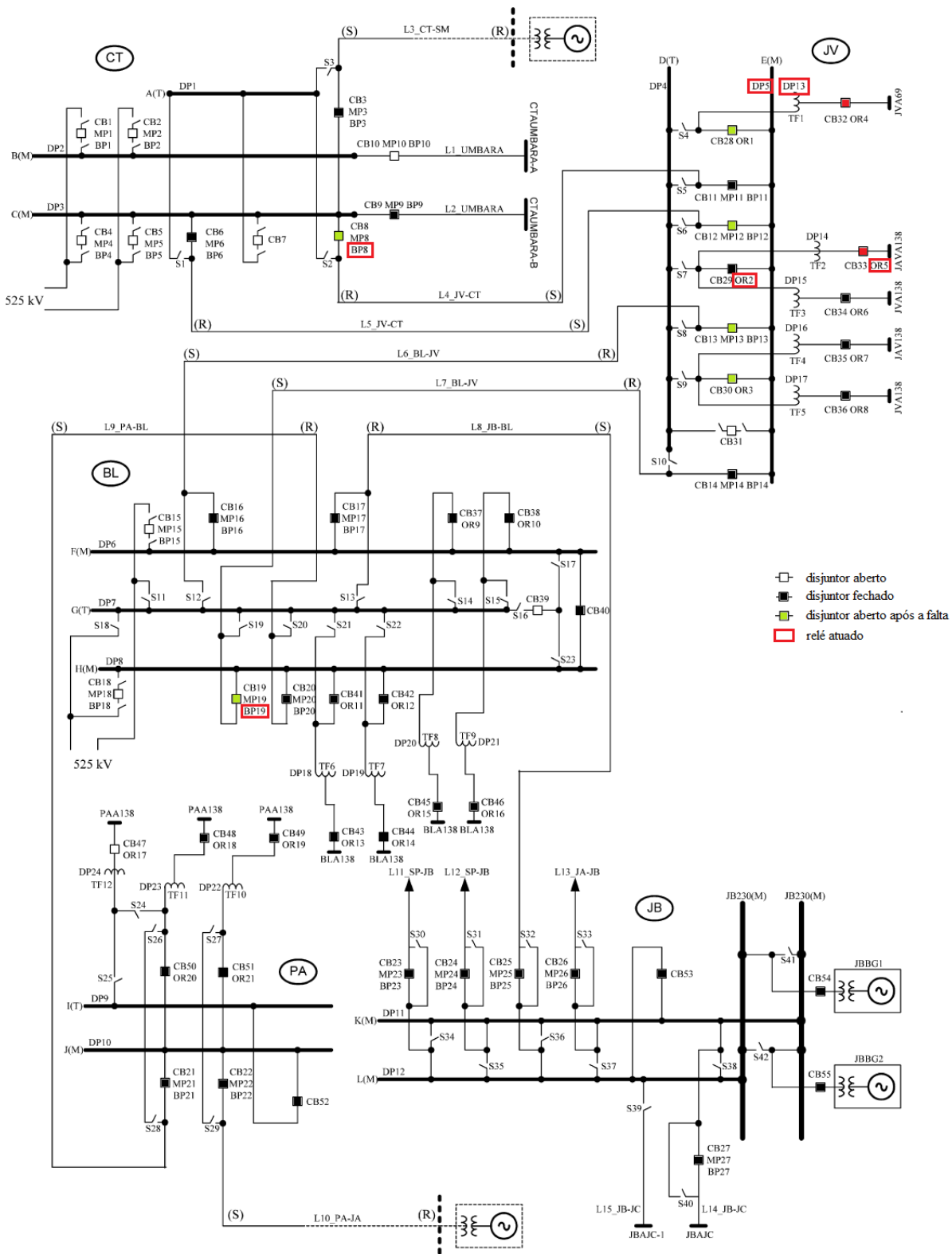


Figura D.5 – Topologia pós-falta da instância 5 de Leão, Pereira e Mantovani (2010)

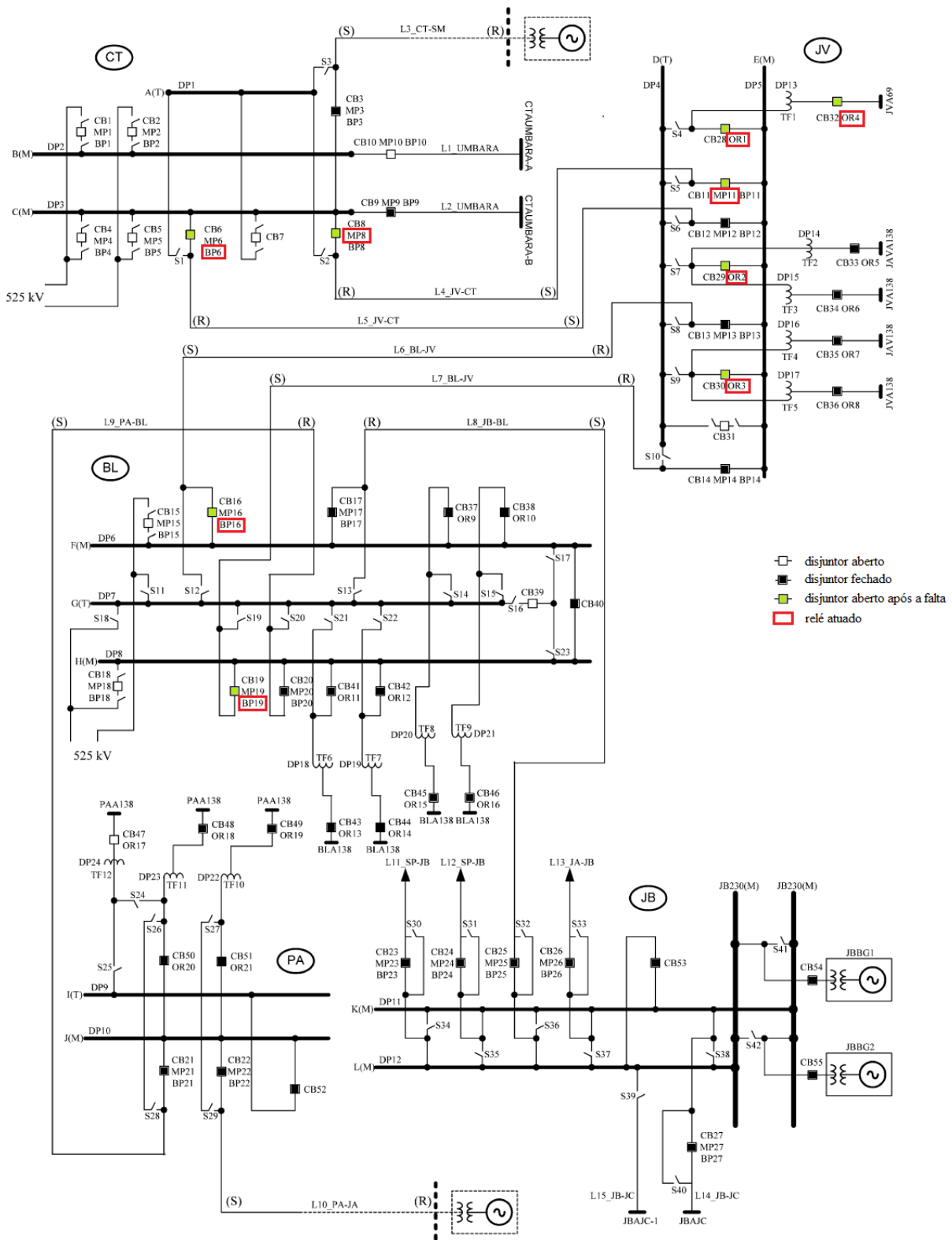


Figura D.6 – Topologia pós-falta da instância 6 de Leão, Pereira e Mantovani (2010)

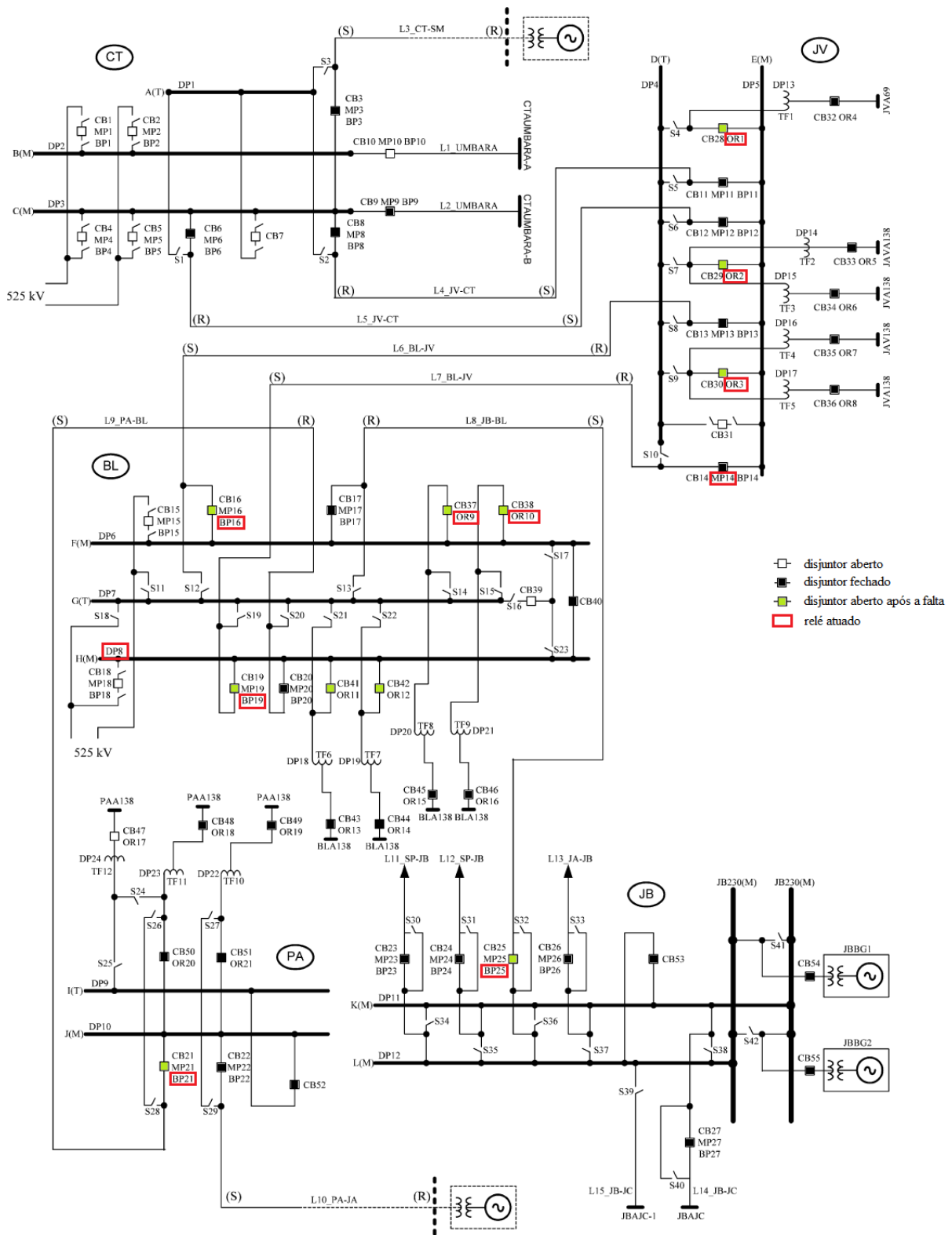


Figura D.7 – Topologia pós-falta da instância 7 de Leão, Pereira e Mantovani (2010)

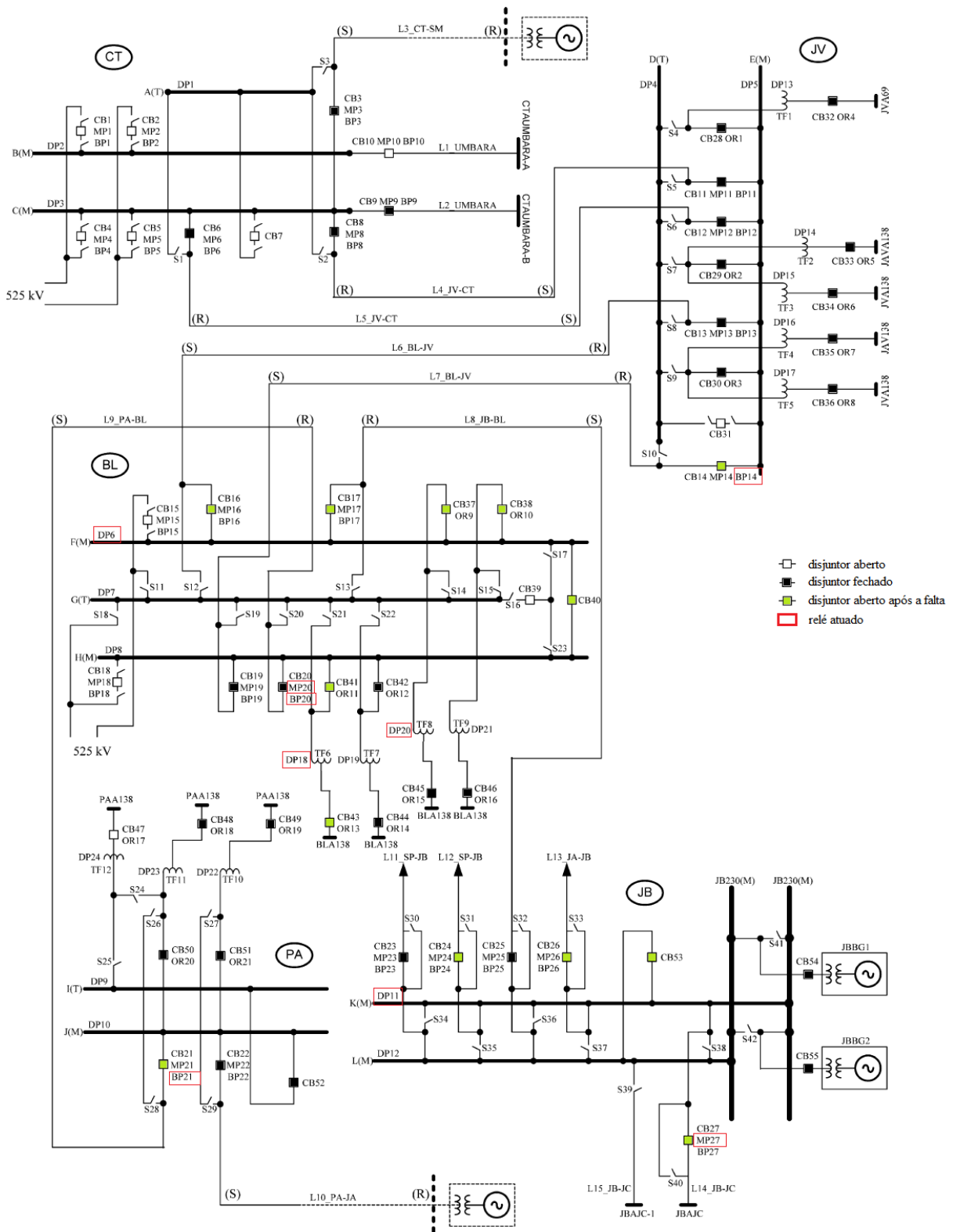


Figura D.8 – Topologia pós-falta da instância 8 de Leão, Pereira e Mantovani (2010)

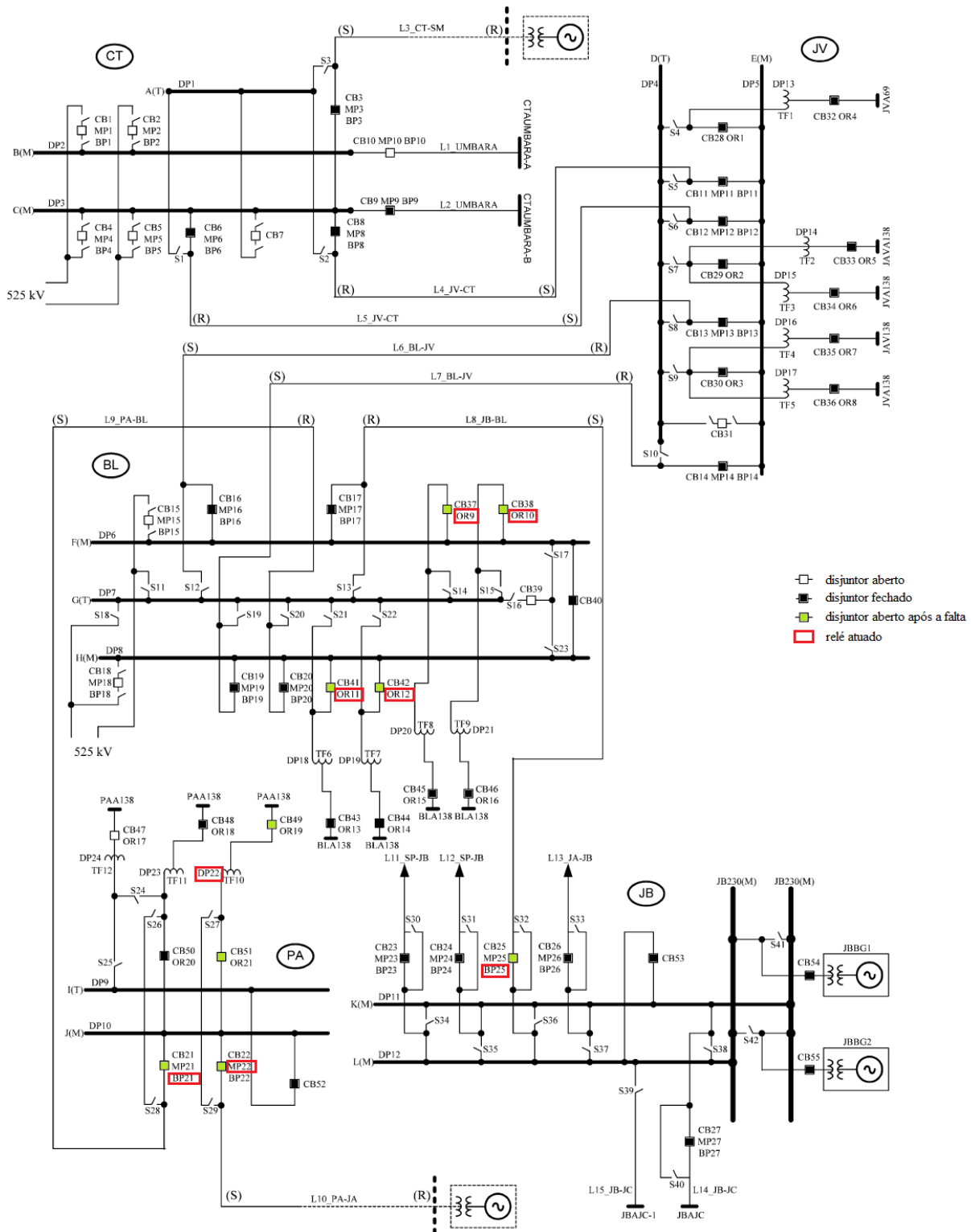


Figura D.9 – Topologia pós-falta da instância 9 de Leão, Pereira e Mantovani (2010)

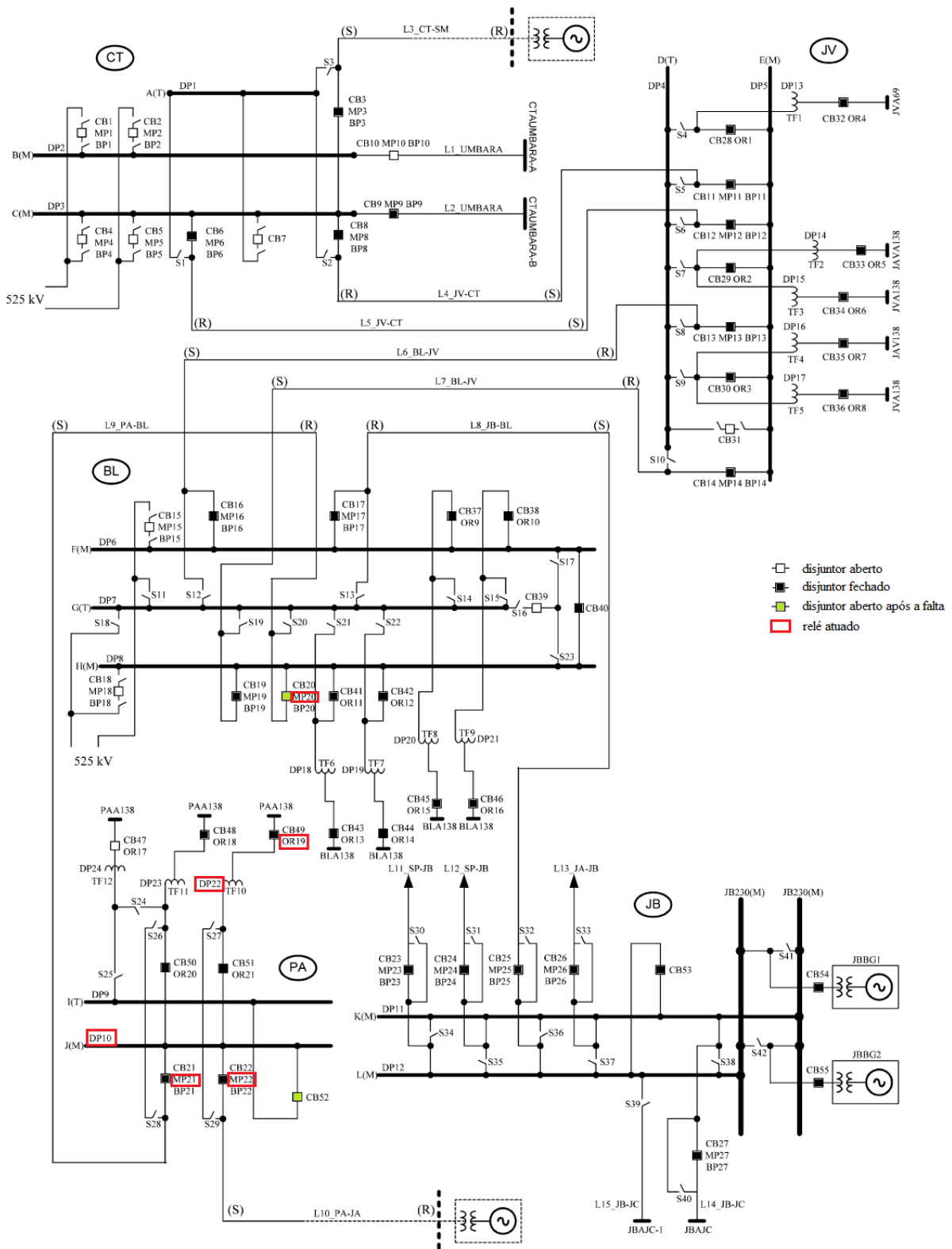
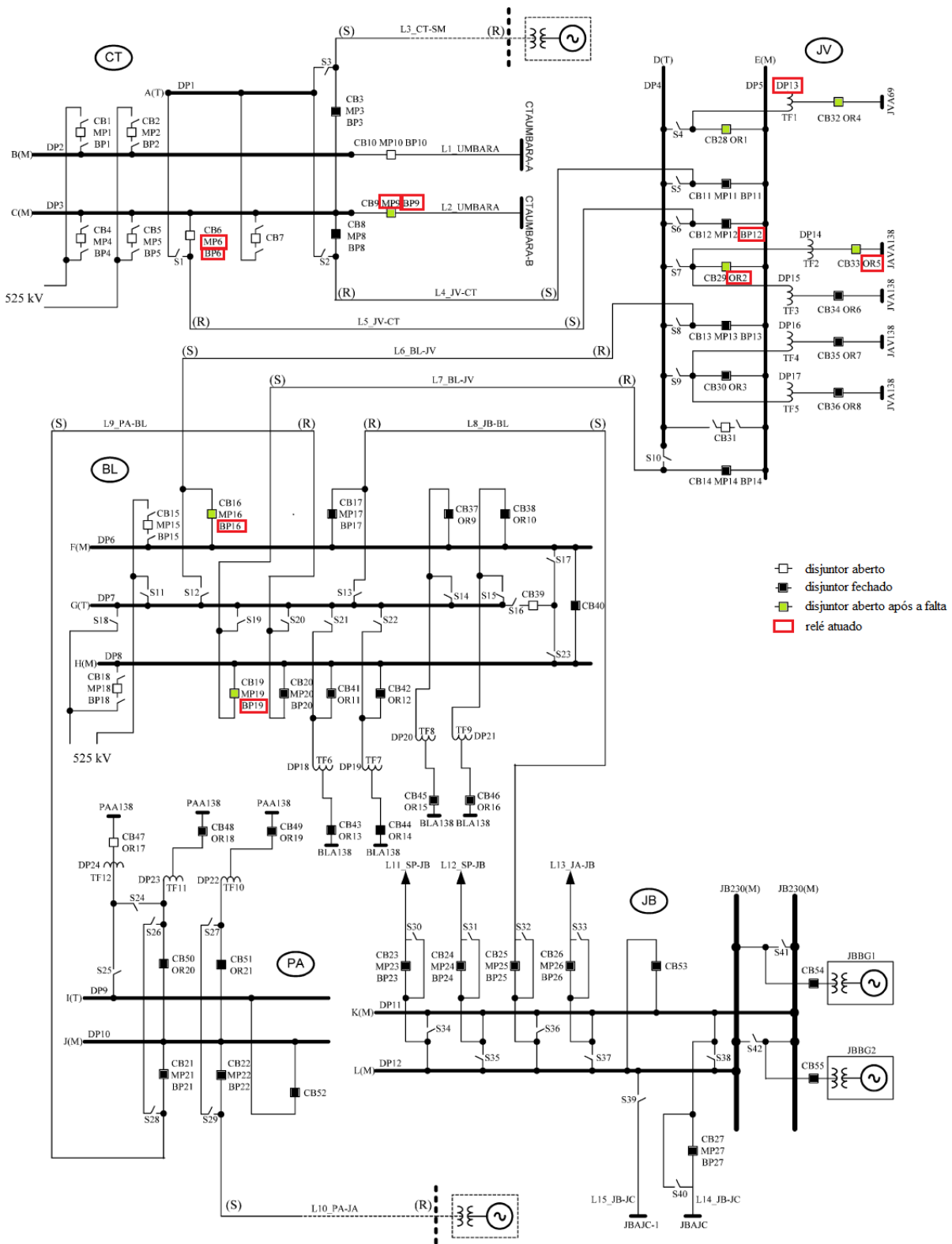


Figura D.10 – Topologia pós-falta da instância 10 de Leão, Pereira e Mantovani (2010)



APÊNDICE E – Topologias pós-falta do sistema da CEEE-GT

Figura E.1 – Topologia pós-falta no gerador G9 (teste 2)

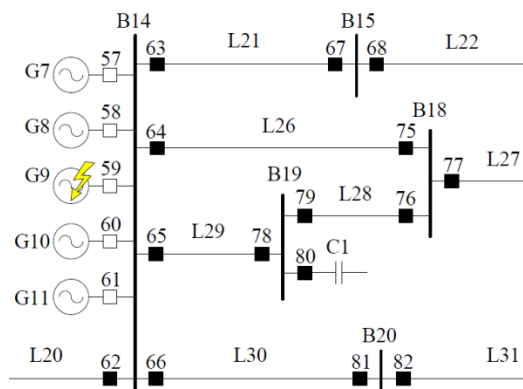


Figura E.2 – Topologia pós-falta na barra B2 (teste 3)

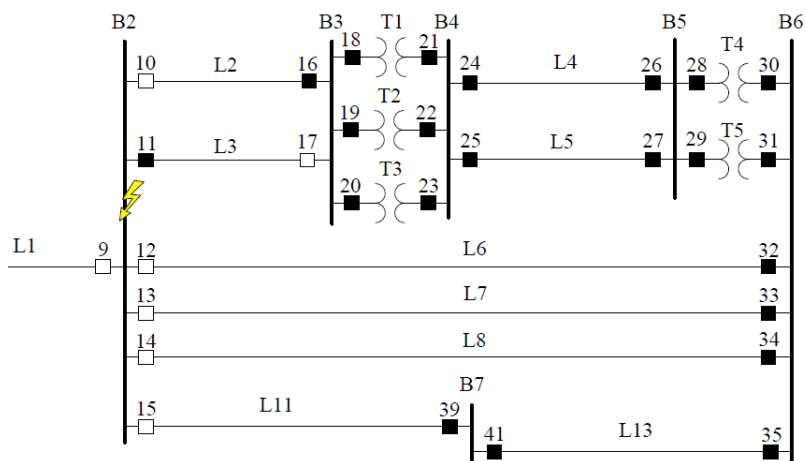


Figura E.3 – Topologia pós-falta no banco de capacitores C1 (teste 4)

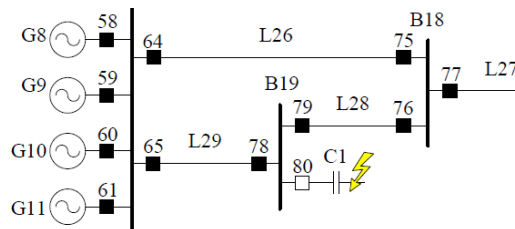


Figura E.4 – Topologia pós-falta no banco de capacitores C1 (teste 5)

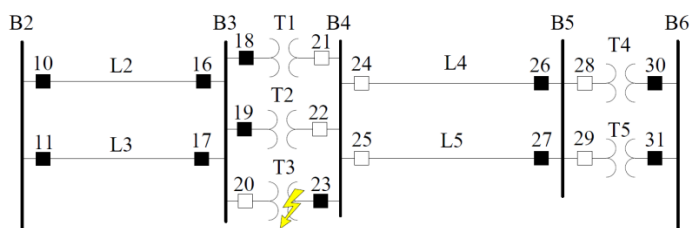
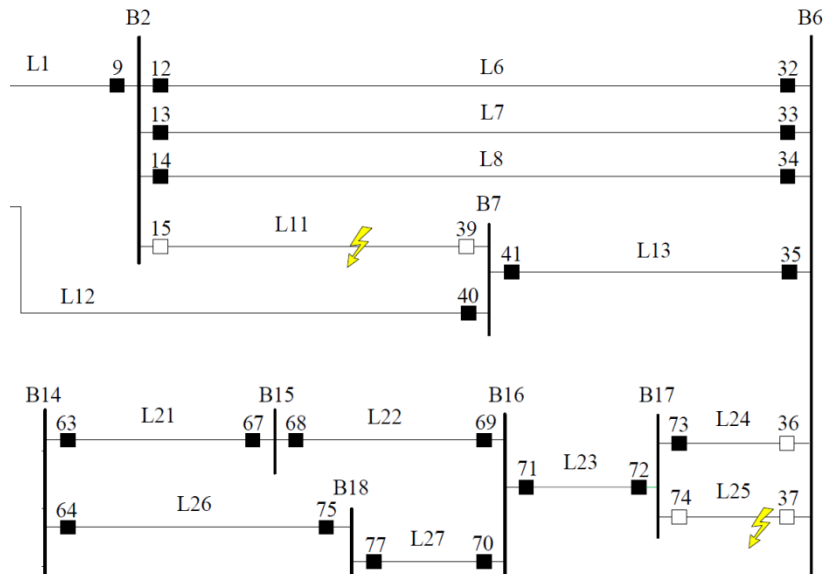


Figura E.5 – Topologia pós-faltas nas linhas L11 e L25 (teste 6)



ANEXO A – Funções de proteção conforme IEEE C37.2 Std.

21	Relé de distância
21G	Relé de distância do gerador
27	Relé de subtensão
40	Relé contra perda de excitação de campo
46	Relé contra desbalanço de corrente de sequência negativa
50	Relé de sobrecorrente instantâneo
51	Relé de sobrecorrente temporizado de fase
51N	Relé de sobrecorrente temporizado de neutro
59	Relé de sobretensão
60	Relé de desbalanço de tensão
61	Relé de desbalanço de corrente
62BF	(Lógica de falha de disjuntor
63	Relé Buchholz
63C	Relé de pressão do comutador de <i>tap</i> sob carga
64R	Relé terra-rotor
64S	Relé terra-estator
67N	Relé de sobrecorrente direcional de neutro
79	Relé de religamento automático
81	Relé de sub/sobrefrequência
86	Relé de bloqueio
86BF	Lógica de falha de disjuntor
87	Relé diferencial
87G	Relé diferencial do gerador
87GT	Relé diferencial do grupo gerador-transformador
87L	Relé diferencial de linha