UNIVERSIDADE FEDERAL FLUMINENSE

YONA LOPES

ARES: UM ARCABOUÇO PARA COMUNICAÇÃO AUTONÔMICA E RESILIENTE EM REDES ELÉTRICAS INTELIGENTES

NITERÓI

2019

UNIVERSIDADE FEDERAL FLUMINENSE

YONA LOPES

ARES: UM ARCABOUÇO PARA COMUNICAÇÃO AUTONÔMICA E RESILIENTE EM REDES ELÉTRICAS INTELIGENTES

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

Orientadora:
DÉBORA CHRISTINA MUCHALUAT SAADE

Co-orientadora:
NATALIA CASTRO FERNANDES

NITERÓI

2019

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

L864a Lopes, Yona
ARES : Um Arcabouço para Comunicação Autonômica e Resiliente em Redes Elétricas Inteligentes / Yona Lopes ; Débora Christina Muchaluat-Saade, orientadora ; Natalia Castro Fernandes, coorientadora. Niterói, 2019.
232 f. : il.

Tese (doutorado)-Universidade Federal Fluminense, Niterói, 2019.

DOI: http://dx.doi.org/10.22409/PGC.2019.d.11132044782

1. Rede elétrica. 2. Rede definida por software. 3. Rede de comunicação de computadores. 4. Automação. 5. Produção intelectual. I. Muchaluat-Saade, Débora Christina, orientadora. II. Castro Fernandes, Natalia, coorientadora. III. Universidade Federal Fluminense. Instituto de Computação. IV. Título.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

YONA LOPES

ARES: UM ARCABOUÇO PARA COMUNICAÇÃO AUTONÔMICA E RESILIENTE EM REDES ELÉTRICAS INTELIGENTES

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

Aprovada em 11 de março de 2019.

BANCA EXAMINADORA

Profª. DÉBORA CHRISTINA MUCHALUAT SAADE, D.Sc. – Orientadora, UFF

Profª. NATALIA CASTRO FERNANDES, D.Sc. – Coorientadora, UFF

Prof. CÉLIO VINICIUS NEVES DE ALBUQUERQUE, Ph.D. – UFF

Prof. MILTON BROWN DO COUTO FILHO, D.Sc. – UFF

Profª. FLÁVIA COIMBRA DELICATO, D.Sc. – UFRJ

Prof. MARCELO GONÇALVES RUBINSTEIN, D.Sc – UERJ

Niterói

2019

À minha mãe.
À minha família.

Agradecimentos

Agradeço, inicialmente à minha família, especialmente à minha mãe, que mesmo diante de todas as dificuldades não deixou, em nenhum momento, que eu perdesse o gosto pela educação nem a sede por conhecimento. Obrigada por tudo, mãe.

Às minhas orientadoras, professoras Débora e Natalia, pelo incentivo constante, pelas valiosas contribuições e ensinamentos, e pelo excelente convívio durante todos os anos de trabalho juntas. Agradeço todo o apoio profissional incontestável, a liberdade que me foi concedida para que eu fizesse o que acredito e, principalmente, pelo apoio pessoal no momento que mais precisei. Se eu tive garra para seguir, muito eu devo a vocês. Mais do que orientadoras, vocês são exemplos de profissionais, pessoas, e, acima de tudo, amigas. Agradeço também a professora Katia Obraczka por todo o suporte concedido enquanto estive no período de Doutorado sanduíche, na *University of California*, Santa Cruz. Suas dicas, sempre valiosas, sua visão e seu cuidado são motivadores. Obrigada por tudo. Aos professores da banca, muito obrigada pela pronta disponibilidade, apoio e colaboração.

Aos amigos do laboratório MídiaCom e do Instituto de Computação da UFF, pelo incentivo e interesse constantes, pelo acolhimento, debates, trocas, colaborações, risadas e cafés. Com certeza, fizeram essa caminhada mais leve. Em especial ao amigo Daniel, por cada tempo despendido em folhas e mais folhas de estudos e modelagem, por cada conversa, apoio e gargalhada.

Aos meus amigos que passaram por anos de quase total ausência, mas entendem, como ninguém, o significado da palavra *deadline*, muito obrigada. Aos amigos que ganhei na Califórnia, não tenho nem palavras para agradecer. Mais do que uma experiência profissional, foi uma experiência de vida. Aos meus alunos, que são a minha verdadeira inspiração em seguir a carreira docente, agradeço pela credibilidade, incentivo e motivação constantes.

Agradeço aos órgãos de fomento à pesquisa FAPERJ, CAPES e CNPq, a empresa TAESA e ao programa de PD ANEEL (PD-07130-0053/2018), pelos recursos financeiros recebidos. Também à empresa *Schweitzer Engineering Laboratories* (SEL), pelo apoio e equipamentos concedidos para testes.

Por fim, agradeço a todos que, embora não estejam citados aqui, contribuíram para a minha formação acadêmica e profissional, me incentivaram e apoiaram.

"O que sabemos não é muito. O que não sabemos é imenso."
"O peso da evidência de uma afirmação extraordinária deve ser proporcional à sua estranheza."
(Pierre Simon Laplace)

Resumo

Com as redes elétricas inteligentes, os dispositivos do sistema elétrico de potência se tornam multifuncionais e passam a se comunicar de forma bidirecional e em tempo real. Para atender a essa nova demanda, os sistemas de supervisão e controle precisam evoluir e incorporar novas funcionalidades, permitindo maior dinamismo e flexibilidade para acompanhar a escala das redes elétricas inteligentes. A inserção de fontes de energia renováveis traz novas possibilidades, e, também, muitos desafios. Nesse novo cenário, a rede de comunicação precisa ser ainda mais confiável, evitando que falhas de comunicação interfiram nos mecanismos de proteção e controle da rede elétrica. As propostas que exploram o novo paradigma das redes elétricas inteligentes dependem de sistemas de comunicação mais flexíveis e dinâmicos, com interação em tempo real, sendo este, um dos principais desafios da área.

Nesta tese, os desafios relacionados às redes de comunicação para o sistema elétrico são identificados e discutidos. Com base neste levantamento, propõe-se um *framework*, intitulado ARES (*Autonomic and Resilient Communication framEwork for Smart grids*), para dar suporte de comunicação às novas aplicações de energia. O ARES objetiva permitir que a capacidade multifuncional dos dispositivos seja explorada e que as aplicações de energia possam contar com uma rede de comunicação mais dinâmica e que atenda às restrições temporais rígidas impostas pelo novos sistemas de proteção baseados na norma IEC 61850. O *framework* permite que os serviços de supervisão e controle configurem dinamicamente a rede, permitindo o desenvolvimento de uma nova geração de aplicações de energia que possam agir sobre a rede de comunicação em tempo real. A norma IEC 61850 foi estendida para permitir que novas implementações baseadas na prioridade do dispositivo físico para o sistema elétrico e nas suas possíveis funções, variáveis ou não ao longo do tempo, sejam realizadas. O ARES é baseado em SDN (*Software Defined Network*), e no modelo de informação da norma IEC 61850.

A implementação do *framework* ARES mostrou sua viabilidade prática, de forma a entregar uma rede mais dinâmica e flexível, permitindo que um novo SCADA, intitulado SCADA-NG, possa ser construído com aplicações de energia mais inteligentes e mais capazes. A resiliência de uma rede para teleproteção de subestações baseada no *framework* também foi avaliada, mostrando que a solução atende aos requisitos impostos pelo setor de energia elétrica para o estudo de caso apresentado.

Palavras-chave: *Software Defined Network* (SDN), Autoconfiguração, Resiliência, SCADA-NG, ARES.

Abstract

In a smart grid solution, power system devices become multifunctional and require bidirectional and real-time communication. To support this new demand, supervisory and control systems need to improve its functionalities, allowing greater flexibility to support the smart grid scale. Distributed energy resources penetration brings new possibilities, and also new challenges. Communication networks need to be even more reliable, in order to avoid disturbs on power systems control and protection due to communication failures. New smart grid proposals rely on a flexible communication system, that has constant changes, with real-time interaction, which is its main challenge.

This thesis addresses the challenges of smart grid communication networks. The framework, called ARES, aims at supporting new energy applications that are communication-based. ARES intends to engage new capabilities for enabling more intelligent energy applications that could use a dynamic communication network that meets power system time requirements. The framework allows the deployment of a new generation of energy applications which can provision dynamically the communication network in real time. Also, this thesis extends the IEC 61850 standard to enable new implementations based on physical device priority and its function, which can be dynamically changed. ARES is SDN and IEC 61850 based.

ARES implementation shows that it is viable in practice, enabling a more flexible and dynamic network, supporting the next generation of SCADA systems, composed of new energy applications that are more capable and intelligent. Teleprotection network resilience of a substation based on ARES was evaluated, showing that this proposal meets the electrical power systems requirements.

Palavras-chave: *Software Defined Network* (SDN), Autoconfiguration, Resilience, SCADA-NG, ARES.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

AD Automação da Distribuição 25

AMI *Advanced Metering Infrastructure* 1

API *Application Programming Interface* 6

ARES *Autonomic and Resilient communication framEwork for Smart grids* . . 3

BPDU *Bridge Protocol Data Units* 200

BRCB *Buffered Report Control Block* 121

CFI *Canonical Format Indicator* 53

CID *Configured IED Description* 42

CIGRE Comitê Internacional de Produção e Transmissão de Energia Elétrica 82

CIM *Computer Integrated Manufacturing* 46

CIP *Critical Infrastructure Protection* 82

CLP Controlador Lógico Programável 90

CPP *Critical Peak Pricing* 11

CS *Charging Station* 2

DA *Data Attributes* 38

DANH *Doubly Attached Node with HSR Protocol* 206

DANP *Double attached node implementing PRP* 202

DAP *Data Aggregation Point* 26

DCC *Data and Control Center* 2

DER *Distributed Energy Resources* 27

DNP3 *Distributed Network Protocol v.3* 78

DO *Data Objects* 38

DPL *Device Name Plate* 123

DR *Demand Response* 25

DRCS *DER controller status* 126

DSM *Demand Side Management* 25

EPRI *Electric Power Research Institute* 25

GD Geração Distribuída . . . 2
GMRP *GARP Multicast Registration Protocol* . . . 152
GoCB *GOOSE Control Block* . . . 121
GOOSE *Generic Object Oriented Substation Event* . . . 45
HSR *High-availability Seamless Redundancy* . . . 61
HTTP *HyperText Transfer Protocol* . . . 131
ICD *IED Capability Description* . . . 41
ICMP *Internet Control Message Protocol* . . . 135
IEC *International Electrotechnical Commission* . . . 36
IED *Intelligent Electronic Device* . . . 2
IETF *Internet Engineering Task Force* . . . 173
IP *Internet Protocol* . . . 93
JSON *JavaScript Object Notation* . . . 133
LAN *Local Area Network* . . . 140
LD *Logical Device* . . . 37
LLDP *Link Layer Discovery Protocol* . . . 93
LN *Logical Node* . . . 38
LPHD *Physical Device Information* . . . 127
LRE *Link Redundant Entity* . . . 203
LT Linhas de Transmissão . . . 138
MAC *Media Access Control* . . . 52
MCAA *Multicast Application Association* . . . 44
MMS *Manufacturing Message Specification* . . . 4
MPLS *Multiprotocol Label Switching* . . . 5
MSVCB *Multicast Sample Value Control Block* . . . 121
NAN *Neighborhood Area Network* . . . 27
NAT *Network Address Translation* . . . 68
NERC *North American Electric Reliability Corporation* . . . 82
NETCONF *Network Configuration* . . . 173
ONF *Open Networking Foundation* . . . 67
PCP *Priority Code Point* . . . 53
PG Progressão Geométrica . . . 134

PLC *Power Line Communications* 13
PMU *Phasor Measurement Unit* 80
PRP *Parallel Redundancy Protocol* 61
PTP *Precision Time Protocol* 141
QoS *Quality of Service* 3
RCT *Redundancy Check Trailer* 204
REST *Representational State Transfer* 130
RFC *Request for Comments* 173
RSTP *Rapid Spanning Tree Protocol* 61
RTP *Real Time Pricing* 11
SAN *Single Attached Nodes* 202
SAS Sistema de Automação de Subestações 36
SCADA-NG SCADA *Next Generation* 88
SCADA *Supervisory Control and Data Acquisition* 1
SCD *Substation Configuration Description* 42
SCL *Substation Configuration Language* 37
SDN *Software Defined Network* 5
SEL *Schweitzer Engineering Laboratories* 107
SEP Sistema Elétrico de Potência 10
SER *Sequential Events Recorder* 142
SONET *Synchronous Optical Network* 140
SSD *System Specification Description* 42
SSL *Secure Socket Layer* 68
STA *Spanning Tree Algorithm* 202
SV *Sampled Values* 45
TC Transformador de Corrente 21
TCAM *Ternary Content Addressable Memory* 68
TCI *Tag Control Information* 53
TCP *Transmission Control Protocol* 68
TOU *Time of Use* 11
TP Transformador de Potencial 21
TPAA *Two Party Application Association* 44

TPID *Tag Protocol Identifier* 53

URCB *Unbuffered Report Control Block* 121

URI *Uniform Resource Identifier* 132

USVCB *Unicast Sample Value Control Block* 121

VE Veículo Elétrico 1

VID *VLAN Identifier* 53

VLAN *Virtual Local Area Network* 52

WAN *Wide Area Network* 140

XML *eXtensible Markup Language* 41

Sumário

Capítulo 1

Introdução

Redes elétricas inteligentes, conhecidas como *smart grids*, trazem propostas inovadoras que mudam de forma profunda a maneira como a energia é provida desde a geração até os consumidores finais. A ideia consiste em aperfeiçoar os sistemas elétricos, com o auxílio de uma infraestrutura de comunicação eficiente, visando o aumento na qualidade e continuidade do fornecimento de energia. Dentre as novas propostas, destacam-se a geração de energia de forma distribuída, o amplo uso de fontes renováveis, o uso de carros elétricos, o uso de medidores inteligentes, entre outros. O consumidor passa a ser parte fundamental do funcionamento da rede elétrica, podendo incorporar também o papel de produtor de energia. Os medidores inteligentes localizados nas residências passam a gerar uma quantidade enorme de informação, que poderá ser usada para o gerenciamento e controle do sistema [184, 125, 151]. As redes elétricas inteligentes requerem um sistema supervisório inteligente para gerenciamento e monitoramento de processos, dispositivos automatizados, dispositivos de campo e medidores inteligentes. O sistema supervisório mais amplamente usado é chamado *Supervisory Control and Data Acquisition* (SCADA). Com a evolução para as redes elétricas inteligentes, o SCADA gerenciará também novos elementos inteligentes, tais como unidades de medição fasorial, relés inteligentes, novas fontes de geração de energia com utilização de fontes renováveis, armazenamento de energia, Veículo Elétricos (VEs), etc [62]. Com um alto grau de automação e inserção de fontes de energia renováveis, as redes elétricas inteligentes trazem benefícios não só para o consumidor, mas também para as concessionárias de energia e para o meio ambiente.

De acordo com o modelo conceitual do NIST (*National Institute of Standards and Technology*) [138], a rede elétrica inteligente é composta por domínios lógicos com agentes e dispositivos inteligentes que devem ser interligados. Nesse novo cenário, os dispositivos finais da rede, como os medidores, se tornam mais inteligentes e podem se comunicar diretamente com os centros de controle de dados através da *Advanced Metering Infrastructure* (AMI). De fato, a implantação da rede elétrica inteligente começa com uma inserção em massa de medidores inteligentes e da AMI, que são elementos chave neste cenário. A introdução de medidores inteligentes permite uma melhor compreensão da demanda e um

melhor controle do consumo de energia e da geração distribuída.

Além disso, o número de *Intelligent Electronic Device*s (IEDs) aumenta a fim de apoiar a automação de todo esse sistema. Em geral, a quantidade de dispositivos de automação, tais como medidores inteligentes e IEDs, e a quantidade de dados coletados a partir desses dispositivos, aumentam significativamente. A comunicação, que antes compreendia apenas parte do sistema, como as subestações e seus centros de controle, passa agora a englobar todo o sistema, incluindo o consumidor. Ademais, a rede elétrica inteligente traz um enorme crescimento no volume de dados que deve ser gerenciado e controlado e depende de uma sofisticada infraestrutura de redes de comunicação para dar suporte à comunicação entre os dispositivos inteligentes que monitoram a rede e funcionam como atuadores. Nesse contexto, o sistema supervisório SCADA passa a ser uma alternativa para supervisão em outras partes do sistema que vão além das subestações. Alguns exemplos de dispositivos que precisam se comunicar neste cenário são:

- IEDs: os dispositivos das subestações que trocam informações com o supervisório, recebem comandos, reportam mudanças de valores para outros IEDs, dentre muitas outras características;
- medidores inteligentes: capazes de enviar medidas para o *Data and Control Center* (DCC) e de receber comandos para corte e religamento de energia. Além disso, fornecem uma maneira econômica de medir essa informação, permitindo que o preço seja introduzido com base na hora do dia [114];
- medidores da Geração Distribuída (GD): monitoram o desempenho do sistema de energia, incluindo o uso de energia e a qualidade de energia (medindo harmônicos, desvio de frequência, afundamento/elevação de tensão e transientes das *microgrids* conectadas). Além disso, o medidor pode ser utilizado para fornecer informações que permitam que o SCADA tome decisões para realizar um controle mais eficiente e/ou economize energia [114]. Nesse contexto, as redes de distribuição passivas tradicionais estão sendo transformadas em redes de distribuição ativas, e com isso, o gerenciamento da rede de distribuição torna-se mais complexo [161];
- medidores das estações de recarga (*Charging Station* (CS)) de VEs: Os CSs possuem medidores que enviam as informações relacionadas às cargas e descargas de veículos, agendamentos, dentre outros.

De forma geral, verifica-se que a comunicação é necessária em todos os domínios, independentemente da função que o dispositivo exerça. Por essa razão, nesta tese, todos os dispositivos finais são intitulados IEDs, já que exercem múltiplas funções e são dotados da habilidade de se comunicar. Ressalta-se que, levando em conta esse ponto de vista, tanto a estação de recarga de veículos elétricos quanto os medidores inteligentes, ou ainda os próprios relés, são considerados dispositivos eletrônicos inteligentes (IEDs).

Com o levantamento do estado da arte em redes elétricas inteligentes (Seção 3.5), cinco desafios foram mapeados para implementação das redes elétricas inteligentes:

- Dispositivos finais multifuncionais;
- Provimento de *Quality of Service* (QoS);
- Configuração e provisionamento da rede de comunicação;
- Configuração dos sistemas supervisórios;
- Modernização dos sistemas supervisórios.

Estes cinco desafios são detalhados no Capítulo 2, que apresenta em detalhes a motivação para o desenvolvimento desta tese.

1.1 Objetivos

O objetivo principal desta tese de doutorado é a proposta de um arcabouço (do inglês, *framework*) para comunicação autonômica e resiliente para redes elétricas inteligentes, o *Autonomic and Resilient communication framEwork for Smart grids* (ARES). Para tanto, foram levantados os principais problemas de comunicação nas redes elétricas inteligentes (Capítulo 2) para proposta de um conjunto de módulos que solucionem esses problemas, respeitando e mantendo compatibilidade com os principais padrões em uso.

O ARES permite a implementação de três novos serviços no sistema supervisório. O primeiro é a identificação dinâmica de dispositivos que podem ser mapeados automaticamente pelo plano de controle ARES. O mapeamento contém tanto informações de rede, como endereços e prioridades, como características do dispositivo, como fornecedor e versão do *firmware*. Ressalta-se que o mapeamento só deve ser realizado após a implementação de políticas de segurança para restringir o acesso indevido. O segundo é o provisionamento dinâmico e em tempo real dos enlaces de comunicação. O provisionamento é realizado por fluxo* e de forma individual, de forma que apenas determinado fluxo ativo (com determinado destino, e prioridade, por exemplo) possa ser provisionado. Fluxos configurados porém inativos, não são configurados. O terceiro serviço permite que notificações da rede de comunicação sejam enviadas para o supervisório, informando, por exemplo, quando um enlace por onde determinado serviço passa sofreu alguma sobrecarga ou reconfiguração. Com esses serviços, uma nova geração de aplicações de energia pode ser desenvolvida de forma a agir sobre a rede de comunicação em tempo real e de forma mais inteligente. Da mesma forma, a implementação das aplicações de energia já propostas na literatura para

*Nesta tese, o termo "fluxo de comunicação" será utilizado no texto em sua forma reduzida, sendo utilizada apenas a palavra "fluxo".

as redes elétricas inteligentes pode ser efetivamente realizada. O provimento de QoS é facilitado, e a configuração da rede de comunicação e dos sistemas de supervisão deixam de ser excessivamente manuais (alguns dos problemas discutidos no Capítulo 2) e passam a ser mais autonômicos.

Esta tese introduz o termo SCADA-NG (*Next-Generation*) para esta nova geração do sistema SCADA, que depende diretamente dos serviços oferecidos pelo ARES. Da mesma forma, o ARES notifica o SCADA-NG em tempo real sobre todas as alterações observadas na rede e novos dispositivos, inclusive as alterações de funções que são reportadas para o SCADA-NG dinamicamente. Isto proporciona escalabilidade e simplicidade, porque a rede se torna autonômica, permitindo a conexão de dispositivos finais sem a configuração manual desse dispositivo e da rede. A implementação do ARES aperfeiçoa o sistema SCADA tradicional e as redes SCADA. Ressalta-se, no entanto, que o desenvolvimento do SCADA-NG não é escopo deste trabalho, mas sim o *framework* de comunicação que o torna possível, e resolve os problemas indicados no Capítulo 2.

Dentro do contexto para provimento de comunicação no *framework* ARES, objetiva-se dar meios para uma redução da inundação de mensagens de proteção e controle, que são realizadas com MAC *multicast*, e uma comunicação resiliente a falhas. Nesse sentido, a rede de comunicação é provisionada de acordo com cada serviço, sem inundações desnecessárias e, sempre que possível, provendo caminhos secundários. Para redução da inundação, o ARES prevê módulos para calcular e definir árvores *multicast* de camada dois de forma a enviar as mensagens apenas para as portas de interesse, reduzindo o congestionamento dos enlaces. Também com este objetivo, o ARES apenas provisiona enlaces de fluxos necessários e ativos para uso naquele sistema, evitando o tráfego de mensagens desnecessárias, como acontece atualmente em subestações de energia. Ressalta-se que, este comportamento com o provisionamento por fluxos de forma individual e específica, também diminui a vulnerabilidade da rede se comparada com as redes tradicionais atuais. Isto ocorre pois, o acesso a rede é dificultado quando comparado as redes tradicionais.

Com relação a resiliência, mesmo em caso de falha na rede de comunicação, a comutação para o caminho *backup* ocorre sem grande interferência na latência de comunicação exigida para aplicações críticas. Esta recuperação de falhas também inclui o registro no sistema supervisório SCADA-NG de todas as falhas ocorridas com a descrição da falha que ocorreu e não depende de comunicação reativa com o controlador.

Após a análise de requisitos e uma pesquisa intensa dos principais protocolos usados no SCADA para dar suporte às aplicações de energia de nova geração, foi verificado que a modelagem da norma IEC 61850 [85] e os seus serviços [86] mapeados no protocolo *Manufacturing Message Specification* (MMS) [3] atendiam aos requisitos impostos pelas redes elétricas inteligentes. No entanto, para tanto, foi necessária a extensão na modelagem da norma IEC 61850 e uma mudança no protocolo MMS, permitida pela ISO 9506 [3]. A extensão deste modelo, mantendo a compatibilidade com os sistemas atuais, também é

objetivo desta tese.

A rede definida por software (*Software Defined Network* (SDN)) foi escolhida para servir como base para a solução de comunicação do *framework* proposto, mais especificamente o OpenFlow [133].

A ideia consiste na separação do plano de controle da rede de comunicação do plano de encaminhamento de dados de forma a permitir mais programabilidade e autonomia. Devido a visão unificada da rede, a implementação de novos algoritmos, métodos e a configuração e a gestão da rede de comunicação se tornam mais flexíveis e orientados às necessidades de cada sistema.

O OpenFlow [133], proposto por Stanford, é a mais popular plataforma SDN. Foi amplamente adotada na indústria para uso em *data centers* e já conta com produtos para uso em subestações de energia. É um padrão promissor que permite controlar o fluxo de comunicação de cada tráfego da rede, escolhendo as ações que devem ser tomadas e o processamento que o tráfego recebe independente de camadas.

Desta forma, o uso do OpenFlow permite que o tráfego da rede elétrica inteligente seja tratado de acordo com suas caraterísticas e requisitos de QoS específicos. Além disso, abordagens tradicionais utilizadas no setor elétrico, como por exemplo *Multiprotocol Label Switching* (MPLS), exigem que os equipamentos sejam reconfigurados a cada vez que é adicionado um novo serviço, resultando na interrupção dos serviços [158]. Assim, a alternativa de uso de SDN e do OpenFlow se mostra promissora já que o *framework* proposto visa o provisionamento dinâmico e em tempo real dos fluxos de comunicação, de forma transparente para os outros serviços. Os principais conceitos de SDN e do OpenFlow são descritos no Capítulo 4.

1.2 Contribuições Esperadas

A principal contribuição desta tese de doutorado é o *framework* ARES. O ARES contribui com o avanço do estado da arte oferecendo:

1. Uma solução para comunicação em *smart grids*, baseada em SDN, que:
   (a) propicie configuração e gerenciamento mais eficientes da rede de comunicação;
   (b) respeite os requisitos de latência na comunicação exigidos para proteção e controle da rede elétrica;
   (c) recupere a rede de comunicação em caso de falha de forma transparente para os dispositivos e em um tempo que permita que a latência da rede se mantenha dentro dos limiares exigidos;
   (d) crie pró-ativamente e dinamicamente árvores *multicast* de camada de enlace para o envio das mensagens IEC 61850 de restrição temporal rígida;

(e) permita que apenas dispositivos com acesso autorizado possam participar da comunicação;

(f) permita que apenas o fluxo necessário esteja sendo utilizado na rede naquele momento;

(g) garanta interoperabilidade permitindo que a modelagem e os protocolos usados em subestações possam ser usados em *microgrids*, medidores inteligentes, etc.

2. Uma *Application Programming Interface* (API) que facilita o desenvolvimento de uma nova geração de sistemas supervisórios para a rede elétrica, permitindo que:

   (a) os dispositivos de energia inteligentes, desde que tenham acesso permitido, possam ser descobertos e mapeados no supervisório automaticamente assim que instalados;

   (b) as aplicações de energia possam fazer pedidos de provisionamento de rede de acordo com as necessidades exigidas, inclusive após a mudança de perfil realizada por equipamentos em tempo real, permitindo que as aplicações dinamicamente modifiquem a rede de comunicação;

   (c) as falhas de comunicação sejam reportadas para o SCADA-NG, informando qual serviço foi afetado por aquela falha e qual o tipo de falha que ocorreu.

3. A extensão da modelagem da norma IEC 61850 de forma a permitir que, com pequenas modificações, novas aplicações de energia sejam criadas.

   (a) os equipamentos multifuncionais possam reportar uma mudança de comportamento/função automaticamente para o supervisório;

   (b) informações da rede de comunicação, como prioridade do dispositivo, prioridade do fluxo e tipo de mensagem possam ser enviadas para o SCADA, permitindo que o mesmo possa provisionar os enlaces de acordo com a QoS exigida pela aplicação;

   (c) informações sobre o fluxo estar ativo ou não possam ser enviada ou coletadas, de forma que a API possa usar essa informação nas aplicações de energia e provisionar o enlace ou ainda desativar e ativar fluxos sob demanda.

Além disso, o ARES é transparente para dispositivos finais, não requerendo qualquer modificação de *hardware* ou *software*, mantendo a compatibilidade com dispositivos de medição e atuação legados. A condição para implementação da proposta em totalidade é relacionada ao uso da Norma IEC 61850, já utilizada para automação do sistema elétrico, e dispositivos SDN na rede de comunicação.

Ressalta-se que outra importante contribuição desta tese é a análise de requisitos de comunicação realizada de forma a compreender uma solução que possa de fato ser implementada na prática para garantir que os requisitos e as necessidades reais de comunicação para o sistema elétrico de potência sejam alcançados.

O ARES foi implementado em três cenários para prova de conceito e avaliação. Foram realizados testes de funcionalidade e desempenho, que mostraram que a proposta é viável e satisfatória aos requisitos levantados. Para tanto, uma aplicação de carga e recarga de veículos elétricos baseada no ARES foi implementada para avaliação da multifuncionalidade dos postos de carga e dos veículos elétricos que hora utilizam a rede elétrica para serem carregados e hora servem de GD. A aplicação utiliza as informações passadas pelos dispositivos através da modelagem IEC 61850 tradicional e da extensão proposta nesta tese. A segunda aplicação envolve a proteção adaptativa que foi avaliada em bancada com IEDs de mercado. Uma aplicação de Teleproteção também foi realizada a fim de testar se a liberação de fluxos ocorreu de forma satisfatória. Os três testes foram realizados em laboratório com *switches* SDN para subestações e o auxílio de equipamentos de sincronização (como GPS e antena) e mala de testes, além de computadores. A API ARES foi implementada e avaliada com o auxílio do Mininet [111], capaz de emular redes SDN, e do controlador RYU [47]. Os testes indicaram que a solução proposta é viável e atende aos requisitos levantados.

1.3 Estrutura do Texto

Esta tese está estruturada em sete capítulos. No Capítulo 2, os cinco problemas que motivaram o desenvolvimento do *framework* são detalhados e discutidos.

No Capítulo 3, para embasamento teórico, são apresentados os conceitos de rede elétrica inteligente necessários para entendimento desta tese. Nesse capítulo, uma breve descrição sobre proteção e a rede elétrica tradicional é apresentada. Em seguida, os conceitos relacionados às redes elétricas inteligentes, como *microgrids*, AMI, dentre outros são descritos. A análise dos protocolos SCADA utilizados nos sistemas supervisórios é realizada neste capítulo, assim como uma introdução à Norma IEC 61850, que é pré-requisito para implementação do *framework* ARES. As considerações sobre o estado da arte para redes elétricas inteligentes também são feitas nesse capítulo.

Em seguida, no Capítulo 4, as redes definidas por software são descritas. Além dos principais conceitos relacionados ao OpenFlow, é feita uma análise sobre os principais trabalhos relacionados ao uso de SDN no contexto de redes elétricas inteligentes, além de trabalhos relacionados ao uso de SDN para sistemas de controle, supervisão e proteção no sistema elétrico.

A proposta do *framework* ARES é apresentada no Capítulo 5, onde os principais requisitos de comunicação para redes elétricas inteligentes são levantados e discutidos. A arquitetura da proposta é detalhada, assim como seus componentes, algoritmos e a API. O uso do ARES pelo SCADA-NG e a extensão da modelagem IEC 61850 também são apresentados nesse capítulo.

O Capítulo 6 apresenta os três cenários de implementação do *framework* ARES, as ferramentas utilizadas para implementação, o ambiente de implementação, a descrição dos experimentos e os principais resultados obtidos com o ARES, assim como a análise dos valores encontrados.

Por fim, o Capítulo 7 conclui a tese, realçando suas contribuições e apontando trabalhos futuros.

Capítulo 2

Definição do Problema

Redes elétricas inteligentes, conhecidas como *smart grids*, trazem propostas inovadoras que mudam de forma profunda a maneira como a energia é provida desde a geração até os consumidores finais. A ideia consiste em aperfeiçoar os sistemas elétricos, com o auxílio de uma infraestrutura de comunicação eficiente, visando o aumento na qualidade e continuidade do fornecimento de energia. Dentre as novas propostas, destacam-se a geração de energia de forma distribuída, o amplo uso de fontes renováveis, o uso de carros elétricos, o uso de medidores inteligentes, entre outros. O consumidor passa a ser parte fundamental do funcionamento da rede elétrica, podendo incorporar também o papel de produtor de energia. Os medidores inteligentes localizados nas residências passam a gerar uma quantidade enorme de informação, que poderá ser usada para o gerenciamento e controle do sistema [184, 125, 151]. As redes elétricas inteligentes requerem um sistema supervisório inteligente para gerenciamento e monitoramento de processos, dispositivos automatizados, dispositivos de campo e medidores inteligentes. O sistema supervisório mais amplamente usado é chamado SCADA. Com a evolução para as redes elétricas inteligentes, o SCADA gerenciará também novos elementos inteligentes, tais como unidades de medição fasorial, relés inteligentes, novas fontes de geração de energia com utilização de fontes renováveis, armazenamento de energia, VEs, etc [62]. Com um alto grau de automação e inserção de fontes de energia renováveis, as redes elétricas inteligentes trazem benefícios não só para o consumidor, mas também para as concessionárias de energia e para o meio ambiente.

De acordo com o modelo conceitual do NIST (*National Institute of Standards and Technology*) [138], a rede elétrica inteligente é composta por domínios lógicos com agentes e dispositivos inteligentes que devem ser interligados. Nesse novo cenário, os dispositivos finais da rede, como os medidores, se tornam mais inteligentes e podem se comunicar diretamente com os centros de controle de dados através da AMI. De fato, a implantação da rede elétrica inteligente começa com uma inserção em massa de medidores inteligentes e da AMI, que são elementos chave neste cenário. A introdução de medidores inteligentes permite uma melhor compreensão da demanda e um melhor controle do consumo de energia e da geração distribuída.

Além disso, o número de IEDs aumenta a fim de apoiar a automação de todo esse sistema. Em geral, a quantidade de dispositivos de automação, tais como medidores inteligentes e IEDs, e a quantidade de dados coletados a partir desses dispositivos, aumentam significativamente. A comunicação, que antes compreendia apenas parte do sistema, como as subestações e seus centros de controle, passa agora a englobar todo o sistema, incluindo o consumidor. Ademais, a rede elétrica inteligente traz um enorme crescimento no volume de dados que deve ser gerenciado e controlado e depende de uma sofisticada infraestrutura de redes de comunicação para dar suporte à comunicação entre os dispositivos inteligentes que monitoram a rede e funcionam como atuadores. Nesse contexto, o sistema supervisório SCADA passa a ser uma alternativa para supervisão em outras partes do sistema que vão além das subestações.

Da mesma forma, uma rede de comunicação eficiente que dê suporte às aplicações das redes elétricas inteligentes deve levar em consideração os diversos domínios das *smart grids*. Os domínios compreendem desde a geração até o mercado de energia.

De forma geral, verifica-se que a comunicação é necessária em todos os domínios, independentemente da função que um determinado dispositivo exerça. Por essa razão, nesta tese, todos os dispositivos finais são intitulados IEDs, já que exercem múltiplas funções e são dotados da habilidade de se comunicar. Ressalta-se que, levando em conta esse ponto de vista, tanto a estação de recarga quanto os medidores inteligentes, ou ainda os próprios relés, são considerados IEDs.

Nesse contexto, o funcionamento do Sistema Elétrico de Potência (SEP) muda de forma considerável entre o modelo atual e o modelo das redes inteligentes. Por exemplo, nas redes elétricas inteligentes, uma residência, em momentos diferentes, participará da [184, 58, 69, 187]:

- medição inteligente – onde o medidor de eletricidade é equipado com capacidade de comunicação para enviar as leituras do medidor automaticamente pela rede para a empresa de distribuição, além de ter a capacidade de receber sinais de corte e religamentos remotamente.
- resposta à demanda – onde o padrão de consumo do cliente é alterado em resposta a mudanças no preço da eletricidade ao longo do tempo ou quando a confiabilidade do sistema é comprometida [171].
- geração distribuída – onde o cliente pode participar como gerador, tanto com um painel solar (por exemplo) quanto com o próprio veículo elétrico. Desta forma, tanto as medidas de resposta à demanda, quanto a medição inteligente têm suas características alteradas.

Considerando o exemplo de uma residência, sua inclusão na *smart grid* inicia com a instalação de um medidor inteligente [171]. Para que o consumidor possa ter um medidor

inteligente funcional, é necessária uma rede de comunicação entre centro de controle e medidor, conforme ilustrado na Figura 2.1. Dessa forma, a infraestrutura de comunicação, conhecida como AMI, é criada para que seja realizada a tarifação automática ou cortes e religamentos de energia. Essas aplicações não têm requisitos rígidos de QoS [69] e, com isso, a comunicação é pensada e configurada levando em consideração essas necessidades. Nesse caso, as redes de comunicação são projetadas para mensagens não prioritárias sem requisitos rígidos de latência ou recuperação de falhas, por exemplo. O provisionamento e configuração da rede de comunicação é realizado de acordo com esses requisitos não rígidos. Além disso, o meio físico também é escolhido com base nesses requisitos. É importante ressaltar que, dependendo da região, o enlace é contratado através de uma operadora de telecomunicações. Com isso, o pagamento deste enlace pode ser feito de acordo com a utilização do enlace. Isto limita a quantidade de tráfego que pode ser transmitido por esse medidor. O mesmo ocorre em outras áreas dos sistemas elétricos como em religadores da rede de distribuição.

Figura 2.1: Exemplo de implementação atual de parte da infraestrutura das redes elétricas inteligentes

Em uma segunda fase, e quando possível, o mesmo consumidor passa a se interessar pela iniciativa de resposta à demanda. Dessa forma, o seu consumo de energia pode ser alterado temporariamente em resposta às condições de fornecimento de energia ou aos eventos na rede elétrica [53]. Com isso, as medidas fornecidas pelos medidores inteligentes passam a ser usadas para dar suporte às aplicações que exigem requisitos de QoS mais rígidos [184, 171]. As aplicações de tarifas em tempo real (*Real Time Pricing* (RTP)), tarifas horo-sazonais (*Time of Use* (TOU)) e tarifa de picos críticos (*Critical Peak Pricing* (CPP)), ferramentas usadas para tarifação e para resposta à demanda [38] possuem requisitos um pouco mais rígidos do que o cenário anterior. Caso a infraestrutura já implementada não atenda a esses requisitos, a rede de comunicação precisa ser novamente projetada.

Considerando um outro caso em que o cliente adquiriu um veículo elétrico, e que, como em diferentes propostas na literatura [181, 16, 29, 14, 91], esse veículo se interconecta com a rede elétrica inteligente para ser carregado ou descarregado ou para servir de geração distribuída. Em sequência, o cliente também instala uma GD, baseada em energia solar, por exemplo. Seria necessário planejar um outro projeto de comunicação para que o medidor da GD ou o ponto de recarga do veículo se comuniquem com o controle local/remoto e com a concessionária. Assim, haveria outro medidor inteligente que passaria a desempenhar um papel muito importante no domínio de geração. A Figura 2.2 exemplifica esse cenário.

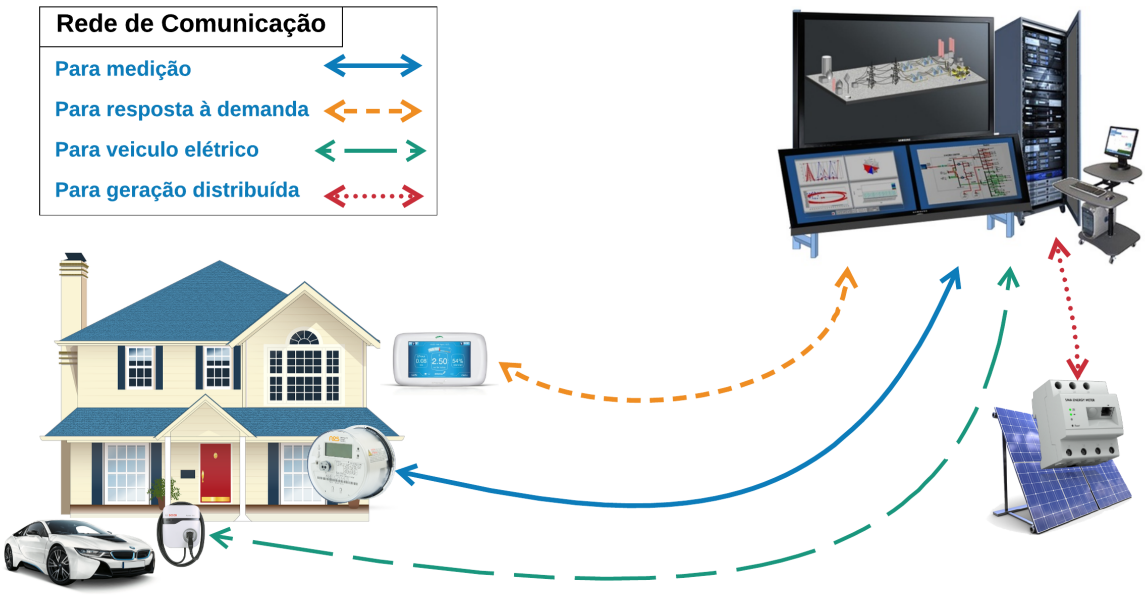


Figura 2.2: Exemplo de implementação atual de parte da infraestrutura das redes elétricas inteligentes, considerando GD, VE e medidor inteligente

Nesse contexto, os requisitos de QoS são muito mais altos, já que as informações enviadas pela GD são marcadas como tráfego prioritário e com requisitos rígidos de QoS, por exemplo. Alguns trabalhos na literatura [33, 89, 129, 99, 72, 182, 188, 167, 12, 41, 66, 178], que abordam a proteção adaptativa* na presença de GDs, mostram que o principal requisito para o funcionamento da proposta é uma rede de comunicação confiável. Como a GD participa da *microgrid* conectada, os requisitos de QoS aumentam muito, já que as novas filosofias de proteção apresentadas para *microgrids* dependem fortemente de um cenário de comunicação mais eficiente [100]. As informações geradas devem ter confiabilidade e baixa latência. Por exemplo, os dados críticos relacionados devem ser recebidos pelo controlador

*A proteção adaptativa é uma filosofia que permite fazer ajustes no sistema de proteção para torná-lo adequado às variações do estado da rede em tempo real. O conceito principal é a alteração de parâmetros no sistema de proteção em resposta a mudanças no sistema causadas por alterações de carga, chaveamentos de operação ou até mesmo faltas elétricas. Isto significa que as características de abertura do relé mudam de acordo com as condições do sistema [100]

em tempo hábil. As redes de comunicação devem fornecer mecanismos para satisfazer esses requisitos de QoS [58]. Em geral, outra infraestrutura é implementada, ou adquirida, para atender a esse novo cenário.

A Figura 2.2 ilustra o cenário apresentado em que as redes de comunicação são criadas em paralelo para atender aos requisitos das aplicações. De uma forma mais realista, geralmente as redes de telecomunicações empregadas também diferem. Pode-se utilizar *Power Line Communications* (PLC), fibra, redes sem fio, satélite, etc [58, 90]. Da mesma forma, é utilizado para cada cenário um protocolo/padrão diferente e muitas vezes proprietário. Os equipamentos não interoperam e tanto a concepção desse cenário quanto sua manutenção são muito difíceis [80]. Essas características criam a falsa teoria no sistema elétrico de que a comunicação entre os dispositivos é algo inviável, descaracterizando o princípio das *smart grids*, que oferece comunicação entre todos os elementos.

Naturalmente, o cenário ideal seria tal que o medidor inteligente integrasse todas as aplicações. Uma infraestrutura paralela apenas se justificaria se fosse ser utilizada como *backup*, o que não é o caso. A implementação de diversas infraestruturas paralelas para viabilização da comunicação de GDs localizadas em residências, somente por serem caracterizados como um tráfego mais crítico, não é adequada. O uso de medidores inteligentes e da AMI no domínio de geração é algo já esperado. Uma abordagem com o uso da AMI, de forma inteligente, traz benefícios muito maiores, com informações em tempo real, contribuindo para um maior retorno de investimento e para um custo operacional mais baixo, o que justifica o investimento em longo prazo. Nesse sentido, ter uma rede confiável, com informações disponíveis em tempo real, torna-se uma premissa básica para que a energia seja entregue de forma confiável para os usuários finais. A grande maioria das falhas no provimento de energia pode ser evitada ou contornada pelo monitoramento em tempo real, pelo diagnóstico e proteção da rede.

Além disso, com um uso bem projetado dos medidores inteligentes, além das funcionalidades já citadas, torna-se possível também a localização de faltas nos sistemas de distribuição [151, 34] e a detecção de furtos de energia. Todas essas funcionalidades têm características próprias e utilizam a mesma infraestrutura, no entanto, possuem requisitos distintos. Dessa forma, o medidor pode trafegar, além das informações tradicionais, informações relacionadas à GD e aos VEs, por exemplo. De forma geral, há sempre um dispositivo inteligente final e multifuncional. As mensagens enviadas por esse dispositivo carregam informações de diferentes domínios e, com isso, exigem QoS distintas de acordo com a sua funcionalidade, que pode variar em tempo real.

Tendo em vista esse cenário, onde considera-se a inserção de GD nos usuários finais e um aumento do número de dispositivos inteligentes instalados, alguns desafios estão relacionados:

- os dispositivos finais multifuncionais são dinâmicos e têm requisitos de comunicação

variáveis;

- os dispositivos finais possuem tráfegos com características extremamente diferentes, e o provimento de QoS deve ser de acordo com cada tráfego e com as aplicações de energia envolvidas;
- a configuração e provisionamento da rede de comunicação deve ocorrer de forma automática;
- a configuração dos sistemas supervisórios também deve ser automática, respeitando princípios de segurança, o que demanda a modernização desses sistemas.

Esses desafios são discutidos nas seções a seguir.

2.1 Dispositivos Finais Multifuncionais

Com a inserção de GD nas residências, são implementados também dispositivos multifuncionais que se comunicam em tempo real. Nesse cenário, há geração de energia em algum momento do dia e em outros não. No caso de painéis solares, por exemplo, não há geração durante à noite. Da mesma forma, caso a residência utilize toda a energia gerada, esta não é exportada para rede. No entanto, no momento em que se tem energia excedente, esta deve ser exportada para a rede, fazendo com que aquela residência saia da função de carga e passe para a função de gerador. Com isso, a rede de comunicação precisa lidar com equipamentos finais que mudam de função e demandam características de QoS diferentes de acordo com a função, em tempo real.

Por esse motivo, os aspectos de proteção e controle do sistema elétrico se tornam muito importantes. A estabilidade do sistema precisa ser mantida, mesmo com a entrada e saída de pontos de geração distribuídos, e as manobras realizadas no sistema elétrico não podem interromper o fornecimento de energia. A entrada de GDs em um sistema que não está ajustado para um cenário com GDs pode resultar em atuações indevidas do sistema de proteção. Áreas inteiras podem ser desligadas pelos sistemas de proteção por considerar que a entrada da GD é na verdade uma falta. A comunicação nesse sentido é grande aliada já que a alteração de função deste dispositivo pode ser informada e a proteção ajustada de acordo com essa informação.

2.2 Provimento de QoS

Outra característica importante é que determinado dispositivo pode participar de aplicações de energia distintas. Um medidor inteligente, ora envia informações referentes a consumo e, em outro momento, informações de geração de energia, sendo representante de aplicações

de energia distintas. Quando for apenas referente a consumo, a QoS geralmente não é crítica. No entanto, no cenário com a GD em funcionamento, as informações trocadas possuem requisitos de QoS mais críticos e semelhantes aos das subestações digitalizadas, que usam o recurso de comunicação para a proteção e controle do SEP.

Da mesma forma, o medidor inteligente pode ser tanto representante de uma aplicação não crítica como de uma crítica, causando diversos impactos sobre os requisitos necessários na rede de comunicação. Durante uma emergência no sistema elétrico, também se observa essa mudança, já que a característica do tráfego oriundo de determinado equipamento pode mudar de prioridade. Um exemplo é o cenário proposto por Maharjan et al. [130], em que os autores propõem o uso de veículos elétricos como fontes de energia temporárias e móveis para apoiar uma infraestrutura crítica durante emergências. Os autores discutem a viabilidade da ideia com um breve estudo de caso. No entanto, no artigo a rede de comunicação é configurada de forma a caracterizar o tráfego destes pontos como prioritário o tempo todo. No entanto, essa situação não é a ideal, já que outras aplicações podem estar usando a mesma infraestrutura de comunicação e ter prioridade sobre as aplicações dos veículos quando estiverem fora do período de emergência. De fato, na maior parte do tempo (fora da situação de emergência), os veículos elétricos participam de outros tipos de aplicação, com características e requisitos diferentes. De forma geral, há um cenário onde um dispositivo de rede trafega informações extremamente prioritárias em uma situação específica, de emergência e, em outro momento, trafega informações com requisitos bem diferentes, como tarifação ou supervisão, etc.

2.3 Configuração e Provisionamento da Rede de Comunicação

A característica dinâmica da rede de comunicação, que necessita de configuração e provisionamento de enlaces de comunicação de acordo com a qualidade de serviço demandada pelas aplicações, é um dos desafios mais relevantes a serem discutidos. A quantidade de dispositivos que precisam ter uma rede de comunicação configurada cresce muito, e com isso, a configuração manual de cada enlace de comunicação já praticamente inviabiliza a implementação das redes elétricas inteligentes em grande escala. Somada a isso, há uma mudança de requisitos em tempo real. A reconfiguração de enlaces é custosa, demorada, e ainda está suscetível a erros de configuração, como todo processo manual. Com isso, o provisionamento autonômico da rede de comunicação, de acordo com os requisitos demandados pelas aplicações de energia, seria o ideal. Ressalta-se que a rede de comunicação tradicional não conseguiria realizar este provisionamento de forma dinâmica. Com isso, todos os recursos teriam que ser previstos e alocados desde o projeto de concepção da rede, o que pode não ser factível ou escalável. Para que esse cenário funcione bem, a alocação de recursos precisa ser dinâmica, acompanhando o comportamento multifuncional dos

dispositivos.

2.4 Configuração dos Sistemas Supervisórios

Especificamente, todos os dispositivos finais da rede elétrica (IEDs) para serem monitorados precisam ser mapeados no sistema supervisório. São configuradas informações relacionadas aos próprios dispositivos e aos equipamentos elétricos a ele conectados. Exemplos dos pontos configurados são o endereço de rede do dispositivo, as características funcionais dos equipamentos, as funcionalidades no sistema e as grandezas analógicas e digitais a serem medidas. Em alguns casos, a localização do dispositivo, o modelo, a versão do firmware, também são mapeados. Isso ocorre, pois o sistema de gerenciamento precisa conhecer as características típicas e reais dos equipamentos conectados, como o valor da potência ativa e reativa que pode ser fornecida ou qual é a quantidade de energia que pode ser armazenada, entre outros. Estes valores devem ser mapeados no supervisório de forma a permitir a supervisão e controle dos mesmos.

Naturalmente, quando essa configuração é feita de forma manual, é comum existirem erros que podem trazer impactos muito negativos para o sistema. Também é importante ressaltar que, quando a configuração é manual, devido aos processos envolvidos, pode ocorrer um tempo longo entre a instalação de um equipamento em campo e sua configuração no supervisório. Com isso, caso tenha alguma mudança em campo, esta não é reportada em tempo real para o SCADA, o que pode resultar em erro de configuração, atraso de configuração e algumas vezes em maiores custos com fornecedores e equipe.

Este problema já é desafiador quando limitado a subestações e é ainda maior se relacionado a todas as áreas das redes elétricas inteligentes e à característica dinâmica das funções dos dispositivos. Apesar de alguns trabalhos, como o de Etherden et al. [56] identificarem este desafio, o problema ainda está em aberto. Somente após cada ponto ter sido mapeado no supervisório, as telas dos sistemas supervisórios são criadas e associadas a esses pontos.

O mapeamento dos pontos a serem supervisionados no SCADA, quando feito de forma manual, além de passível de erros humanos e financeiramente custoso torna todo o processo lento. Segundo [56], a falta de serviços de gerenciamento ainda é uma lacuna para que o funcionamento das *smart grids* seja completo. Segundo os autores, o ideal seria que o sistema fosse dinâmico para permitir que uma GD se registre em um cliente SCADA especificado com apenas seu endereço IP. Assim, o cliente SCADA poderia consultar as características e propriedades do recurso de forma automática. Com isso o sistema poderia responder a solicitações de um sistema de gerenciamento de distribuição (ou um sistema de negociação de mercado) fornecendo como resposta as características, as propriedades e a capacidade disponível de geração. O banco de dados poderia ser atualizado com os parâmetros reais e as estimativas seriam feitas em tempo real com as capacidades

disponíveis [56].

Outra razão importante para que o mapeamento dos dispositivos no supervisório seja automatizada é relacionada à característica dinâmica das funções dos dispositivos. Por exemplo, as informações vindas de um medidor inteligente geralmente são usadas para uma medição tarifária, caracterizando o consumidor como uma carga que demanda energia e é cobrado por isso. No entanto, quando um painel solar estiver gerando energia excedente e essa for colocada na rede elétrica, as informações que passarão a ser enviadas do medidor podem incluir informações de geração de energia. O mapeamento dos dispositivos deve permitir o dinamismo que os equipamentos multifuncionais exigem. Percebe-se um desafio imposto pela modernização do sistema tradicional que é relacionado à necessidade de evolução dos sistemas de supervisão e controle e sua rede de comunicação. O sistema SCADA precisa ser mais autonômico para incorporar um sistema que se tornou mais dinâmico.

2.5 Modernização dos Sistemas Supervisórios

As redes elétricas inteligentes não podem ser gerenciadas pelos sistemas supervisórios atuais [113]. Como detalhado em [113], o alto custo e baixa interoperabilidade tornam as soluções baseadas no SCADA tradicional impraticáveis para instalações com maior escala que em subestações, limitando efetivamente sua adoção. Como mencionado em Silva et al. [172], a modernização das redes de comunicação SCADA é necessária. Como afirmado por Ethernen et al. [56], para a evolução das redes elétricas inteligentes, com a inclusão de AMI, GDs e VEs, é necessário que sejam realizadas extensões nas funcionalidades dos sistemas de controle e gerenciamento, e nesse caso, as estratégias utilizadas atualmente não permitem essa evolução.

O supervisório atual é passivo em relação à rede de comunicação, ou seja, o supervisório passa a funcionar após a sua configuração completa (mapeamento de pontos, criação de telas, etc.) e após o provisionamento da rede de comunicação, ambos definidos em projeto e realizados de forma manual. Nas implementações atuais, o SCADA não solicita ou provisiona os recursos de comunicação de que precisa para determinada aplicação de energia de forma automática. Para que seja feito o provisionamento dos recursos de comunicação necessários para que o sistema SCADA se comunique com os dispositivos que serão supervisionados e controlados, a rede SCADA é previamente projetada e instalada. Após esse processo, o provisionamento dos recursos de comunicação pode ser realizado pelo administrador da rede. Por exemplo, para as aplicações de energia que utilizem a AMI, toda a infraestrutura de comunicação entre os medidores e o centro de controle, após projetada e instalada, precisa ser devidamente provisionada. Isto é feito de forma manual por administradores de rede que configuram os equipamentos de rede, seus endereços, suas rotas, protocolos, etc. Além disso, caso um novo equipamento seja instalado, uma expansão

seja realizada ou caso um equipamento passe a ser usado por outra aplicação de energia (com requisitos de comunicação diferentes), esses recursos precisam ser provisionados novamente pelo administrador, com as novas características ou inclusões necessárias. Todo esse processo é lento e envolve custos.

Visando a contribuição com o estado da arte das redes elétricas inteligentes, diversos autores [100, 16, 15, 31, 164, 180, 131] propõem soluções de controle e gerenciamento (intituladas aplicações de energia nesta tese) que permitem melhorar o sistema como um todo. No entanto, os trabalhos partem da premissa que os operadores vão ter conhecimento de toda a rede de comunicação e de todos os equipamentos de energia conectados a ela em tempo real. Dessa forma, podem receber dados, fazer cálculos e, quando for o caso, enviar comandos.

Com uma infraestrutura de comunicação robusta e sistemas supervisórios eficientes com novas funcionalidades, as aplicações de energia podem reduzir o risco de indisponibilidade energética e otimizar o uso da rede elétrica, equilibrando produção de eletricidade e consumo. Exemplos de novas aplicações de energia são os sistemas de gerenciamento pelo lado da demanda, onde o equilíbrio entre geração e consumo de energia é feito com o auxílio do consumidor. Uma rede que permita que os dispositivos de energia sejam descobertos automaticamente pelo supervisório e que tenham suas características atualizadas em tempo real permitiria o desenvolvimento de novas aplicações de energia mais eficientes. A possibilidade de registro automático no supervisório e leitura automática das capacidades dos dispositivos de geração distribuída foram recentemente discutidas em [56] como sendo uma excelente solução futura para evolução das redes elétricas inteligentes. No entanto, ressalta-se que esse tipo de abordagem precisa seguir alguns requisitos de segurança mínimos, como autenticação e controle de acesso para minimizar possíveis ataques cibernéticos.

O provimento de uma rede de comunicação autonômica para as redes elétricas inteligentes, que, além de se autoconfigurar, permita que o sistema supervisório possa dinamicamente alocar os recursos da rede de comunicação permitindo a criação de aplicações de energia de nova geração, mais inteligentes e robustas é o desafio motivador desta tese. Com isso, as novas aplicações de energia que estão sendo propostas, abstraindo a forma com que a informação ficará disponível em tempo real, poderão de fato ser implementadas. O tráfego de pacotes será liberado de acordo com a aplicação de energia, após o seus provisionamento ter sido realizado de acordo com as suas características.

Capítulo 3

Redes Elétricas Inteligentes

Devido ao crescente aumento populacional e ao aumento do número de equipamentos em uso nas residências, a demanda por energia tem crescido cada vez mais nos últimos anos [57]. No entanto, para acompanhar esse crescimento, o setor precisa investir muito em infraestrutura. Um caminho, usado por muito tempo, foi o investimento no aumento da infraestrutura para geração de energia, com a construção de novas usinas geradoras para suprir essa demanda. Contudo, a regulamentação para as construções e demandas ambientais muitas vezes atrasam e/ou impedem esse tipo de construção. Essas caraterísticas resultam na necessidade de estudos e implementação de novos mecanismos e sistemas para suprir o aumento da demanda sem a construção de novas usinas geradoras. Assim, a modernização da infraestrutura existente e o desenvolvimento de novas propostas ganharam força nos últimos anos. Por conseguinte, surgiram as redes elétricas inteligentes, ou *Smart Grids*, tornando imprescindível a implantação de um sistema de comunicação mais robusto [125].

Esta modernização vem causando uma grande revolução nas redes de energia elétrica, aumentando os ganhos em confiabilidade, eficiência energética, participação dos consumidores e geração de uma energia mais limpa [148]. No entanto, para que as principais características e desafios das redes elétricas inteligentes sejam de fato compreendidas, o conhecimento, mesmo que mínimo, do sistema tradicional é desejável. Ao conhecer as principais características dos sistemas elétricos tradicionais, tanto os desafios quanto as principais características esperadas das redes de comunicação e dos novos sistemas para automação do sistema elétrico podem ser levantados.

3.1 Uma Breve Introdução à Rede Elétrica Tradicional e à Proteção

O sistema elétrico atual é um conjunto de usinas, subestações, linhas de transmissão e outros equipamentos que possibilitam a geração, transmissão e distribuição de energia

elétrica em uma área específica. Esse sistema tradicional possui uma separação clara em suas estruturas de geração, transmissão e distribuição. Na geração, as usinas são classificadas conforme os recursos que utilizam, podendo ser hidroelétricas, termoelétricas, eólicas, nucleares, etc. Assim, certo tipo de energia é transformado em energia elétrica e após gerada, a tensão é aumentada e a energia é transportada em altas tensões para que se evite perdas. Por fim, na rede distribuição, a energia é entregue ao consumidor final em baixas tensões.

Nesse cenário, as subestações desempenham uma papel essencial. Entre os tipos de subestações, destacam-se as subestações de transmissão, as quais conectam linhas de transmissão com voltagens iguais ou diferentes; as subestações de distribuição, as quais conectam linhas de transmissão com linhas de distribuição, além de regular a tensão; e as subestações coletoras, as quais são usadas para ligar a geração com as linhas de transmissão. Elas são responsáveis por aumentar ou diminuir a tensão na transmissão e na distribuição. Internamente, a subestação também desempenha funções de proteção e controle que são características de extrema importância. Isto porque o SEP deve trabalhar de forma estável mesmo em condições de aumento de carga de consumo, suportando efeitos indesejáveis como curto-circuitos ou quedas de linhas de transmissão de forma a manter a frequência e amplitude de tensão constantes, bem como a continuidade no fornecimento de energia [63].

Os dispositivos de proteção são utilizados para estabilizar o sistema amortecendo oscilações, de forma a garantir a estabilidade do sistema de forma dinâmica [63]. Uma área ou um equipamento defeituoso é isolado de forma confiável e rápida pelo sistema de proteção pela interrupção do menor trecho possível da rede elétrica, evitando, com isso, grandes perdas. É graças aos sistema de proteção que fenômenos como faltas, curto-circuitos e manobras, que prejudicam a estabilidade do sistema elétrico e danificam seus componentes, podem ser evitados e/ou contidos.

O sistema de proteção, tradicionalmente, utiliza dispositivos inteligentes capazes de, a partir da medição de grandezas do sistema elétrico e de acordo com suas lógicas internas, executar ações em campo, como os relés de proteção*. Os principais componentes que compõem esse sistema são:

- Relés: São elementos detetores-comparadores e analisadores, auxiliados pelo disjuntor. Cada relé, no sistema convencional, opera de forma instantânea ou temporizada, com o objetivo de sanar variações nas condições normais de operação dos equipamentos da sua zona de proteção ou do circuito o qual está ligado. Desta forma, promovem a retirada rápida de um elemento do sistema por meio de um sinal de abertura para um disjuntor, o qual é chamado de *trip*, e indicam a localização e o tipo do defeito detectado. Por exemplo, um relé de sobrecorrente tem como função abrir o circuito protegido quando a corrente que passa em seus contatos é maior que um

*Mais recentemente, os IEDs além de se comunicarem diretamente com o supervisório podem se comunicar entre si realizando automatismos e proteções através do uso de protocolos de comunicação.

valor pré-estabelecido.

- Disjuntores: São dispositivos de manobra que permitem ligar e desligar dois condutores que fazem parte de uma rede elétrica. Podem ser comandados automaticamente por relés por meio de *trips* ou de forma manual pelo operador. Dessa maneira, são responsáveis por desconectar a área defeituosa do sistema, isolando as falhas.

- Transformadores de Instrumentos: O transformador de instrumentos coleta correntes e tensões elevadas da rede elétrica e as transforma em níveis adequados para utilização em dispositivos de medição e proteção (como os relés). Isso é importante porque os relés não aceitam entradas de alto valor de tensão ou corrente. O transformador de instrumento relacionado à transformação de potencial é chamado de Transformador de Potencial (TP), enquanto que o relacionado à corrente é chamado Transformador de Corrente (TC).

Desta forma, o relé processa os sinais provenientes dos TPs e TCs para identificar um defeito e, caso alguma situação de falha seja identificada, o relé envia um comando de abertura para os disjuntores, que, por sua vez, isolam a falha abrindo os terminais mais próximos para que não haja propagação do defeito para outros circuitos e equipamentos. Esse conjunto de ações é chamado de manobra. É necessário que as manobras sejam feitas da forma mais rápida possível para proteger o sistema.

Em geral a filosofia de proteção é dividida em zonas de proteção. A Figura 3.1 detalha essa divisão, em que a zona de proteção é definida por um conjunto de sistemas de energia entre dois disjuntores, incluindo os equipamentos de proteção. Enquanto a proteção de transformadores (item 2 da Figura 3.1) é feita localmente, o limite para proteção de linhas, item 4 da Figura 3.1, é geralmente localizado em duas subestações diferentes que podem ser separadas por uma distância considerável.

Os sinais de intertravamento[†] e proteção no sistemas elétricos tradicionais são enviados através de circuitos físicos dedicados, constituídos por fiação de cobre, interligando diretamente os circuitos de comando dos disjuntores. Observa-se que, nesse sistema, não é utilizada uma rede de comunicação, apenas sinais de controle fiados. Assim, se um sinal precisa ser enviado entre um ou mais dispositivos, é preciso que exista um cabo dedicado interligando cada par de dispositivos.

Tem-se ainda sistemas de proteção temporizados onde uma proteção *backup* (chamada de proteção de retaguarda) atua momentos depois da falha, caso esta ainda não tenha sido sanada. Como exemplo, tem-se a necessidade de acionamento de outro disjuntor

[†]O intertravamento é um conjunto de passos ou laços que devem existir para garantir a segurança de um equipamento, pessoa ou processo. É um processo de ligação entre os contatos auxiliares de vários dispositivos (como relés), pelo qual as posições de operação desses dispositivos (por exemplo, se estão abertos ou fechados) são dependentes umas das outras. Através do intertravamento, evita-se a ligação de certos dispositivos antes que os outros permitam essa ligação.

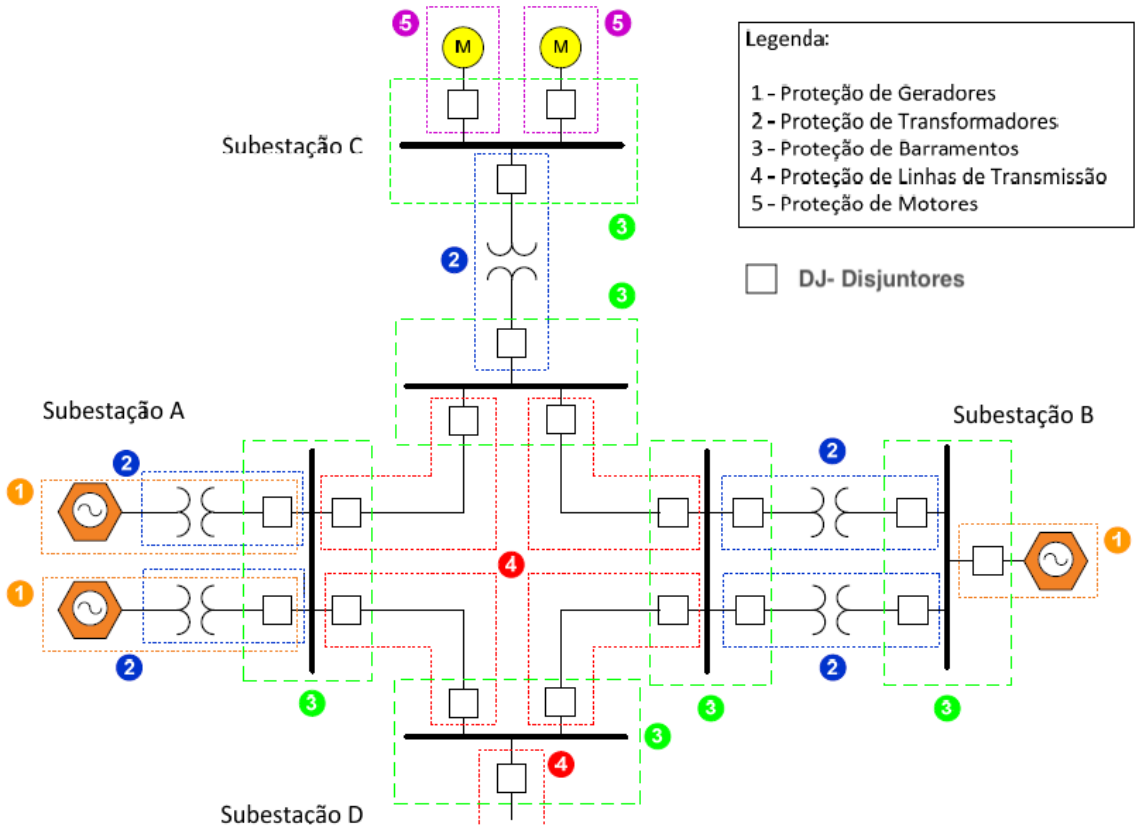


Figura 3.1: Cinco zonas de proteção básicas, sendo elas: 1 - Geração; 2- Transformadores; 3 - Barramentos; 4 - Linhas; 5 - Carga. (Fonte: [134])

quando o principal falha e não é aberto. Com isso, caso o relé *backup* (chamado de relé de retaguarda) ainda enxergue uma falha em sua zona de proteção, em um período de tempo em que essa falha já deveria ter sido sanada, ele atua. Da mesma forma, caso a zona de proteção englobe uma distância considerável, como na proteção de linhas de transmissão, faz-se necessária a instalação de pelo menos um relé em cada extremidade da linha para operar os disjuntores desta, como indica o item 4 da Figura 3.1. Neste caso, eles podem operar independentemente (temporizados) ou compartilhar informações para melhorar a sua velocidade de operação (o que exige comunicação entre eles).

Ressalta-se que a possibilidade de usar uma rede de comunicação para que dois relés possam trocar informações e decidir pela atuação de determinada proteção, apesar de algo intuitivo, é uma solução mais recente. De fato, essa comunicação entre relés foi padronizada pela norma IEC 61850 através de mensagens GOOSE, como será visto em detalhes adiante. A forma temporizada é a opção utilizada no sistema tradicional de forma a não depender da rede de comunicação. No sistema temporizado, a atuação tende a demorar muito mais do que nos sistemas baseados em comunicação por rede, já que as temporizações costumam ser de ordens maiores do que a latência da rede. Exemplos são

a falha de disjuntor que usa uma temporização de 200 ms[‡] contra a latência numa rede local, de mais ou menos 1ms[§].

Por fim, as subestações podem ser assistidas ou não e contam com sistemas do tipo SCADA para controle e supervisão remotos. O SCADA é utilizado para supervisionar, controlar, otimizar e gerenciar os sistemas de geração e transmissão de energia elétrica. Diferentemente dos sistemas de proteção tradicionais, os sistemas de supervisão e controle, desde sua concepção, são amparados por sistemas de comunicação.

As operadoras de energia no Brasil utilizam o SCADA para realizar diversos tipos de medições, como: diagramas fasoriais de tensões e correntes, queda de consumo, queda de demanda de energia, perfis de curvas de carga de potências ativas e reativas, entre diversos outros. Esses dados são analisados por especialistas que disparam medidas corretivas, de contingência e planejamento da rede. Uma grande parte dessa análise é automatizada baseada em dados históricos, topologia da rede e experiências humanas [49]. Com a evolução das redes elétricas inteligentes, o SCADA incorporará novos elementos inteligentes, tais como: unidades de medição fasorial, relés inteligentes, novas tecnologias com utilização de fontes renováveis, armazenamento de energia em veículos elétricos, etc [62].

Dessa forma, a supervisão e a proteção são pontos chave para as redes elétricas. O sistema de supervisão e controle é responsável pelo monitoramento da rede e o sistema de proteção pela defesa contra falhas dentro e fora das subestações.

Mesmo com todo esse sistema de supervisão, controle e proteção, a rede elétrica tradicional ainda carece de modernização. De forma geral, com relação às redes elétricas tradicionais, essa inteligência encontrada em subestações e centros de controle, não é percebida no usuário final. Ao consumidor, cabe apenas consumir e pagar a conta. Não há a possibilidade de venda de parte da energia produzida por ele, quando existe a utilização, por exemplo, de painéis solares. Da mesma forma, os consumidores são desinformados, no sentido de não terem informações em tempo real sobre o consumo, preços, etc. O controle do consumo, corte e religamento ainda são realizados de forma manual. A automação no controle dos dispositivos da rede de distribuição ainda é pequena. A geração é realizada muito distante dos grandes centros consumidores e a qualidade na energia entregue ao consumidor pode ser baixa, devido a falhas nos sistemas de transmissão e de distribuição.

Com os recentes desenvolvimentos em monitoramento avançado, tecnologias de informação e comunicação aplicadas as redes elétricas inteligentes, as novas redes de distribuição de energia serão capazes de responder com mais eficiência às necessidades dos consumidores. Atualmente, diversas iniciativas já são notadas tanto no mercado quanto

[‡]Esse tempo é configurável, sendo dependente da filosofia de proteção adotada pela empresa, podendo, assim, variar.

[§]A falha de disjuntor é uma função realizada localmente, logo a latência esperada numa rede local é da ordem de 1ms, podendo variar de acordo com a arquitetura e configuração dos dispositivos.

na pesquisa, como é descrito na Seção 3.2.

3.2 O Novo Modelo para a Rede Elétrica

Além do apelo por sustentabilidade, o novo modelo da rede elétrica a torna mais inteligente. Nota-se uma abordagem para modernização tanto nos consumidores finais, quanto nas subestações, que passam a contar com sistemas digitais. Essa transição para a rede elétrica inteligente traz uma série de benefícios; dentre eles um melhor controle de recursos que, por sua vez permite oferecer um maior nível de confiabilidade do sistema, mesmo em face da demanda crescente. Os consumidores vão ganhar maior controle sobre faturas, além de contar com programas de resposta à demanda [125].

As empresas de energia já começaram a implementar alguns dispositivos inteligentes aonde antes não existiam equipamentos com comunicação. Para a localização e isolamento rápidos de falhas, ou para melhora do sistema de proteção, dentre outras características, a implementação de IEDs tem crescido cada vez mais. Esse dispositivos exercem as funções dos relés, porém incorporam muitas outras como a comunicação entre IEDs, o monitoramento, o controle e a supervisão. Do lado do consumidor as iniciativas compreendem a implementação de *smart meters*, que são medidores inteligentes para permitir a medição automática do consumo, além de cortes e religamentos automáticos. Esses dispositivos entram em uma primeira fase de implementação, tanto para permitir que os clientes tenham maior controle sobre seu uso de energia e custos, quanto para permitir o desenvolvimento de novas áreas das redes elétricas inteligentes.

Percebe-se que tal revolução está ocorrendo baseada em comunicação entre todos os elementos do sistema. Crescem conceitos como a monitoração inteligente de todos os dispositivos do sistema e a transmissão dos fluxos de comunicação e de energia de forma bidirecional, cenário bastante distinto do tradicional. Com as redes elétricas inteligentes, o consumidor passa a ser parte fundamental do funcionamento e controle da rede elétrica. Os consumidores, que no sistema tradicional apenas consomem energia, podem ter, nesse novo modelo, também o papel de produtores de energia elétrica. Ao permitir a geração de energia pelo consumidor, uma rede elétrica inteligente promove uma estreita relação entre compradores e vendedores, clientes e concessionárias. Um fluxo bidirecional de energia e comunicação bem como as capacidades *plug-and-play* são seu objetivo final e permitirão que várias tecnologias possam fornecer, entregar e utilizar os recursos de forma confiável, eficiente e segura.

Ressalta-se que, nesse novo modelo, os dispositivos finais da rede, como os medidores, se tornam mais inteligentes e podem se comunicar diretamente com os centros de controle de dados através da AMI. Assim sendo, a AMI trafegará dados oriundos destes dispositivos de acordo com a função que o dispositivo enxerga para o sistema. Nota-se que o domínio dos consumidores passa a compreender a geração de energia em pequena escala, exigindo

que o tráfego de dados relacionados à geração também seja tratado.

Em geral, a quantidade de dispositivos de automação, tais como medidores inteligentes e IEDs, e a quantidade de dados coletados a partir desses dispositivos aumentam significativamente nas redes elétricas inteligentes. Desta maneira, para que o desenvolvimento da rede elétrica inteligente seja possível, a inteligência e as tecnologias como as de supervisão, controle e proteção, antes existentes apenas em parte do sistema elétrico, se tornam imprescindíveis da geração até o consumidor final [123]. Além disso, o sistema precisa dar suporte às novas propostas de aplicações, tais como a geração de energia de forma distribuída (GD), a criação de *microgrids*, o uso de carros elétricos, um intenso monitoramento da rede elétrica, o uso de medidores inteligentes e a implementação da AMI, entre outros [125]. As áreas mais importantes para esta tese são detalhadas a seguir.

3.2.1 Gerenciamento pelo lado da Demanda e Resposta à Demanda

Segundo o *Electric Power Research Institute* (EPRI), resposta à demanda (*Demand Response* (DR)) é uma mudança temporária no consumo de energia em resposta às condições de fornecimento de energia ou aos eventos na rede [53]. A inclusão de novas fontes de energia e elementos de armazenamento combinados com a necessidade de reduzir os picos de carga impulsionaram a introdução de aplicações de resposta à demanda. Para isso, incentivos monetários podem ser usados de modo a evitar preços elevados de energia. Essas aplicações objetivam prover confiabilidade por meio de uma série de ações que visem reduzir a carga da rede no horário de pico, quando a concessionária está perto da sua capacidade máxima. Por exemplo, pode-se reduzir a quantidade de energia consumida pelos aparelhos durante o período de pico de potência, evitando inclusive apagões. Nesse cenário, o cliente passa a ter um papel ativo no fornecimento de energia elétrica. Esse sistema permite que consumidores transfiram o consumo de energia para momentos fora do horário de pico, tomando vantagem do preço da energia em tempo real, das informações da rede, controle da carga, etc [35].

Conceitualmente, a resposta à demanda é equivalente ao aumento de geração no processo de equilíbrio do sistema. A solução de reduzir o uso de energia e utilizar a geração distribuída quando a oferta de energia é baixa tem ganhado cada vez mais aceitação no mercado. A DR e a *Demand Side Management* (DSM) reduzem a carga e acrescentam a capacidade de geração em caso de emergência. A DR, muitas vezes, permite que a carga passe a receber energia de outras fontes conectadas à rede. Em alguns casos, a DR pode também reduzir o consumo global de energia.

Para que seja possível a implementação da DR, a Automação da Distribuição (AD) precisa também ser implementada. A AD é a ideia de se estender o monitoramento e controle da rede até a distribuição de forma que dispositivos antes não automatizados

passem a sê-lo. Atualmente, empresas de energia estão acostumadas com a gestão de um número limitado de pontos de monitoramento e controle, por exemplo, centenas de subestações e, neste novo cenário, novas tecnologias de comunicação devem ser introduzidas na distribuição a fim de conectar dezenas de milhares de *end points* encontrados na automação da distribuição.

3.2.2 Infraestrutura de Medição Avançada e Faturamento

A AMI é uma infraestrutura integrada composta por medidores inteligentes, infraestrutura de comunicação e sistemas de gerenciamento capazes de permitir comunicação bidirecional entre medidores (consumidores) e concessionária.

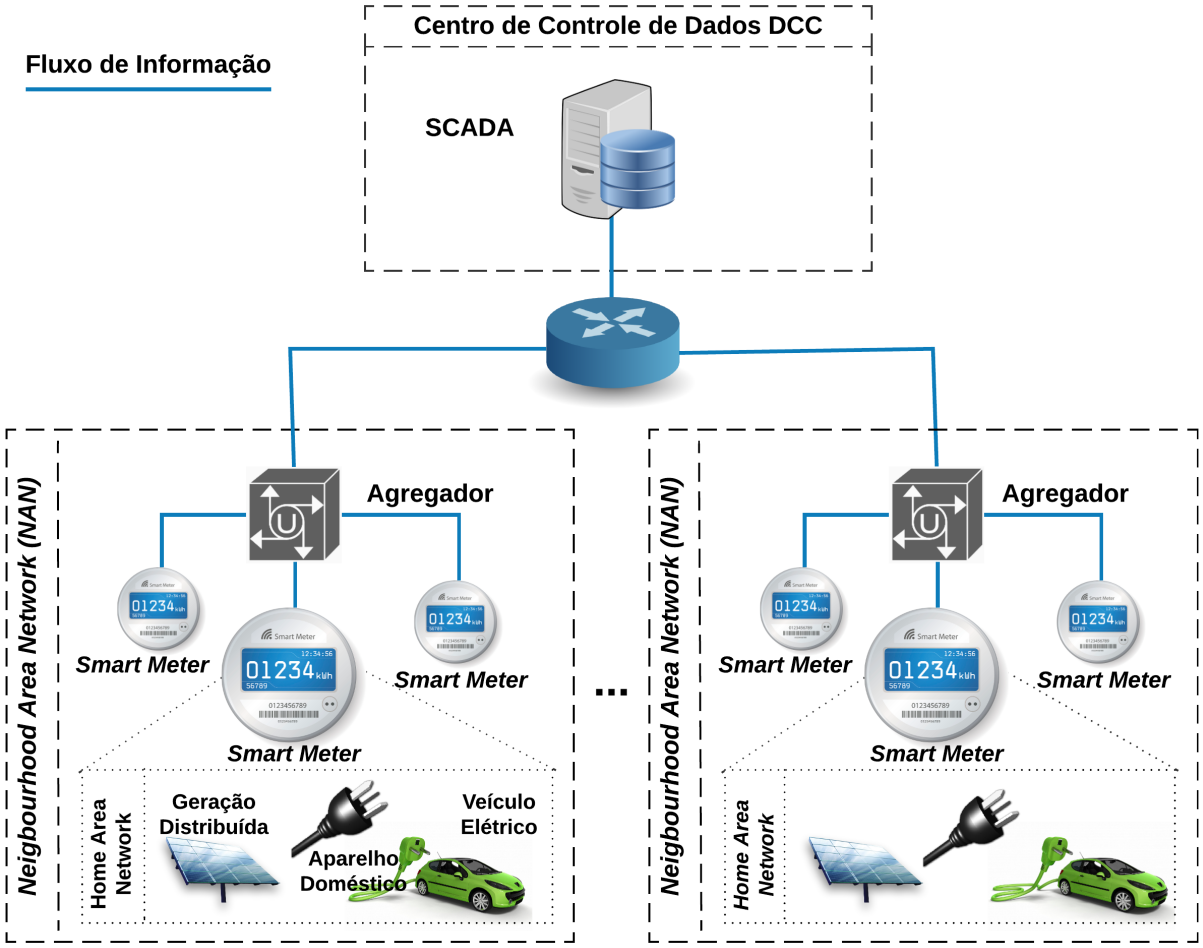


Figura 3.2: Visão detalhada da AMI [121].

A implantação de uma comunicação bidirecional é um elemento chave nesse novo modelo. De fato, a implantação da rede elétrica inteligente começa com uma inserção em massa de medidores inteligentes. Uma infraestrutura comum para as redes de medidores é a ligação direta com o centro de controle de dados (DCC) ou através de um concentrador de medidores, geralmente chamado de agregador (ou *Data Aggregation Point* (DAP)), como

mostra a Figura 3.2. Esta rede local de medidores que se comunica com um concentrador é conhecida como *Neighborhood Area Network* (NAN). O medidor pode ainda fazer parte de uma rede local de automação residencial permitindo o desenvolvimento de aplicações muito mais inteligentes. A rede local pode ainda combinar vários Recursos Energéticos Distribuídos (*Distributed Energy Resources* (DER)). As unidades de DER são as fontes geradoras de energia que podem ser compostas por unidades de geração distribuída (GDs), como painéis solares, e por unidades de armazenamento distribuído, incluindo veículos elétricos (VE) [123, 130].

Com essa infraestrutura instalada, os medidores são capazes de enviar medidas para o DCC e de receber comandos para corte e religamento de energia. Destaca-se que os medidores elétricos tradicionais medem somente o consumo total e não fornecem informações sobre quando e por qual dispositivo a energia foi consumida. Medidores inteligentes fornecem diversas medidas adicionais em tempo real e podem, inclusive, permitir que o preço seja introduzido com base na hora do dia [114].

Nesse cenário, uma das propostas para faturamento é a cobrança dinâmica. Com a existência de mais de um distribuidor de energia elétrica em cada região, surgem dois tipos de usuários: os usuários tradicionais e os usuários oportunistas. Para cada fornecedor de energia, o preço para os usuários tradicionais é fixo, enquanto que o preço para os usuários oportunistas pode ser ajustado dinamicamente, dependendo da demanda de eletricidade dos usuários. Com o surgimento de um novo modelo de usuário de energia elétrica, os oportunistas poderão escolher diferentes distribuidoras com base nos preços fornecidos [37]. Contudo, esse novo tipo de usuário só será possível com integração de todo o sistema elétrico [125] e exige uma comunicação automatizada com a concessionária, já que inclui a presença de medidores multifuncionais, como será tratado adiante.

3.2.2.1 Medidores Inteligentes e a Qualidade de Serviço

Apesar da maior abordagem da literatura estar direcionada para tarifação automática, que não possui exigências muito rígidas de QoS, as medidas fornecidas pelos medidores inteligentes também são usadas para dar suporte às aplicações que exigem requisitos mais rígidos [127]. As aplicações de tarifas em tempo real (RTP), tarifas horo-sazonais (TOU) e tarifa de picos críticos (CPP), ferramentas usadas para tarifação e para resposta à demanda [38], possuem requisitos um pouco mais rígidos.

Além disso, tem-se a introdução da geração distribuída na casa no consumidor, fazendo com que o medidor inteligente passe a desempenhar um papel muito importante também no sistema de geração. Ele monitora o desempenho do sistema de energia, incluindo o fluxo de energia, o uso de energia e a qualidade de energia (medindo harmônicos, desvio de frequência, afundamento/elevação de tensão e transientes das *microgrids* conectadas). Além disso, o medidor pode ser utilizado para fornecer informações que permitam que o

SCADA tome decisões para realizar um controle mais eficiente e/ou economize energia [114]. Nesse contexto, as redes de distribuição passivas tradicionais estão sendo transformadas em redes de distribuição ativas e, com isso, o gerenciamento da rede de distribuição torna-se mais complexo [161].

Com um uso bem projetado dos medidores inteligentes, além das funcionalidades já citadas, torna-se possível também a localização de falhas nos sistemas de distribuição [151, 34] e a detecção de furtos de energia. Todas essas funcionalidades têm características próprias e utilizam a mesma infraestrutura, mas possuem requisitos distintos. Como ilustrado na Figura 3.2, o medidor pode trafegar, além das informações tradicionais de medição, informações relacionadas à GD e aos veículos elétricos, por exemplo. Quando fora das residências, tem-se ainda as estações de carga de veículos elétricos, conhecidas como CS. Essas estações desempenham um papel de comunicação muito similar aos medidores inteligentes multifuncionais.

Ressalta-se que, quando a AMI está trafegando informações de alguma GD, torna-se parte do sistema de proteção e controle, necessitando de requisitos temporais muitos mais rígidos dos que os usados para tarifação. Propostas como as de Lu et al. [128], que usam os medidores inteligentes como parte da GDs, precisam lidar com requisitos de comunicação muito mais rígidos dos que os aceitos para tarifação, cenário bem diferente do mais popularmente conhecido.

O uso de medidores inteligentes e da AMI em conjunto com dados de geração é algo já esperado. Isso porque a implementação de uma segunda infraestrutura para viabilização da comunicação de GDs localizadas em residências, somente por serem caracterizados como um tráfego mais crítico, não se justifica. Uma abordagem com o uso da AMI, de forma inteligente, traz benefícios muito maiores, com informações em tempo real, contribuindo para um maior retorno de investimento e para um custo operacional mais baixo, o que justifica o investimento em longo prazo. Nesse sentido, ter uma rede que atende aos requisitos de QoS estabelecidos por ambas as aplicações, com informações disponíveis em tempo real, torna-se uma premissa básica para que a energia seja entregue de forma confiável para os usuários finais. A grande maioria das falhas no provimento de energia pode ser evitada ou contornada pela proteção da rede elétrica, pelo diagnóstico e monitoramento em tempo real.

3.2.3 Microgrids

A *microgrid* é um novo paradigma que consiste na criação de pequenos sistemas elétricos localizados e compostos por geração, armazenamento e cargas com a ideia de ser autossuficiente. Pode combinar vários recursos energéticos distribuídos para formar um todo. Assim, este conceito inclui GD, armazenamento de energia, conexão entre GDs e

rede externa de energia, mecanismos de controle e cargas [147]. As cargas são quaisquer dispositivos elétricos conectados à rede que necessitem de energia elétrica para funcionar, ou seja, os consumidores de energia. As cargas podem ter características bem diferentes, podendo ser usuários residenciais, comerciais ou industriais.

Nas *microgrids*, são usados controladores e dispositivos conectados aos geradores e às cargas para controlar o funcionamento da rede elétrica. As *microgrids* são controladas e gerenciadas pelo DCC. Com isso, o controle de uma *microgrid* deve considerar três camadas, sendo elas o fluxo de informação, o fluxo de tensão e a camada física (real), mostradas na Figura 3.3.

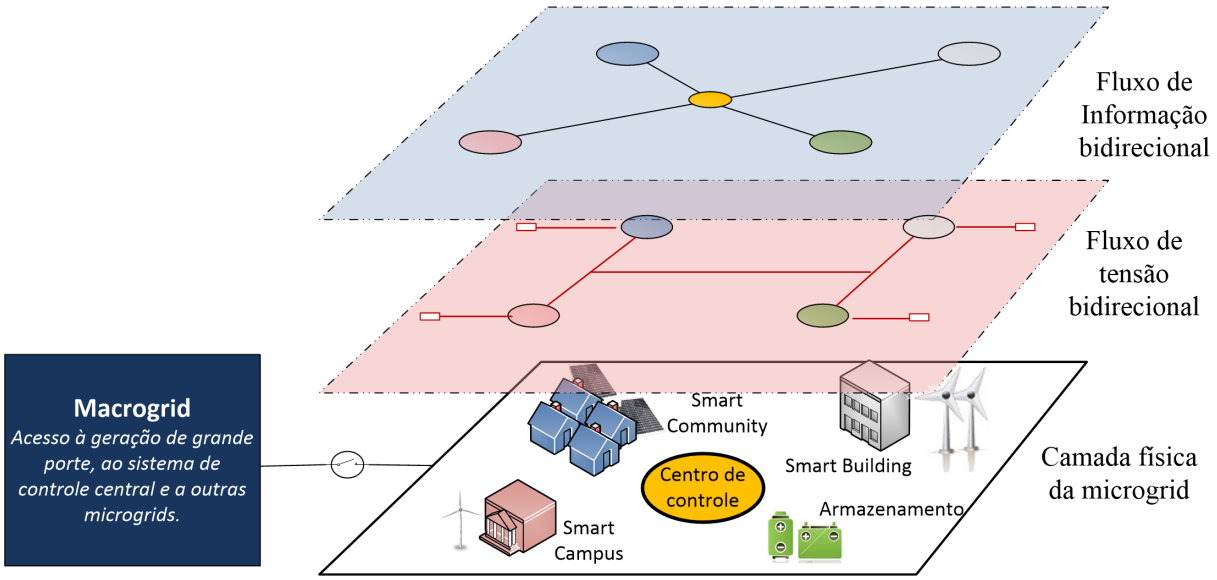


Figura 3.3: Exemplo de uma *microgrid*, onde a comunicação e a distribuição elétrica coexistem, interligando as diversas fontes de geração distribuídas [125].

Em um futuro, a GD e as *microgrids* serão muito comuns em casas e prédios fazendo uso da energia renovável. Quando a capacidade das fontes geradoras exceder a própria demanda, o restante da energia deverá ser exportada para a rede. Uma programação dinâmica e otimizada destes geradores distribuídos pode alimentar as demandas e reduzir o custo total, além de alcançar maior eficiência energética em escala.

Ressalta-se que a *microgrid* tem seus próprios requisitos de controle entre geradores e consumidores de energia devido à sua escala limitada. Os métodos de controle utilizados dentro das *microgrids* podem ser centralizados, distribuídos, hierárquicos ou combinações de vários tipos. O mecanismo de controle deve permitir a adição e remoção flexível de geradores distribuídos em um estilo *"plug-and-play"*, sem perturbar o resto do sistema ou sem a necessidade de reconfigurar todo o sistema. O controle também pode atribuir diferentes prioridades às cargas, que podem ser priorizadas de acordo com a sua importância como mais ou menos críticas [123].

Embora a *microgrid* opere principalmente ligada à rede de distribuição [35], ela pode

operar na forma de "ilha", onde a própria energia gerada pela geração distribuída supre a necessidade da demanda [44]. Esse modo, também chamado de ilhamento, faz com que a *microgrid* funcione de forma autônoma, desligada da rede externa. O ilhamento proporciona continuidade do fornecimento em caso de falhas na rede de transmissão e distribuição de energia. Na técnica de ilhamento adaptativo, clientes que ficam desconectados da fonte primária de energia após a falha são seletivamente conectados a fontes de recurso secundárias, escolhidas com base em:

- quantidade de energia disponível nos recursos de geração distribuídos;
- tempo esperado até reparar a falha;
- histórico de demanda daquele cliente;
- nível de prioridade atribuído àquele cliente.

Assim, os clientes são dinamicamente ajustados durante o tempo de existência da falha. Portanto, esta técnica quebra o sistema elétrico em diversas pequenas ilhas sempre que o sistema está sujeito a uma falha que leve à instabilidade. Essa técnica é um recurso para impedir os apagões no sistema elétrico [44]. De fato, estudos sobre os apagões mais famosos mostram que, se essa técnica já estivesse suficientemente avançada, ou seja, a criação das ilhas fosse ativa ao invés de passiva, muitos desastres poderiam ter sido evitados [43]. A implantação das redes elétricas inteligentes deve garantir a infraestrutura necessária para a implantação dessa técnica, considerando amplo suporte de redes de telecomunicações e incentivo ao uso de fontes renováveis.

3.2.3.1 Comunicação entre Recursos Energéticos Distribuídos na *Microgrid*

Os recursos energéticos distribuídos estão presentes em diversos domínios das redes elétricas inteligentes e são parte fundamental desse sistema. Os principais componentes das *microgrids* podem fazer parte também da resposta à demanda e utilizar a AMI para comunicação. Isso mostra a importância da avaliação e estudo destes recursos dentro das redes elétricas inteligentes. Em várias partes do mundo, empresas e pesquisadores estão reconhecendo os benefícios econômicos, sociais e ambientais da integração dessas tecnologias em sua infraestrutura [80]. No entanto, a inserção desses recursos no sistema não é trivial [130]. Os fabricantes de dispositivos DER, que vão desde painéis solares até *switches* e conversores, estão enfrentando problemas com a comunicação desses recursos similares aos enfrentados em subestações [80].

A possibilidade de comunicação entre todos os dispositivos da *microgrid*, além da comunicação com o supervisório, permite que soluções mais inteligentes, como, por exemplo, a realização de ilhamentos dinâmicos, sejam implementadas. Apesar das vantagens dessa modernização, a escolha do protocolo de comunicação que será usado na *microgrid* para, por

exemplo, monitorar e controlar esses dispositivos, em particular quando estão conectados com o sistema da concessionária de energia, ainda é um grande desafio [80]. Não somente o protocolo, mas qual tipo de rede de comunicação dará suporte para essas aplicações são assuntos essenciais atualmente.

Quando os sistemas de automação compreendiam uma menor parte do sistema elétrico, era comum o uso de protocolos proprietários desenvolvidos por cada fabricante para monitoramento destes dispositivos. A rede de comunicação também acompanha essa ideia, sendo instalada e escolhida de forma diferente para cada projeto. No entanto, os participantes do mercado de energia, como os fabricantes, as concessionárias e os provedores de serviço de energia passaram a ter a necessidade de gerenciar uma quantidade muito maior de dispositivos que agora estão interconectados. Segundo [80], é consenso na área de energia que é muito difícil manter essa infraestrutura com protocolos de comunicação diferentes, pois existe uma maior dificuldade técnica e maiores custos para implementação e manutenção. Consequentemente, fabricantes e concessionárias de energia reconheceram uma crescente necessidade de se definir um padrão internacional que defina as interfaces de comunicação para todos os dispositivos envolvidos nesse sistema [80].

Neste sentido, foi proposta a norma IEC 61850 [177], que apesar de ter sido inicialmente criada para comunicação em subestações, como será visto na Seção 3.4, foi estendida para englobar a automação do sistema de energia como um todo. Em 2009, a sua parte 7–420 [80] foi lançada, abordando a padronização dos recursos de energia distribuídos. Em 2016, foi lançada a parte 90–8 [88] para padronização para veículos elétricos e segue sendo estendida e atualizada. A norma IEC 61850 tornou-se muito popular na área de engenharia de potência, abordando aspectos vitais para a comunicação no sistema de energia [180]. De fato, existe um esforço para incentivar sua utilização também em *microgrids* e não somente em subestações, pavimentando o caminho para a implementação das redes elétricas inteligentes ao fazer integrações entre sistemas de monitoramento, proteção, medição e controle.

3.3 Protocolos de Supervisão

Os protocolos de supervisão usados na comunicação entre dispositivos e supervisório são chamados protocolos SCADA. Esses protocolos têm sido usados em subestações desde a década de 1970. Com o decorrer do tempo, novas funcionalidades foram requeridas pelos supervisórios de sistemas elétricos, e, com isso novos protocolos e padrões surgiram.

O MODBUS, da década de 70 e utilizado até hoje, é extremamente leve e simples, com funcionalidades bastante básicas. Foi criado para comunicação serial e tem versões proprietárias e a versão para Ethernet, intitulada MODBUS TCP. A comunicação é mestre/escravo sempre iniciada pelo SCADA (mestre), e os dispositivos escravos não se comunicam entre si. Os valores de todas as variáveis são sempre estáticos, ou seja, não tem

estampa de tempo referenciando a transição do valor nem informações mais detalhadas. No entanto, exigem pouca capacidade de processamento, possibilitando o uso em *hardwares* de baixo custo.

O DNP3 já é mais robusto do que o MODBUS com características mais avançadas como a possibilidade de selecionar o ponto a ser operado antes da ação (*select-before-operate*) e o suporte ao envio por exceção[¶]. Possui uma concepção orientada a objetos, além do suporte a eventos. Da mesma época que o DNP3 e com basicamente as mesmas funcionalidades tem-se o conjunto de normas e protocolos para sistemas de energia elétrica da IEC 60870-5. São eles IEC 60870-5-101: Tarefas básicas de telecontrole; IEC 60870-5-103: Interface com equipamentos de proteção; IEC 60870-5-104: 101 sobre TCP/IP.

[¶]É chamado de envio por exceção o envio de uma variação em campo para o sistema supervisório assim que ocorre sem aguardar o próximo pedido de *polling*

Tabela 3.1: Comparação entre os protocolos SCADA mais utilizados

Características	**MODBUS**	**DNP3**	**IEC 60870-5**	**MMS (IEC 61850)**
Padronização	Não padronizado	Especificação aberta na indústria (1993)	Norma IEC (1995), revisões em 2000 e 2001	Norma IEC (2005)
Órgão padronizador	Modicon Inc.	DNP User's Group	IEC TC 57 WG 03	IEC TC 57 WG 10, 11 e 12
Meta pretendida	Implementação simples; rápido; frames pequenos	Otimizar o uso de banda e hardware	Otimizar o uso de banda e hardware	Simplificar a integração dos dispositivos
Troca de Dados	Troca de dados por acesso a endereços de registradores	Troca de listas numeradas de pontos	Troca de listas numeradas de pontos	Modelagem de objetos padronizada
Estrutura da informação	Poucos tipos de dados. Registradores com 16 bits no máximo	Permite ao fabricante criar extensões de aplicações específicas	Poucos tipos de dados de aplicação.	Permite criar extensões de aplicações específicas
Variações	Modbus RTU, ASCII, TCP e Plus	DNP serial ou TCP/IP	Serial (101), Ethernet (104)	Ethernet. Mínimo de 100Mbps
Tipos de Dados	Um tipo apenas é enviado por vez	Múltiplos tipos enviados por vez	Um tipo enviado por vez	Múltiplos tipos por mensagem + bits de indicação da qualidade da informação.
Suporte a reportes	Não	Sim	Sim	Sim
Identificação e endereçamento	Endereço do registrador	Índice	Índice	Nomes hierárquicos (orientação a objeto)
Estampa de tempo	Não	Sim	Sim	Sim
Descrição própria dos dados	Não	Poucos	Não	Muitos
Adição de novos modelos	Não	Não	Não	Sim
Serviço de autodescrição	Não	Não	Não	Sim
Mercado dominante	Global	Américas, Austrália e China	Europa	Global

O protocolo MODBUS diferencia-se do IEC 60870-5-101 e do DNP3 principalmente na estruturação interna dos dados. No MODBUS os dados ficam armazenados em uma área de memória definida, porém sem divisão clara entre tipos diferentes de dados. Já nos outros dois protocolos existe uma definição de objetos e os dados armazenados são referenciados por índices e não por endereços de memória. Em resumo, essa diferença altera de maneira significativa o formato das mensagens de requisição de dados.

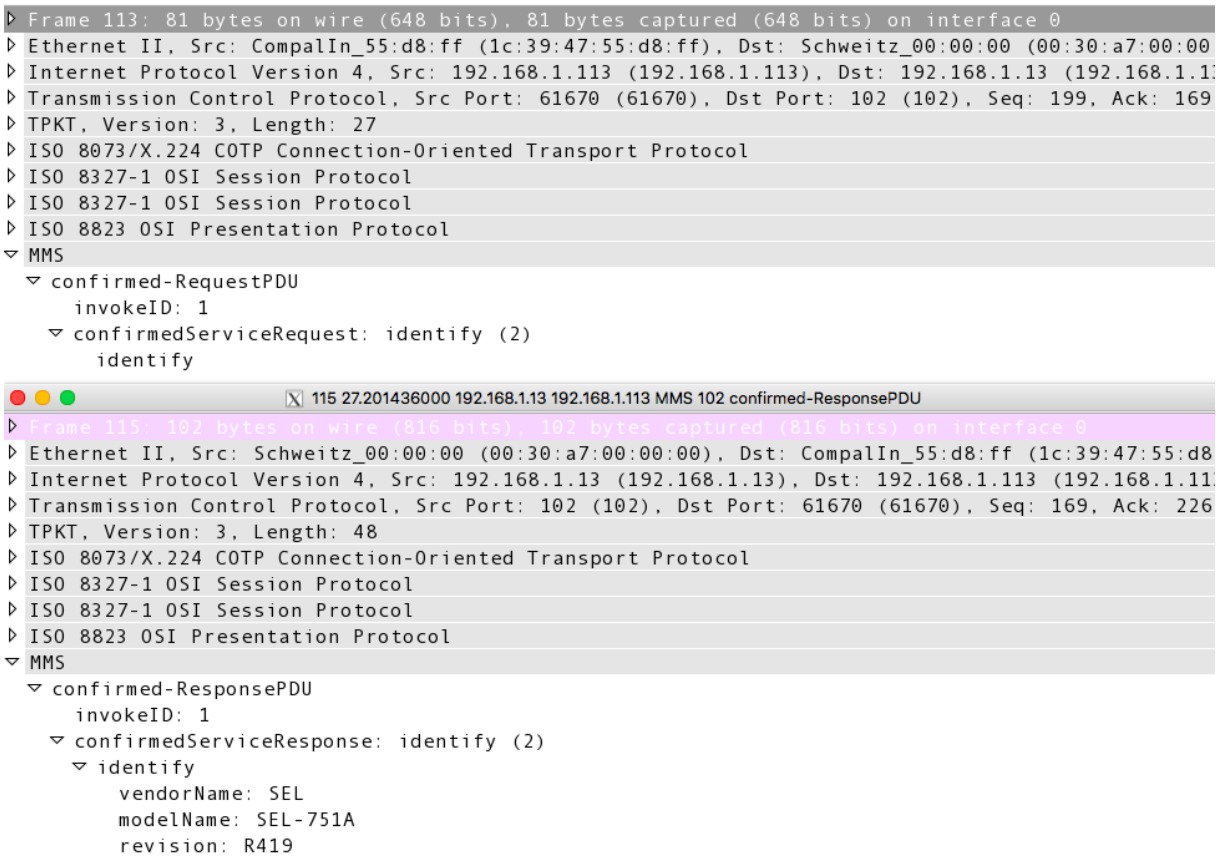


Figura 3.4: Captura de mensagem MMS no início da comunicação com o supervisório, na qual são enviadas informações que identificam o dispositivo, com o serviço `Identify`.

Ressalta-se que, além das suas vantagens perante os outros protocolos, ele faz parte da norma IEC 61850 que tem sido definida como base para a implementação das redes elétricas inteligentes com um apelo por interoperabilidade.

Um outro protocolo com destaque atualmente é o MMS [86]. Diferente dos outros protocolos, o MMS estabeleceu um outro conceito para distinguir e separar os dados estruturados sobre o domínio da norma IEC 61850, que define a semântica da troca de dados entre aplicações e servidores no sistema elétrico de potência. Como foi visto na Seção 3.4, a norma IEC 61850 definiu os tipos de objetos de acordo com uma estrutura hierárquica que agrupa as informações por funcionalidades em comum. Enquanto no protocolo DNP3, separam-se os objetos apenas por tipo de dados (binário, analógico, contadores), na norma IEC 61850, realiza-se uma separação mais funcional onde o tipo de objeto já indica a sua função dentro do equipamento. Além disso, o MMS possui todos

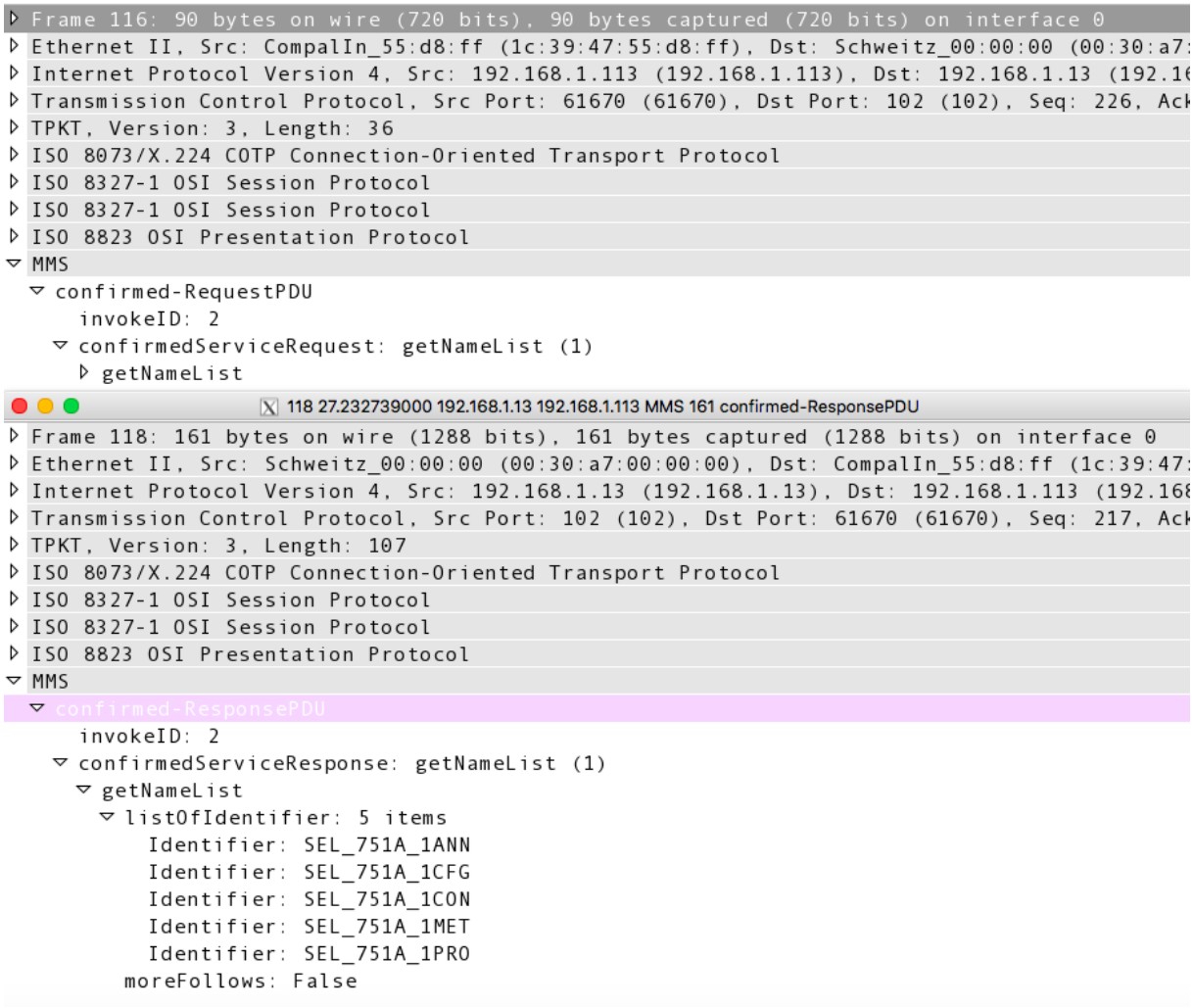


Figura 3.5: Captura de mensagem MMS no início da comunicação com o supervisório, na qual o processo de auto-descrição do dispositivo é realizado com o serviço `GetName`.

os recursos citados para o DNP3 e outros adicionais. Possui serviços mais inteligentes, como o envio para o supervisório da confirmação que o comando foi realizado com sucesso, envio de reportes (chamado envio por exceção no DNP3) *bufferizados*. Essas e outras características são resumidas na Tabela 3.1.

Os outros protocolos, como o DNP3, não possuem a capacidade de *bufferizar* o evento, logo, se houver falha na comunicação a variação é perdida. Além disso, o MMS possui os serviços `Identify` (Figura 3.4) e `Get` (Figura 3.5) que possuem a capacidade de identificar um IED e implementar o processo de auto-descrição (*self-description*), serviço que provê a capacidade de explorar o conteúdo dos dispositivos de forma automática, sua principal vantagem quando comparado aos outros. Informações sobre os dispositivos, como modelo e fornecedor, são trocados com o serviço `Identify`.

3.4 A Norma IEC 61850

A norma IEC 61850 [177], desenvolvida pelo Comitê Técnico 57 (TC57) da *International Electrotechnical Commission* (IEC), padroniza a comunicação do sistema de proteção e automação de subestações, independente de fornecedores [150].

Com a evolução dos relés de proteção, que passaram a possuir características microprocessadas, o Sistema de Automação de Subestações (SAS) vem mudando para se adaptar a esse novo cenário. Os relés passam a ter funções adicionais e, além da proteção, passam a controlar e registrar eventos, medidas, etc.

Assim, os relés digitais modernos, agora intitulados IEDs, passaram a possuir a capacidade de se comunicar entre si, funcionando como um nó na rede, além da comunicação já tradicional com o supervisório, componente do SAS responsável pelo monitoramento e controle dos IEDs. Nesse contexto, o comando de atuação deixa de passar pelo fio rígido de cobre para trafegar por uma rede de dados.

Para permitir integrações entre sistemas de monitoramento, proteção, medição e controle, ela é baseada em três aspectos básicos:

1. Modelagem de informação: os tipos de dados que devem ser trocados, onde a norma define classes e nomes padronizados para qualquer dado a ser transmitido.
2. Modelagem de serviços: as ações que devem ser realizadas sobre os dados como a leitura ou a gravação de uma informação.
3. Protocolos de comunicação: o mapeamento dos modelos de informação e serviço.
4. Linguagem de configuração: a forma com que os dispositivos devem ser configurados.

A norma IEC 61850 modela a interconexão dos elementos de automação, representando em um plano lógico todos os elementos envolvidos na comunicação do sistema. Desta maneira, ela possui um conjunto de funções que interoperam de forma distribuída, podendo estar alocadas em um ou mais IED conectados em rede. Este mesmo princípio é usado para integrar funções de medição, de controle e de proteção. Isso possibilita a substituição dos cabos de controle por redes de comunicação, reduzindo o custo global no comissionamento, na engenharia, no monitoramento, na manutenção e no diagnóstico [150]. A norma também determina requisitos temporais rígidos para a comunicação. Esses requisitos estão detalhados na Seção 3.4.3.

A especificação de um SAS baseada em IEC 61850 é, até certo ponto, semelhante à especificação de um sistema convencional. Devem ser fornecidas informações sobre o diagrama unifilar da subestação[‖], as funcionalidades requeridas, os requisitos de desempenho,

[‖]O diagrama unifilar é uma representação simplificada das interligações entre equipamentos, onde os

as interfaces com o processo e com outros IEDs, além de protocolos, condições ambientais, índices de confiabilidade admitidos ou critérios de tolerância a falhas aceitáveis, etc. Seu uso, porém, demanda adicionalmente outros requisitos, como características do sistema de comunicação, além de toda a documentação em linguagem de configuração de subestações (*Substation Configuration Language* (SCL)) e procedimentos de teste específicos para o SAS que está sendo adquirido [150].

Devido à visibilidade da norma e ao fato de ser baseada na comunicação de dados em rede, preocupações inerentes à redundância e ao restabelecimento da rede em caso de falha têm aumentado. Alguns métodos utilizados em subestações são discutidos no Apêndice C.

3.4.1 Modelagem de Informação

Os dispositivos são representados de acordo com a sua função, ou seja, têm suas funcionalidades textualmente descritas. Desta forma, o modelo de dados especificado pela norma define os atributos dos dispositivos físicos de uma subestação elétrica e das funções envolvidas. O modelo de dados é baseado numa estrutura de dados orientada a objeto [189], utilizando os seguintes conceitos:

- Classe: representação de um conjunto de objetos com características afins.
- Objeto/instância de uma classe: serve para armazenar estados através de seus atributos e interagir com outros objetos através de mensagens;
- Atributos: são as características de um objeto;
- Métodos: são as funções implementadas nos objetos, como por exemplo, a capacidade de enviar e receber mensagens;
- Herança: funcionalidade de uma classe estender a outra classe, herdando seus métodos e atributos. Dessa forma, tem-se como vantagem o reaproveitamento das características e atributos das classes ascendentes.

A norma define dispositivos físicos e lógicos. Um dispositivo físico é definido como um dispositivo que se conecta à rede através de um endereço específico e possui um hardware e um conjunto de classes que caracterizam o seu comportamento [85]. Dentro de cada dispositivo físico pode haver um ou mais dispositivos lógicos (*Logical Device* (LD)) que servem para especificar um grupo com as mesmas características, por exemplo: controle, medição, nível de tensão, subestação ou vão de que faz parte, veículos elétricos carregando, GD conectada, etc.

aspectos do circuito elétrico como localização dos elementos, percursos de uma instalação, condutores, distribuição da carga, proteções, dentre outros são contemplados.

Por sua vez, cada dispositivo lógico é formado por um conjunto de nós lógicos (*Logical Node* (LN)). Cada nó lógico contém objeto de dados (*Data Objects* (DO)), compostos por atributos (*Data Attributes* (DA)). O objeto de um nó lógico pode representar uma função de automação e controle ou um dispositivo. Por exemplo, um objeto seria um disjuntor específico ou uma chave seccionadora. Da mesma forma, uma proteção de sobrecorrente também seria definida através de um objeto. O atributo é o valor desse objeto, como o estado fechado ou aberto da posição de um disjuntor. Assim, seguindo o modelo de orientação a objeto, a norma disponibiliza uma visão hierarquizada para classificar as funções exercidas por cada dispositivo da rede, sendo iniciada pelo dispositivo físico até alcançar o atributo de dados. Além disso, com o intuito de agrupar as características das classes, a norma padroniza os nós lógicos [82] em grupos. Cada nó lógico possui uma denominação iniciada com a letra do grupo que faz parte. É dessa forma que a funcionalidade do nó lógico é textualmente descrita com a primeira letra indicando de qual grupo faz parte e as restantes indicando seu papel. Por exemplo:

- **P**XXX - Funções de Proteção
  - **PTOC** - Proteção de Sobrecorrente (***T****ime* ***O****ver****C****urrent*)
  - **PDIS** - Proteção de Distância (***DIS****tance*)
- **C**XXX - Controle
  - **CSWI** - Controlador de Chaveamento (***SWI****tch*)
- **M**XXX - Medições
  - **MMXU** - Medição Operativa e Indicativa (***M****easurement* ***U****nit*)
- **T**XXX - Transformadores e Sensores
  - **TCTR** - Transformador de Corrente (***C****urrent* ***TR****ansformer*)
  - **TVTR** - Transformador de Potencial (***V****oltage* ***TR****ansformer*)
- **X**XXX - Interface com chaves de processo
  - **XCBR** - Disjuntor (***C****ircuit* ***BR****eaker*)
  - **XSWI** - Seccionadora (***SWI****tch*)
- **S**XXX - Supervisão e Monitoramento
- **G**XXX - Funções genéricas
- dentre outras

A Figura 3.6 ilustra a estrutura hierárquica do modelo de dados e provê um exemplo de nomes de objetos para identificar o estado de um disjuntor. De forma geral, cada classe tem um nome único. Esses nomes são determinados pela norma e funcionalmente ligados à finalidade do sistema de potência. A Figura 3.6 apresenta um disjuntor que é modelado por um nó lógico chamado `XCBR` (***C**ircuit **BR**eaker*) que contém uma variedade de objetos de dados, entre os quais, `Pos` para indicações associadas à posição do equipamento e `Mod` relacionado ao modo de funcionamento deste. O objeto de dados `Pos` possui, por exemplo, o atributo `StVal`, que indica o estado atual do disjuntor (intermediário, aberto, fechado ou falha).

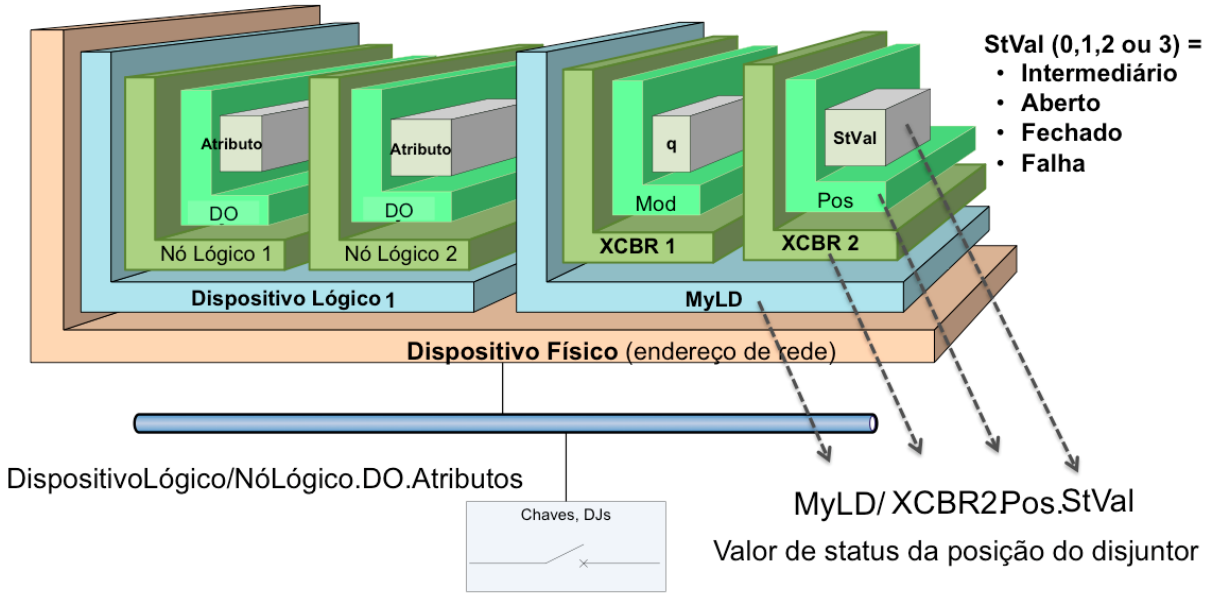


Figura 3.6: Exemplo de uma referência de nome de objetos do IEC 61850 e sua estrutura hierárquica.

Com base no nome, é possível identificar por qual "caminho" pode-se chegar até o dado, ou seja, em qual dispositivo físico, dispositivo lógico e nó lógico está o dado desejado. Nesse modelo de dados, qualquer dado pode ser diretamente acessado, usando para isso o seu caminho. Pode-se referenciar o nome de objetos da seguinte forma:

`DispositivoLógico/NóLógico.ObjetodeDados.AtributosdeDados`

Na Figura 3.6, o termo `MyLD` representa o dispositivo lógico. O objeto disjuntor é representado pelo nó lógico `XCBR2`, o termo `Pos` representa o objeto de dados e finalmente o termo `stVal` representa o atributo de dados.

Com isso tem-se:

`MyLD/XCBR2.Pos.StVal`

Então, o caminho acima seria usado para acessar informações sobre o estado de um disjuntor. Esse modelo de informação hierárquica é ilustrado também na Figura 3.7, onde é mostrado o nó lógico `XCBR` que é a raiz ao nível dos nós lógicos e a árvore completa desse nó com as referências a essa raiz [85].

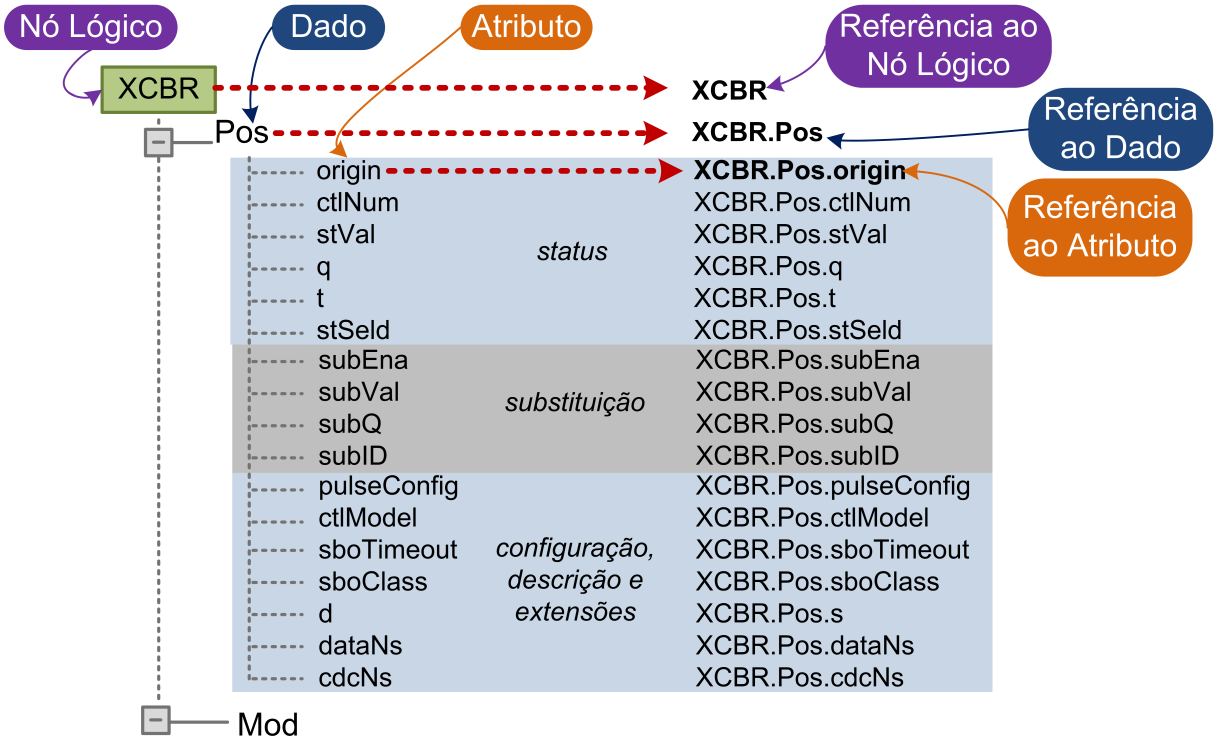


Figura 3.7: Exemplo simples de modelagem de um IED [85].

Para criar objetos e diferenciar os nós lógicos com o mesmo nome, um sufixo e/ou prefixo podem ser usados. Por exemplo, para o nó lógico `XCBR` pode-se usar um sufixo de 1 a n pra diferenciar cada disjuntor, por exemplo, `XCBR1`...`XCBRn`. Um prefixo pode também ser utilizado na mesma infraestrutura.

Por exemplo:

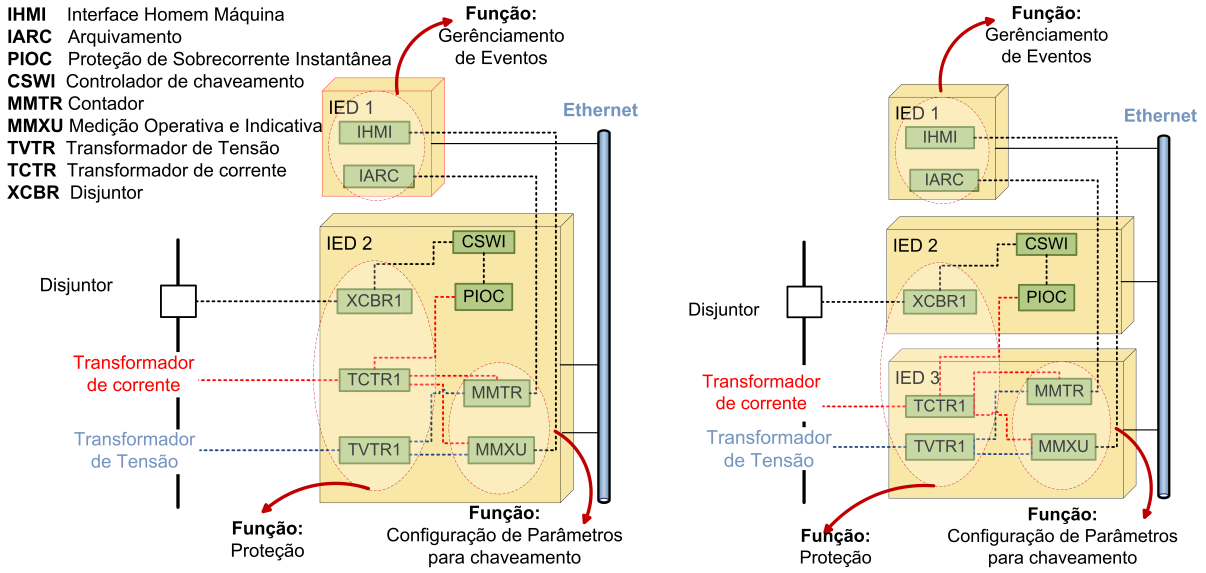
```
MyLD/Bay1XCBR2.Pos.StVal
```

Onde `Bay1` é o prefixo, `XCBR` é a classe que descreve o nó lógico e `2` o sufixo.

Ressalta-se que estes objetos são agrupados em *datasets*. As informações de rede, como endereçamento, prioridades, etc, são atribuídas aos *datasets* que, por sua vez, podem possuir vários objetos.

Em alto nível, a tarefas que devem ser executadas, sendo utilizadas para controlar, monitorar e proteger o sistema são realizadas por funções. Estas funções são formadas por um conjunto de nós lógicos com características afins. Os IEDs são multifuncionais e, portanto, podem disponibilizar várias funções em um único elemento, como mostra a

Figura 3.8(a). Além disso, uma função pode não estar localizada em um único dispositivo, mas distribuída entre vários dispositivos físicos, conforme Figura 3.8(b), se comunicando através da rede de comunicação.



(a) Distribuição em 2 IEDs.

(b) Distribuição em 3 IEDs.

Figura 3.8: Exemplo de distribuição de funções no IED.

3.4.2 Linguagem de configuração de Subestações (*Substation Configuration Language* - SCL)

A norma IEC 61850 padroniza uma linguagem de descrição que norteia a configuração do sistema. Isto significa dizer que são configurados desde os canais de comunicação até a alocação de funções para os sistemas de automação. Ela é designada como Linguagem de Configuração de Subestação (*Substation Configuration Language* - SCL) [79]. A SCL é baseada em *eXtensible Markup Language* (XML) [79]. Desta forma, incorpora conceitos de herança e referências abstratas de linguagens orientadas a objetos, encaixando-se com a modelagem dos dispositivos descrita na norma. Seu objetivo principal é padronizar os atributos de configuração, ou seja, criar uma nomenclatura uniformizada, de maneira a permitir configurações de IEDs com maior segurança e confiabilidade. O intuito é manter a interoperabilidade, garantindo a troca de dados entre IEDs independente do fabricante.

A linguagem SCL é composta pelos seguintes arquivos de configuração [79], no que diz respeito à configuração dentro de subestações:

1. *IED Capability Description* (ICD): arquivo (.icd) que contém todas as características e funcionalidades do IED. Nele, estão descritas todas as funções que poderão ser

utilizadas nos dispositivos. Esse arquivo deve ser fornecido pelo fabricante do IED com o intuito de ser uma espécie de *template*;

2. *System Specification Description* (SSD): arquivo (.ssd) que contém a especificação completa de um sistema de automação de subestações, incluindo o diagrama unifilar para a subestação, os seus nós lógicos e o modelo de tipo de dados requeridos;

3. *Substation Configuration Description* (SCD): arquivo (.scd) é composto pela união do arquivo que especifica a capacidade dos IEDs (arquivo .icd) com o arquivo que especifica o sistema (arquivo .ssd). O arquivo .scd descreve detalhadamente a subestação no que tange à comunicação, e contém uma seção de configuração de comunicação e uma seção de descrição da subestação. Desta maneira, este arquivo pode conter, por exemplo, as seguintes informações: aonde está alocado cada nó lógico do sistema, endereços de rede, endereços de grupos *multicast*, etc;

4. *Configured IED Description* (CID): é o arquivo (.cid) que contém a descrição de configuração de um IED específico. Este arquivo possui as funções parametrizadas ou habilitadas pelo usuário no IED. É este arquivo que é configurado em cada IED individualmente.

A formatação em XML permite que a descrição da configuração de um IED seja passada a uma ferramenta de engenharia de aplicação e comunicação, no nível de sistema, e retorne com a descrição da configuração do sistema completo para a ferramenta de configuração do IED [149, 27].

A Figura 3.9 exemplifica o processo de composição dos arquivos citados e apresenta o configurador do sistema, o qual é uma ferramenta de gerenciamento para fazer as configurações. No ambiente de trabalho da engenharia têm-se os seguintes passos numerados na figura:

- *Passo 1*: A configuração do sistema de automação, contendo o diagrama unifilar, os nós lógicos utilizados e o modelo de tipo de dados necessários são entregues à ferramenta de configuração do sistema (configurador do sistema), na forma do arquivo .ssd.

- *Passo 2*: O arquivo .icd contendo a capacidade dos IEDs com todas as características e funcionalidades destes deve também ser entregue ao configurador do sistema.

- *Passo 3*: De posse desses dois arquivos, .icd e .ssd, o configurador do sistema gera o arquivo .scd com o conteúdo descrito acima. Este proverá os recursos necessários para que a ferramenta de configuração do IED (configurador do IED) defina o arquivo CID com a configuração dos IEDs.

- *Passo 4*: O configurador do IED gera os arquivos .cid, os quais especificam os parâmetros com os quais o IED deve operar.

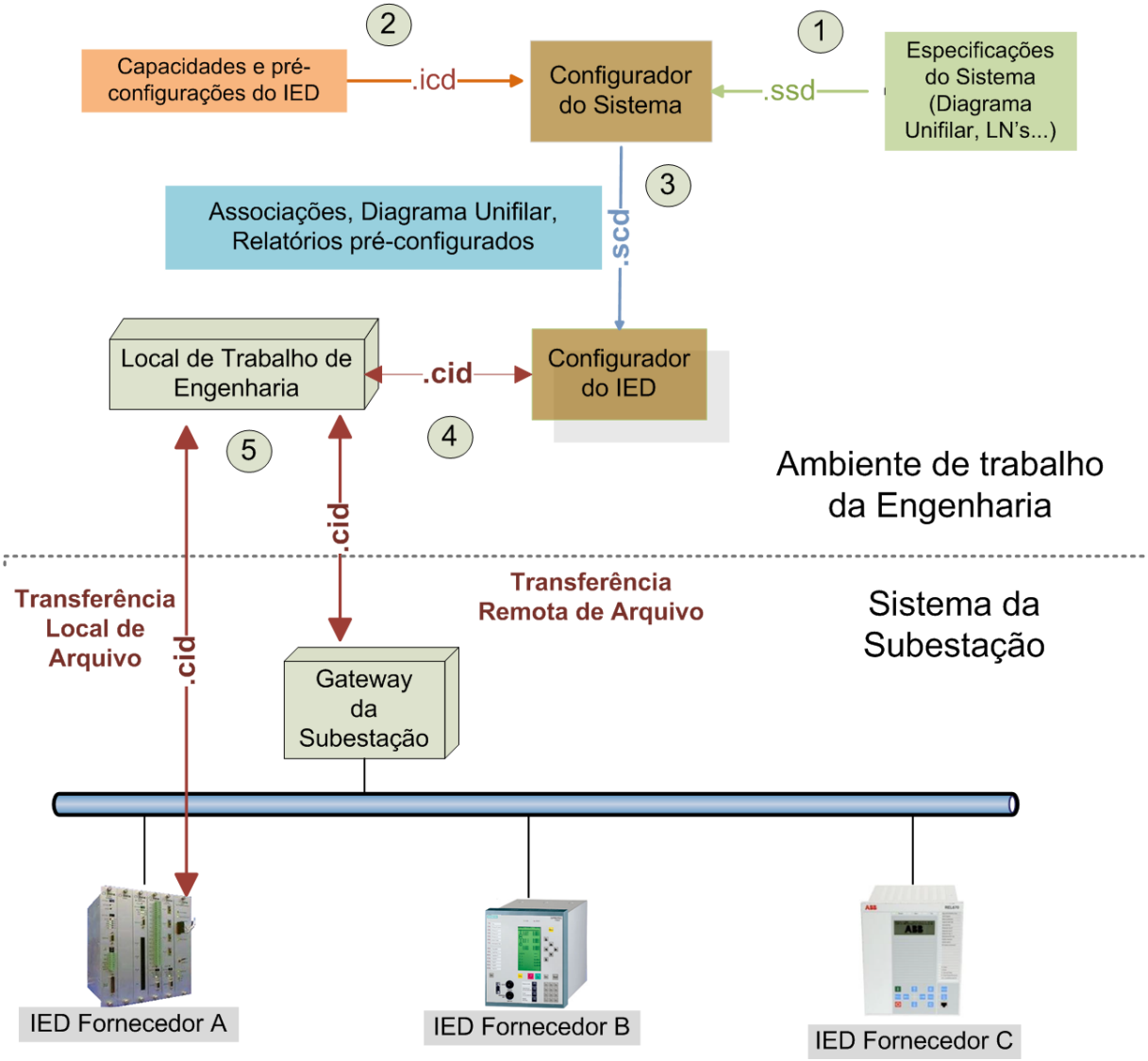


Figura 3.9: Arquitetura de composição dos arquivos da linguagem SCL [79].

- *Passo 5*: Por sua vez, pode-se distribuir o arquivo de forma local (diretamente para o IED) ou de forma remota, enviando o arquivo para que um *gateway* o distribua.

A linguagem SCL, em seu escopo completo, permite descrever modelos que abordam:

- Estrutura do sistema primário (potência): relata a forma pela qual os equipamentos estão conectados e quais funções serão utilizadas;
- Sistema de comunicação: descreve como os IEDs serão conectados à rede;
- O nível de aplicação da comunicação: informa qual será o agrupamento de dados a ser transferido, a maneira pela qual os IEDs acionarão o envio e qual o serviço escolhido;
- A configuração de cada dispositivo lógico no IED, os nós lógicos com suas respectivas classes e tipo de dados, relatórios e conteúdo dos dados;

- Definições de tipo para cada instância de nó lógico;
- Relacionamento entre as instâncias dos nós lógicos e seus respectivos IEDs.

3.4.3 Modelagem da Comunicação

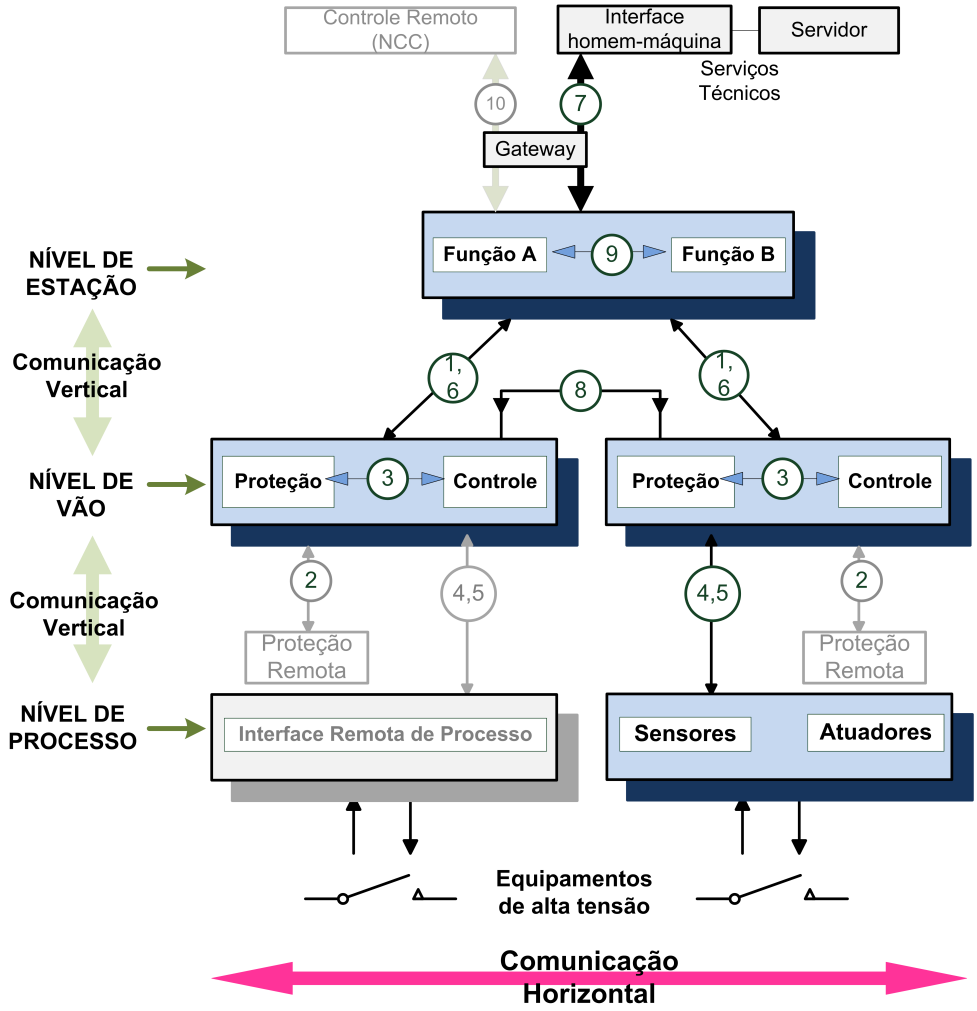
Com relação à comunicação e ao sistema de automação, a norma recomenda que se estruture o sistema em diferentes níveis hierárquicos [78], a saber: estação (*station level*), vão (*bay/unit level*), ou processo (*process level*). Dessa forma, as funções de proteção, controle e supervisão podem ser logicamente alocadas. Estes níveis compreendem:

- Funções de nível de processo: todas as funções que interagem com os dispositivos do nível de processo, tipicamente I/O remotos, transformadores, seccionadoras e disjuntores.
- Funções de nível de vão: todas as funções que interagem com os dispositivos típicos de nível de vão, como relés de proteção, medidores de energia, equipamentos de teleproteção e oscilógrafos.
- Funções de nível de estação: funções que utilizam dados de um vão ou de toda a subestação para interagir com o equipamento primário, com o supervisório ou com o operador. Os dispositivos nesse nível compreendem computadores, a interface homem-máquina, e interfaces com enlaces para o centro de controle.

É importante observar que essa separação em níveis hierárquicos é lógica. Fisicamente, existe apenas um enlace físico por onde trafegam as informações dos barramentos de estação, vão e processo para uma implementação completa da IEC 61850 [78]. Estes níveis hierárquicos podem ser compreendidos através da interpretação da Figura 3.10, que ilustra a arquitetura de comunicação, assim como a separação lógica em níveis dos elementos e as principais interfaces entre esses.

Além de especificar as interfaces, a norma também define o modo de comunicação que deve ser realizado pelos dispositivos para requisitar um serviço como envio de um evento ou de valores de tensão e corrente, comandos, manipulação de *logs*, leitura de informações, dentre outros. Podem ser de dois tipos [81]: *Two Party Application Association* (TPAA) ou *Multicast Application Association* (MCAA), como ilustrado na Figura 3.11.

Observa-se que o modelo de comunicação TPAA transmite os serviços de pedidos e resposta através de uma troca bidirecional de informação ponto-a-ponto orientada a conexão. A conexão é confiável, dispondo de um controle de fluxo fim-a-fim. O modelo de comunicação MCAA permite uma troca de informação unidirecional entre um publicador (*publisher*) e um ou mais assinantes (*subscriber*). O assinante deve ser capaz de detectar perdas ou duplicação da informação recebida.

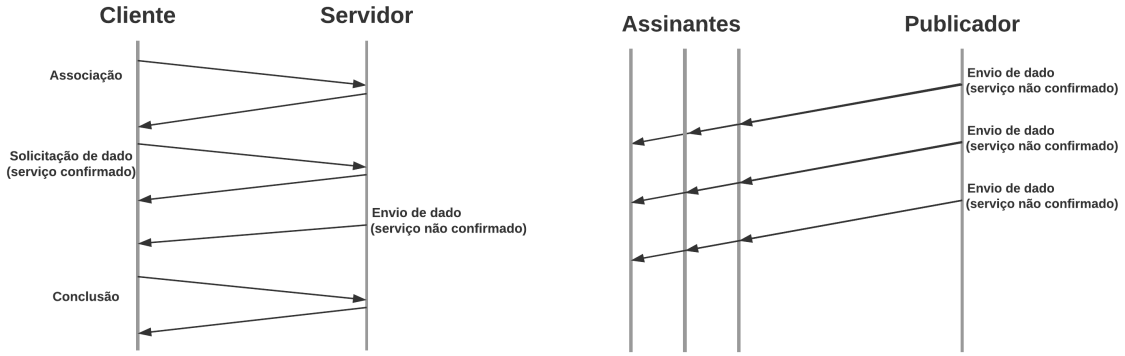


1) Troca de dados de proteção entre os níveis de vão e de estação;
2) Troca de dados de proteção entre os níveis de vão e de proteção remota;
3) Troca de dados dentro do nível de vão;
4) Troca de dados instantânea do TC e TP entre os níveis de processo e de vão;
5) Troca de dados de controle entre os níveis de processo e de vão;
6) Troca de dados de controle entre os níveis de vão e de estação;
7) Troca de dados entre o nível de estação e a estação de trabalho remota do engenheiro;
8) Troca direta de dados entre diferentes níveis de vão, especialmente para funções rápidas como as de intertravamento;
9) Troca de dados dentro do nível de estação;
10) Troca de dados de controle entre os dispositivos e o centro de controle remoto.

Figura 3.10: Níveis de uma subestação e interfaces de comunicação entre estes níveis de acordo com a arquitetura proposta na IEC 61850 [78].

O modelo TPAA é usado para a comunicação das mensagens MMS [3], descritas na Seção 3.4.3.1 e o MCAA para mensagens *Generic Object Oriented Substation Event* (GOOSE) [86], descritas na Seção 3.4.3.2. As mensagens *Sampled Values* (SV) [86] podem usar os dois modelos dependendo da aplicação [81], e também são descritas na Seção 3.4.3.2.

Os dois modelos devem permitir que os requisitos temporais de comunicação, estabele-



(a) TPAA, baseado em mensagens *unicast*.

(b) MCAA, baseado em mensagens *multicast*.

Figura 3.11: Princípios de comunicação TPAA e MCAA da norma IEC 61850 [81].

cidos pela IEC 61850, sejam atendidos. A garantia de atendimento aos valores de atraso descritos na norma é imprescindível para a correta execução das funções dos dispositivos e do desempenho geral do sistema. Estes requisitos temporais são definidos de acordo com o tipo de mensagem e estão descritos na Tabela 3.2 que resume os tipos de mensagens disponibilizas pelo padrão. Suas respectivas classes de desempenho são [78]:

- Classe P1: Refere-se ao nível de vão de distribuição ou aos níveis cujo requisito temporal não seja de alta criticidade;
- Classe P2: Aplica-se ao nível de vão de transmissão se não especificado de outra forma pelo cliente.
- Classe P3: Designada para o nível de vão de transmissão com características críticas de sincronização.

Por exemplo, para as mensagens do Tipo 1A (*trip*), por ser considerada a mensagem rápida mais importante, são definidos limites temporais de 3ms para as classes P2 e P3 e 10ms para a classe P1. As mensagens do Tipo 6A, utilizadas para sincronização de tempo no barreamento de estação, são definidas para uma precisão com desvio temporal de módulo 1 ms no máximo. Já as mensagens do Tipo 6B, usadas para sincronização temporal no barramento de processo, toleram para a precisão da amostra desvios temporais de módulo 4 μs e 1 μs, e +/- 25 μs de acordo com aplicação.

3.4.3.1 *Manufacturing Message Specification*

O MMS é um protocolo da camada de aplicação projetado para suportar comunicações entre dispositivos programáveis em um ambiente de Manufatura Integrada por Computador (*Computer Integrated Manufacturing* (CIM)) [2]. É padronizado pela ISO 9506 [3] e

Tabela 3.2: Tipos de mensagens suportadas pelo padrão IEC 61850 [78].

Tipo	**Descrição**	**Exemplo**	**Classes**	**Mensagem e Requisitos Temporais**
1A	Mensagens Rápidas	*Trips*	P2 e P3	GOOSE (3ms)
			P1	GOOSE (10ms)
1B	Mensagens Rápidas (outras)	Comandos, Mensagens Simples	P2 e P3	GOOSE (20ms)
			P1	GOOSE (100ms)
2	Velocidade Média	Valores de Medidas	-	MMS (100ms)
3	Velocidade Baixa	Alteração de Parâmetros	-	MMS (500ms)
4	Rajada de Dados	Valores amostrados de tensão e corrente	P2 e P3	SV (3ms)
			P1	SV (10ms)
5	Transferência de Arquivos	Arquivos	-	MMS($\geq$1000ms)
6A	Sincronização de Tempo A	Sincronização (*station bus*)	-	TimeSync (+–1ms)
6B	Sincronização de Tempo A	Sincronização (*process bus*)	-	TimeSync ($\leq 25\ \mu s$)
7	Mensagem de Comando	Comandos da estação HMI	-	MMS(500ms)

desenvolvido e mantido pelo Comitê Técnico ISO 184 (TC184). Foi incorporado à norma IEC 61850 [86] com o objetivo de efetuar as funções de controle e supervisão dos dispositivos de automação do sistema elétrico. Com isso, não só a supervisão dos dispositivos é feita com esse protocolo mas também os comandos realizados a partir do supervisório (local e remoto).

O MMS roda sobre TCP/IP ou OSI dependendo da aplicação. Em geral, atende os sistemas de aquisição de dados de um sistema de supervisão, como, por exemplo, o sistema SCADA. É orientado a conexão e a troca de informações entre dispositivos segue o modelo cliente-servidor, conforme a Figura 3.11(a), com uma modelagem orientada a objetos. O servidor MMS representa os objetos aos quais o cliente MMS pode acessar, como os vários IEDs de uma subestação. Centros de controle e monitoramento como o SCADA geralmente são definidos como clientes MMS. Um *gateway* de subestação ou outro dispositivo inteligente também pode ser definido como cliente. Ressalta-se que os dispositivos envolvidos na comunicação podem desempenhar ambas as funções (cliente e servidor) simultaneamente [2]. Exemplos são os supervisórios locais (*gateways*) que estabelecem uma conexão para o centro de controle e ao mesmo tempo requisitam informações de diversos dispositivos na subestação. A norma IEC 61850 intitula esse tipo de comunicação como sendo vertical, conforme Figura 3.12.

As operações MMS realizadas pelas entidades envolvidas são definidas como serviço. Serviços são usados também para estabelecer e/ou terminar conexões e para o tratamento

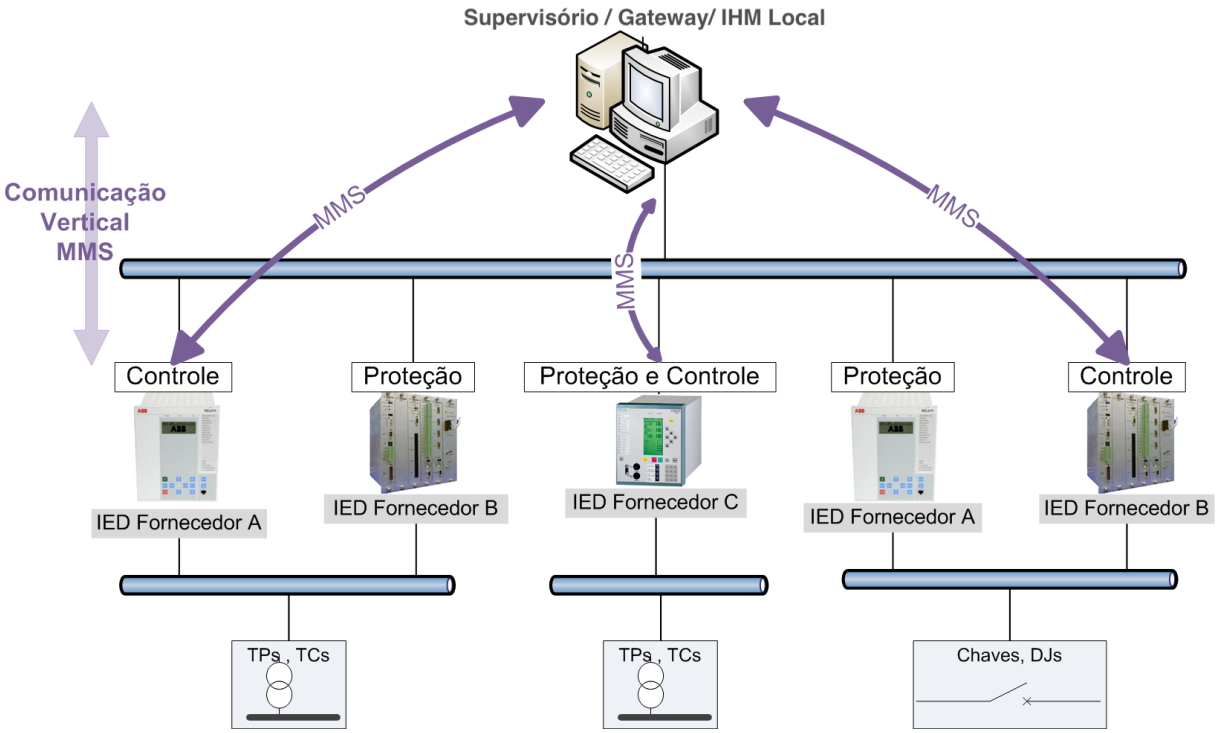


Figura 3.12: Comunicação dentro de uma subestação via MMS, através da troca de mensagens entre o cliente e o servidor.

de erros entre dois nós MMS. Duas aplicações MMS estabelecem uma conexão usando o serviço de inicialização. Este processo consiste na permuta de alguns parâmetros e a negociação de outros. Os serviços são organizados em grupos, dos quais uns necessitam de confirmação e outros não, variando de simples a altamente complexos. Não é esperado que todos esses serviços sejam suportados por todos os dispositivos [2]. O subconjunto a ser suportado é limitado pela norma IEC 61850 e pode ser limitado pelo implementador [2]. Os serviços mais usados e conhecidos na norma IEC 61850 são [86]:

1. `Initiate`: utilizado para inicializar a comunicação entre cliente e servidor e contém, entre outras informações, quais serviços são implementados ou não nos pares da comunicação.

2. `Identify`: utilizado para identificar o dispositivo descrevendo o modelo, o fornecedor e o *firmware*.

3. `Read`: utilizado para ler o objeto IEC 61850 (podendo ser um conjunto de dados (*Data Sets*) ou o próprio dado).

4. `Write`: responsável por permitir que um comando seja executado. Com esse serviço pode-se alterar o valor de determinado atributo de forma a efetuar o comando.

5. `Get`: utilizado para se ter um mapa dos objetos que existem dentro do dispositivo, processo chamado de *self-description*. Para suportar este processo, vários serviços get

são utilizados, como GetXXDirectory e GetXXDefinition. A Figura 3.13 exemplifica o processo de *self-description*.

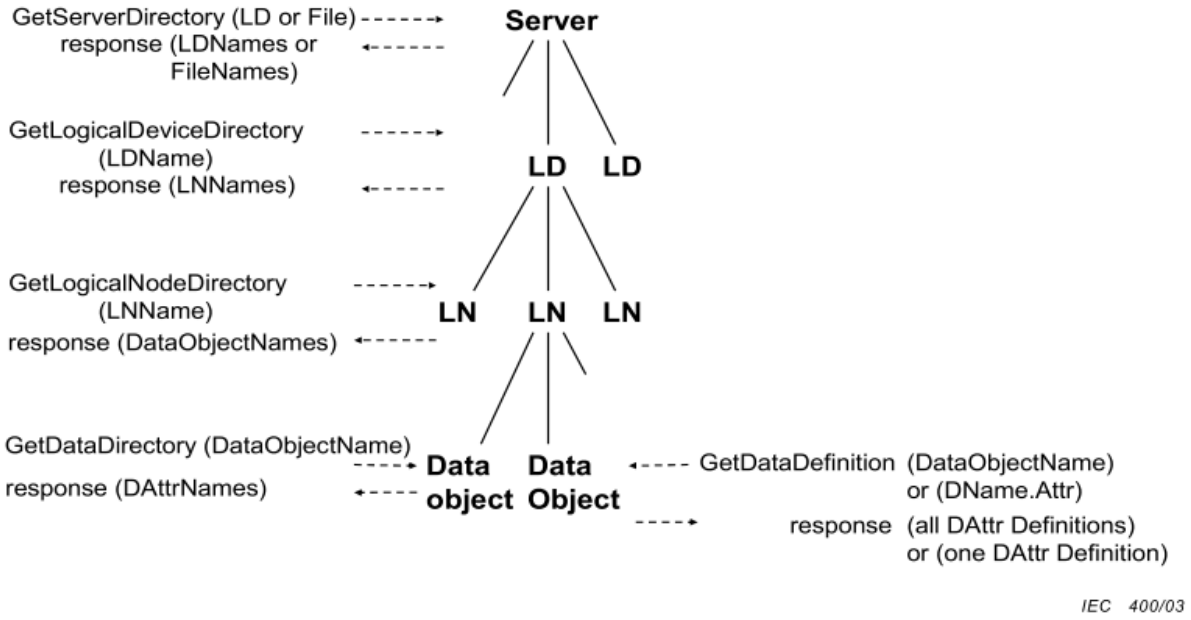


Figura 3.13: Serviços `Get` e o processo *self-description* [81].

6. `Information Report`: Utilizado para enviar um relatório. O envio ocorre por exemplo quando tem-se a mudança de um valor de uma variável, ou a mudança da qualidade desta.

7. `Conclude`: utilizado para encerrar a conexão.

Após a conexão ser estabelecida, cada nó pode assumir a condição de servidor ou cliente, independente de qual iniciou a conexão [2]. A ISO 9506 permite que o sistema real possa adotar a função de cliente ou servidor ou ambos durante o tempo de vida da associação [3]. Apesar disto, nas implementações atuais geralmente o SCADA permanece como cliente durante todo o tempo, e os IEDs como servidores.

Ressalta-se que a comunicação com as estações de carga de veículos elétricos (CS) [88] também é feita com mensagens MMS. Dessa forma, o monitoramento da carga de uma bateria, por exemplo, pode ser feito com um serviço *Read* ou com um *Information Report* de acordo com a implementação proposta.

3.4.3.2 GOOSE

A GOOSE é uma mensagem na qual os valores de uma ou mais variáveis de um dispositivo são agrupados em um datagrama e transmitidos dentro de um período curto de tempo. As mensagens GOOSE são trocadas entre IEDs para envio de alarmes críticos, contendo

informações que permitem ao IED receptor tomar conhecimento da ocorrência de um novo evento, sabendo qual foi e quando ocorreu este evento para tomar uma ação apropriada. Essas mensagens são direcionadas às aplicações de proteção no sistema elétrico de potência. São orientadas a eventos e, consequentemente, tem o seu disparo efetuado de forma assíncrona, sendo transmitidas no modelo publicador assinante como foi ilustrado na Figura 3.11(b). Neste tipo de comunicação, os IEDs trocam informações entre si utilizando MAC *multicast* [86]. Dessa forma, o publicador envia as mensagens para rede e apenas os assinantes, que formam um grupo *multicast* específico, abrem o *frame* e utilizam as informações ali contidas. Essa comunicação, ilustrada na Figura 3.14, é intitulada comunicação horizontal.

Um exemplo típico dessa comunicação é a função de falha de disjuntor. Suponha uma função de sobrecorrente onde um IED esteja parametrizado para abrir o seu disjuntor e eliminar uma falta caso o valor de corrente medido seja igual ou superior ao limiar ajustado**. Caso o IED verifique que não foi possível abrir seu disjuntor enviará uma mensagem GOOSE com essa indicação para o IED de destino que abrirá o seu disjuntor para eliminar a falta. Apesar da mensagem GOOSE ser publicada para todos os IEDs da rede, apenas aquele(s) a que se destina a mensagem, o(s) assinante(s) abre(m) o *frame* e executa(m) o *trip*.

Para que se consiga manter o atraso na rede dentro dos limiares de tempo descritos na Tabela 3.2, as mensagens GOOSE são transmitidas diretamente sobre Ethernet [86]. Um quadro Ethernet tem a estrutura mostrada na Figura 3.15, onde o campo `ethertype` indica o tipo de protocolo no quadro ethernet. Para GOOSE o valor é $88B8$ em hexadecimal.

O envio de mensagens em camada de enlace resolve o problema do atraso pertinente às mensagens do tipo cliente-servidor de camada de rede, entretanto remove a confiabilidade que seria garantida por meio de estabelecimento de conexões e confirmações de recepção das mensagens. Para contornar a falta da confirmação de entrega do quadro e aumentar a confiabilidade nas mensagens GOOSE, a norma define um mecanismo baseado em temporização para reduzir o impacto das perdas de quadros. Desta maneira, uma mesma mensagem GOOSE é enviada diversas vezes, aumentando progressivamente o intervalo entre as retransmissões, até que um novo evento ocorra, reiniciando o processo, ou se alcance um limite máximo de retransmissões. Esse procedimento é definido na parte 8-1 da norma [86] e exemplificado na Figura 3.16, onde:

- $T0$ - retransmissão em condições estáveis (tempo máximo, $Tmax$)
- $(T0)$ - retransmissão em condições estáveis sendo interrompida por um evento
- $T1$ - tempos de retransmissão mais curtos após um evento

**Por simplicidade o tempo de operação para trip está omitido.

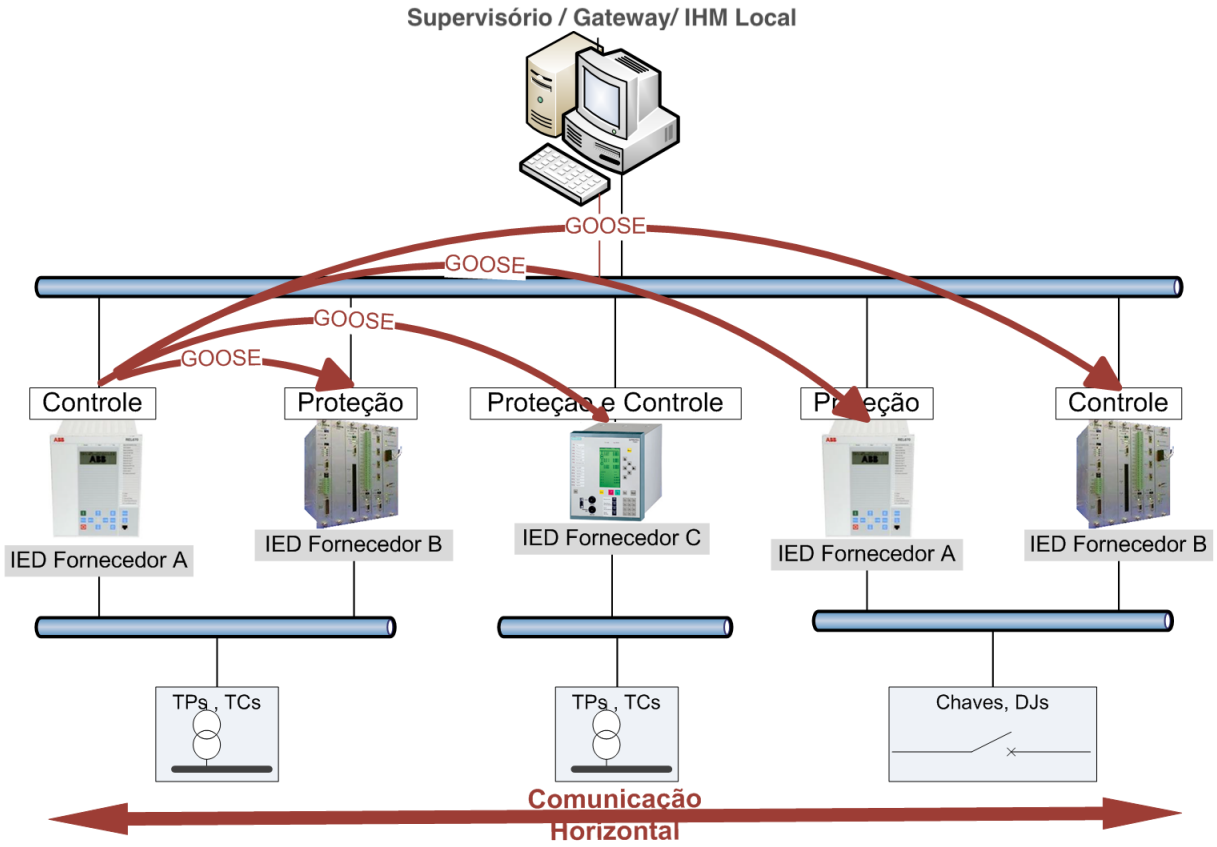


Figura 3.14: Comunicação dentro de uma subestação via mensagens GOOSE, com um IED notificando aos demais sobre algum evento específico.

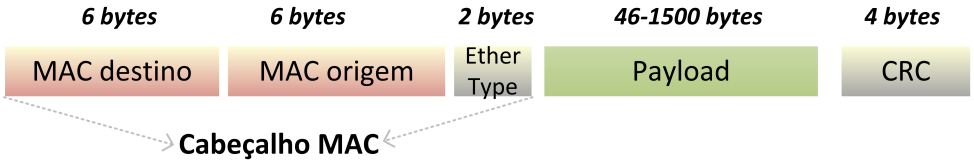


Figura 3.15: Estrutura do quadro Ethernet (64 – 1518 bytes)

- $T2, T3$ - incremento de tempo de retransmissão até alcançar $Tmax$ e retornar a uma condição estável.

Observa-se, na Figura 3.16, que os intervalos de retransmissão após a ocorrência de um evento são aumentados gradativamente até alcançar o tempo máximo T0 ($Tmax$), que representa a retransmissão já em condições estáveis do sistema. Assim, uma confiabilidade adicional é conseguida através da retransmissão dos mesmos dados, com aumento gradual de um campo da GOOSE chamado $SqNum$, que é um número de sequência, e do tempo de retransmissão. A retransmissão pode ser baseada em uma progressão geométrica, ou numa equação por exemplo. A escolha do método e da razão da progressão geométrica fica a cargo dos fornecedores dos equipamentos.

Cada mensagem carrega um parâmetro *timeAllowedToLive* que informa ao dispositivo

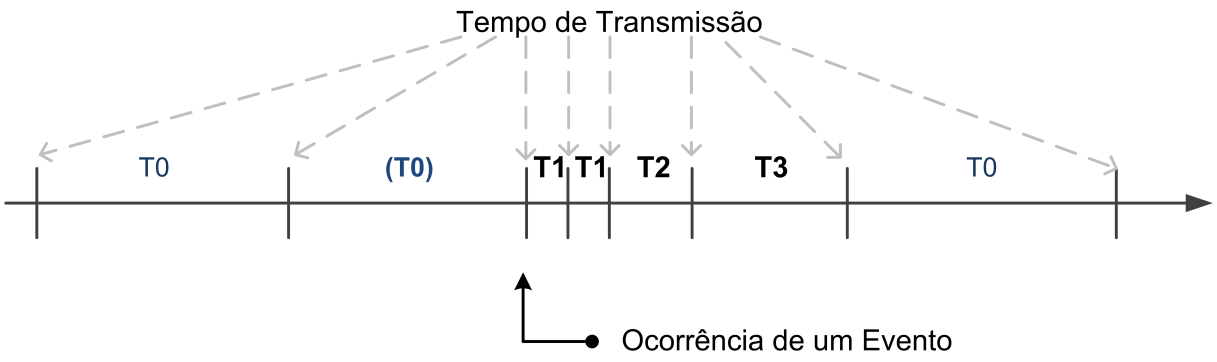


Figura 3.16: Tempos de Transmissão para eventos. Mensagens GOOSE [86]

receptor o tempo máximo de espera para a retransmissão seguinte. Dessa forma, se uma nova mensagem não for recebida dentro desse intervalo de tempo (duas vezes o tempo de intervalo entre uma mensagem e outra), o receptor assumirá que houve um problema na comunicação [86].

Com relação à recomendação da norma para estrutura desse endereço, seus anexos informativos B da parte 8-1 [86] descrevem a estrutura do endereço *multicast* da seguinte forma:

- Os três primeiros octetos são atribuídos pelo IEEE com sendo 01-0C-CD.
- O quarto octeto deve ser 01 para GOOSE.
- O valor 00-00-00-00-00-00 deve ser usado para indicar que o endereço *multicast* não foi configurado.
- Os dois últimos octetos devem ser usados como endereços individuais atribuídos pelo intervalo definido na Tabela 3.3.

Tabela 3.3: Faixa de endereços *multicast* recomendados [86, 87].

Serviço	**Endereço de Início** (hexadecimal)	**Endereço Final** (hexadecimal)
GOOSE	01-0C-CD-01-00-00	01-0C-CD-01-01-FF

Além do esquema de retransmissão para aumentar a confiabilidade na comunicação, a norma define, também, a marcação de prioridade, feita com base no IEEE 802.1Q [25], para segmentar o tráfego crítico e de alta prioridade do tráfego de baixa prioridade [86, 87], visando um aumento no desempenho e na segurança do sistema.

O padrão 802.1Q especifica uma *tag* que é acrescida a um quadro *Media Access Control* (MAC) Ethernet, permitindo o uso de *Virtual Local Area Networks* (VLANs) com

diferentes prioridades nas mensagens. Dessa forma, torna-se possível a criação de redes virtuais entre os IEDs que se encontram conectados a uma mesma rede física. Para marcar o quadro com as *tags* do IEEE 802.1Q/802.1p, os campos ilustrados na Figura 3.17 devem ser adicionados:

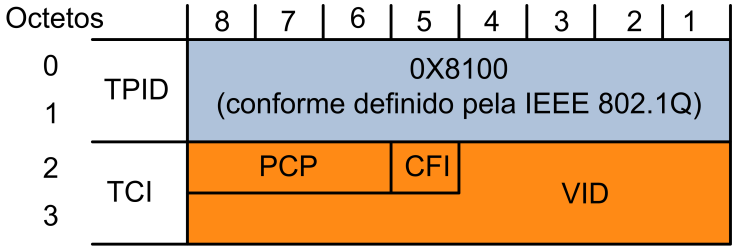


Figura 3.17: Estrutura da *tag* [86, 87].

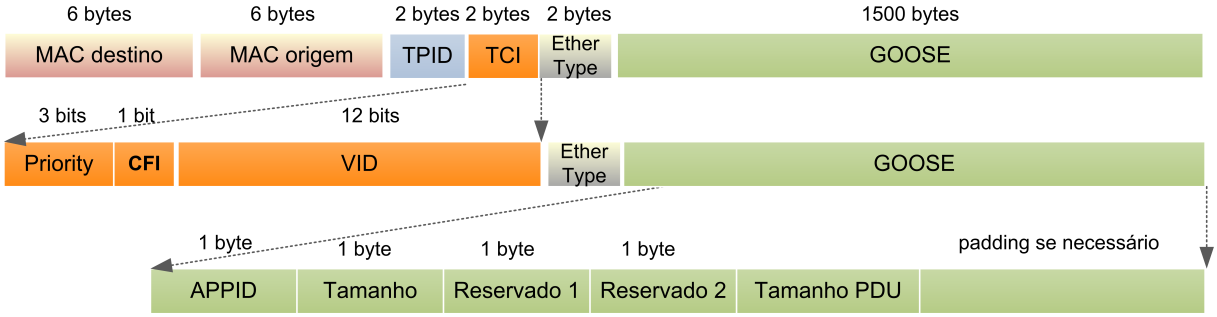


Figura 3.18: Estrutura do Quadro Ethernet

- *Tag Protocol Identifier* (TPID): campo com 16 bits. Valor definido como $0x8100$, o que indica que o quadro contém *tags* IEEE 802.1Q/802.1p.
- *Tag Control Information* (TCI): campo com 16 bits. Contém os seguintes campos:
  - *Priority Code Point* (PCP): campo com 3 bits. É o código de prioridade IEEE 802.1Q que define oito níveis de prioridade (2^3), sendo o nível zero como mais baixo e sete como mais alto. Pode ser usado para dar prioridade a diferentes classes de tráfego, como GOOSE e SV. Os valores *default* estão descritos na Tabela 3.5, no caso, o valor quatro para ambas as mensagens.
  - *Canonical Format Indicator* (CFI): campo com 1 bit. Se o valor for zero, o endereço MAC está no formato canônico. Para essa norma e para *switches* Ethernet, o bit deve ser ajustado como zero[††].
  - *VLAN Identifier* (VID): campo com 12 bits, permitindo até 4094 VLANs. Especifica a qual VLAN aquele quadro pertence e seu uso é opcional. Um valor 0 indica que o quadro não pertence a qualquer VLAN.

[††]Se definido o valor igual a um, seguirá o campo ethertype conforme ISO / IEC 8802-3. Essa forma é usada para ser compatível com Redes Token Ring.

Esses campos são acrescidos entre o campo de endereço MAC de origem e o campo ethertype, conforme ilustrado na Figura 3.18, usando um quadro GOOSE como exemplo.

Ressalta-se que o campo VLAN ID igual a um está reservado para fins de gerenciamento no *switch* Ethernet e, portanto, não deve ser usado para GOOSE ou SV [86, 87]. Além disso, o tráfego marcado com VLAN ID igual a zero fica sem tag e qualquer prioridade associada a esse quadro também é perdida.

A norma define que todas as implementações que receberem GOOSE ou SV têm que ser capazes de entender qualquer VID, assim como as prioridades. Desta forma, devem ser capazes de processar mensagens que contenham, e que não contenham, informações IEEE 802.1. Nesse último caso, processa-se o campo ethertype [86].

3.4.3.3 Sampled Values

Em subestações convencionais, os cabos que saem dos transformadores de corrente e transformadores de potencial são ligados às entradas de corrente e tensão dos relés de proteção, medidores e controladores de vão. Os sinais analógicos dessas entradas são processados por conversores A/D (Analógico/Digital) dentro dos IEDs para utilização das funções de proteção e controle [132].

As mensagens SV, definidas na parte 9-2 da norma IEC 61850 [87], têm por objetivo possibilitar o envio das amostras digitalizadas de tensão e corrente sobre Ethernet, também com restrição rígida de tempo. Nesse contexto, existe a separação física entre os sinais analógicos e o processamento das funções de proteção e controle. Os sinais são digitalizados em transformadores eletrônicos e enviados aos IEDs de proteção e controle através em uma rede de comunicação Ethernet [132].

Duas combinações são definidas para suportar a transmissão dos valores amostrados, tanto cliente/servidor (baseados em MMS), quanto SV (baseados na camada de enlace). Este perfil de comunicação cliente/servidor deve ser utilizado somente em adição ao perfil de comunicação SV se for necessário um acesso via cliente remoto [87]. No entanto, na prática, apenas o modelo da camada de enlace tem sido utilizado. Para a mensagem SV, a comunicação pode ser feita com *multicast* ou *unicast*, dependendo da aplicação. A comunicação *multicast* é ilustrada na Figura 3.19.

Além de padronizar os métodos de comunicação dos valores de tensão e corrente, a SV especifica as taxas de amostragem com diferenças para aplicações de proteção e medição. Cada *frame* Ethernet SV contém 4 amostras de tensão (V) e 4 de corrente (I). Para proteção, é necessário que cada amostra chegue rapidamente ao destino, portanto são realizadas 80 amostras por ciclo (16,6ms) e enviadas 80 mensagens por ciclo, ou seja, a cada grupo de amostras de tensão e corrente envia-se uma mensagem na rede. Para medição, ou registro de oscilografias, precisa-se de uma resolução maior da forma de onda, portanto são realizadas 256 amostras por ciclo, porém as amostras são agrupadas em 8

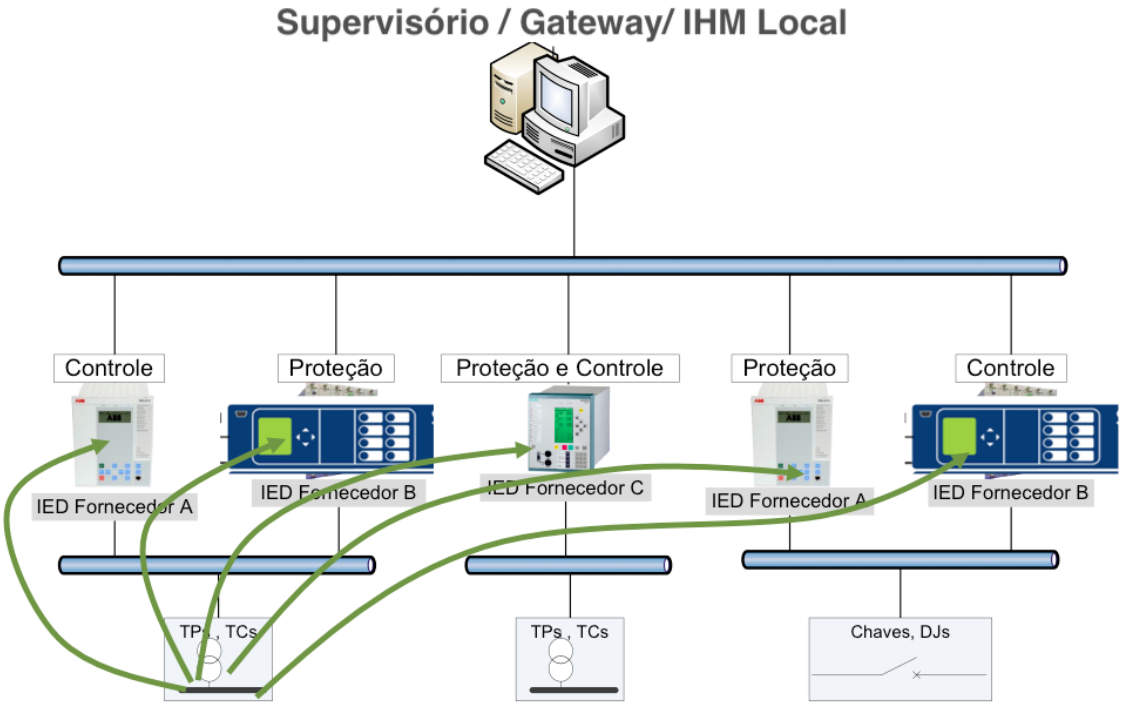


Figura 3.19: Comunicação dentro de uma subestação via mensagens SV, com valores de corrente e tensão sendo amostrados e enviados para rede.

conjuntos e enviadas a uma taxa de 32 mensagens por ciclo pois o tempo de transmissão não é tão importante [36].

Tabela 3.4: Faixa de endereços *multicast* recomendados [86, 87].

Serviço	**Endereço de Início** (hexadecimal)	**Endereço Final** (hexadecimal)
GOOSE	01-0C-CD-01-00-00	01-0C-CD-01-01-FF
Multicast Sampled Values	01-0C-CD-04-00-00	01-0C-CD-04-01-FF

Com relação à recomendação da norma para estrutura desse endereço, seus anexos informativos B da parte 9-2 [87] descrevem a estrutura do endereço *multicast* exatamente da mesma forma que a GOOSE com a diferença que o quarto octeto deve ser 04 para *Sample Values*, conforme Tabela 3.4.

O quadro Ethernet tem a mesma estrutura GOOSE, mostrada na Figura 3.15, com o valor $88BA$ em hexadecimal para o campo `ethertype`. Os campos, `APPID`, `Tamanho`, `Reservado` 1 e 2 também seguem a mesma ideia descrita na Figura 3.18. Os valores, tanto para GOOSE quanto para SV, são resumidos na Tabela 3.5.

Tabela 3.5: Valores *default* para Ethertype, APPID, VLAN IDs, e Prioridades [86].

Uso	**Valor Ethertype** (hexadecimal)	**APPID**	**Prioridade** *Default*	**VID** *Default*
IEC 61850-8-1 GOOSE	88-B8	00	4	0
IEC 61850-9-2 SV	88-BA	01	4	0
IEC 61850-8-1 GOOSE 1A	88-B8	10	4	0

3.5 Considerações sobre o Estado da Arte em Redes Elétricas Inteligentes

Para a modernização do sistema de energia elétrica, torna-se necessária a investigação das tecnologias de comunicação e seu impacto nos sistemas de energia [68, 45]. Como resultado, os sistemas de comunicação tornam-se uma parte necessária das soluções propostas para as aplicações críticas das redes elétricas inteligentes [137]. Além disso, a modernização e a ampla aceitação de DERs dependem da implementação de esquemas de proteção e controle similares aos usados em redes de alta tensão [169]. Como detalhado por Ali et al. [31], a automação do gerenciamento de energia em tempo real é necessária para melhorar a qualidade de energia, mas é uma questão desafiadora, pois requer uma arquitetura de comunicação robusta e rápida. Ali et. al [31] propuseram uma arquitetura de comunicação baseada na norma IEC 61850 [177] como solução, assim como outros autores [164, 180, 131], que, da mesma forma, propõem soluções que requerem uma comunicação rápida para sistemas de proteção e controle. Esses trabalhos têm soluções muito inovadoras e motivadoras que avançaram o estado da arte para as redes elétricas. Contudo, os autores não lidam com desafios de comunicação e apenas consideram que haverá uma rede de comunicação robusta e livre de falhas para as suas propostas. Um exemplo é que estes autores ressaltam a vantagem do uso norma IEC 61850, contudo não abordam o grande desafio de comunicação existente nas redes que utilizam os protocolos GOOSE e SV da norma IEC 61850, que é a inundação da rede. Esses protocolos são padronizados em camada de enlace, restringindo o tráfego das mensagens em rede local, com endereço de destino MAC *multicast*, que na prática são transmitidas como se fossem mensagens *broadcast*, causando uma inundação na rede. Devido ao comportamento típico de *switches*, as mensagens com destino MAC *multicast* são enviadas por todas as portas do *switch*. Isso ocorre pois o *switch* não reconhece esse endereço e, como recurso para que a informação chegue no destino, ele envia a mensagem por todas as portas. Esse comportamento traz uma sobrecarga tanto para a rede quanto para os dispositivos finais que recebem mensagens mesmo não estando no grupo *multicast* de destino. Ressalta-se que esse desafio já ocorre em redes locais de subestações. Diversos trabalhos em subestações digitalizadas concentram esforços em resolver este problema [77, 173, 136] além de tentar reduzir o volume de dados recebidos pelos dispositivos [186]. Quando relacionado às

microgrids e à rede de distribuição, esse desafio aumenta potencialmente. Isso ocorre porque o número de dispositivos conectados à rede de comunicação e enviando mensagens por inundação é muito maior. Além de sobrecarregar os dispositivos que recebem as mensagens, as filas nos *switches*sobrecarregados aumentam bastante o que pode gerar grandes atrasos e até descarte de mensagens, o que impediria o correto funcionamento do sistema de proteção.

A importância da comunicação para as novas propostas é tamanha que vários esforços recentes, como os apresentados em [157, 143, 115, 116, 185, 74], têm focado na inclusão de módulos comunicação em simuladores já conhecidos na área de Sistemas de Potência. Com essa inclusão, novas propostas podem ser analisadas e a dependência dos sistemas de comunicação pode ser avaliada. Alguns autores [166, 76, 137] já mostram que o emprego de mecanismos baseados em uma comunicação robusta irá aumentar o desempenho de todo o sistema elétrico e seus componentes. Para isso, as mensagens de proteção precisam ser trocadas com atrasos máximos da ordem de milissegundos [80], o que demonstra a existência de um demanda rígida de qualidade de serviço para a proteção da rede elétrica inteligente. Assim, o que se observa é que os sistemas de proteção e controle modernos passam a depender diretamente dos sistemas de comunicação[‡‡].

Além do desempenho, a resiliência da rede é fundamental para garantir que a comunicação entre os dispositivos esteja sempre disponível. A rede precisa entregar a mensagem de proteção dentro do tempo esperado mesmo em condições de falha na rede de comunicação. Isso implica em métodos para recuperação de falhas eficientes e escaláveis. A não entrega de uma mensagem de proteção da rede elétrica pode resultar em instabilidade do sistema ou ainda em propagação de uma falha elétrica.

Apesar da importância, os protocolos usados atualmente para garantir a recuperação da rede de comunicação em caso de falha geralmente não atendem aos requisitos de atraso da rede elétrica [169, 179, 152, 120]. Além disso, os métodos que atendem aos requisitos de atraso fazem isso ao custo de inundar a rede com pacotes redundantes ou possuem premissas para implantação tão rígidas que tornam o método não escalável [152]. Dessa forma, um primeiro desafio para a implementação das redes elétricas inteligentes consiste no provimento de uma rede resiliente, com uma recuperação de falhas eficiente e que não interfira na latência de comunicação exigida (milissegundos) para aplicações críticas e que seja, ao mesmo tempo, escalável.

Deve-se enfatizar que a questão da resiliência da comunicação é mais relevante quando se trata de ações em tempo real, geralmente relacionadas ao comportamento transiente dos circuitos [137]. Exemplos de aplicações críticas, além da proteção do sistema, incluem o controle de emergência em sistemas elétricos de potência [5], a regulação de tensão [59],

[‡‡]Os sistemas de proteção (principal ou *backup*) que não utilizam comunicação, por exemplo os baseados em atuações temporizadas, não são objeto de estudo desta tese já que não permitem que os benefícios trazidos pela inserção de comunicação sejam alcançados.

a restauração de energia [160], a localização de falhas inteligente [92] e a gestão inteligente de energia [142]. Segundo [137], todas as aplicações que propõem o uso de sistemas multiagentes como solução, também se encaixam no grupo de aplicações críticas.

A área que mais demanda qualidade na comunicação das redes elétricas inteligentes é relacionada à proteção do sistema elétrico. Com a inserção da geração distribuída e o advento das *microgrids*, vários trabalhos [33, 89, 129, 99, 72, 182, 188, 167, 12, 41, 66, 178] têm mostrado novos mecanismos de proteção e com eles necessidades rígidas de comunicação. De forma geral, os métodos utilizam medições do sistema de potência que precisam estar disponíveis nos elementos de proteção em tempo hábil para atuação. Isto ilustra a grande necessidade de garantias de qualidade de serviço em *microgrids* e infraestruturas que contenham GDs.

A medição e coleta de informações em GDs, além da rede de comunicação entre essas GDs e os dispositivos de proteção, são um dos desafios desse cenário que precisam ser explorados. Driesen et al. [52] discutem questões de proteção relativas a essa inserção. Os autores analisam o impacto da geração local nos sistemas de seletividade da proteção. O cenário da proposta contemplava um sistema com conexão de geradores em paralelo com o sistema de distribuição. Neste sentido, Nikkhajoei e Lasseter [139] mostram que a filosofia para a proteção de *microgrids* deve seguir as mesmas estratégias de proteção de subestações. Estes autores ressaltam que é importante que as funções de proteção sejam *plug-and-play*, o que é um ponto importante do trabalho. Sobre os sistemas de proteção nas *microgrids* de baixa voltagem, Laaksonen [100] descreve os princípios e os principais problemas. O autor afirma que com relação ao conceito de proteção para este cenário é essencial a utilização de comunicação de alta velocidade. Os autores abordam a necessidade do uso de um padrão geral, como a norma IEC 61850, para obter uma operação de proteção rápida, seletiva e confiável. O autor obteve bons resultados a partir de simulações com o PSCAD[§§]. Também propondo novos esquemas de proteção, Sortomme et al. [175] propuseram um esquema de proteção da *microgrid* usando relés digitais através de uma rede de comunicação entre os relés e as fontes de GD de propriedade dos clientes. Os autores exploraram novos métodos para faltas de alta impedância com uma estrutura em *loop* para aumentar a confiabilidade do sistema. Salomonsson et al. [165] também propuseram um sistema de proteção para *microgrids* de baixa voltagem. Eles também discutiram diferentes métodos de detecção de falhas e aterramento. Apesar das soluções inovadoras e motivadoras dos artigos, o provimento de uma rede com QoS de acordo com a aplicação é um desafio. Como detalhado no trabalho de Wang et al. [184], a rede de comunicação que vai dar suporte para as redes elétricas inteligentes precisa lidar com diversos requisitos de comunicação. Além disso, os autores ressaltam a necessidade do suporte ao uso de *multicast*, de forma que apenas os dispositivos de destino recebam o tráfego. Com isso, desconsidera-se o tráfego de rede indesejado, o que é útil para os dispositivos eletrônicos inteligentes compartilharem informações relacionadas à proteção

[§§]https://hvdc.ca/pscad/, acesso em junho de 2018

com seus pares [184].

Não somente a proteção em *microgrids* tem sido discutida na literatura, mas também as áreas de controle e monitoramento, dentre outras. Com isso, a investigação das tecnologias de comunicação também cresce pois elas têm ainda mais impacto nos sistemas de energia [68, 45, 184]. A comunicação é fundamental para as estratégias de controle para aplicações críticas de redes elétricas inteligentes [137, 100]. A importância da comunicação para as novas propostas é tamanha que vários esforços recentes, como os apresentados em [157, 143, 115, 116, 185, 74], têm focado na inclusão de módulos comunicação em simuladores já conhecidos na área de sistemas de potência. Com essa inclusão, novas propostas podem ser melhor analisadas e a dependência dos sistemas de comunicação em soluções para o sistema elétrico pode ser avaliada. Esses autores ressaltam a importância do estudo das vulnerabilidades na comunicação utilizada em sistemas de energia [137]. Ao se incorporar um módulo de comunicação dentro de simuladores já utilizados para o SEP, são evitados problemas de sincronização na integração do simulador com outras ferramentas [137] permitindo a realização de análises mais eficientes em soluções que dependam de comunicação entre dispositivos.

Wei e Chen [185] abordam o efeito que o desempenho da rede de comunicação causa no sistema de potência onde são implementadas. Para isso, os autores simulam a rede desejada no OPNET, coletam os resultados encontrados e os incluem na simulação do sistema de potência medindo o desempenho do sistema estudado na presença de uma rede de comunicação. Também com o intuito de investigar o efeito dos meios de comunicação sobre a confiabilidade de um sistema de potência, Naeini et al [157] estudam as vulnerabilidades dos sistemas de controle e comunicação. Os trabalhos [157, 143, 115, 116, 185, 74] ressaltam muito bem a importância dos sistemas de comunicação para o SEP, mas seus esforços são direcionados para a inclusão de módulos de comunicação em simuladores do sistema de potência e nenhuma solução de comunicação é apresentada, já que os autores consideram como premissa que a rede de comunicação atende aos requisitos necessários.

Alguns autores [137, 68, 117] vão além e mostram que a integração tecnológica advinda das redes elétricas inteligentes requer novos mecanismos de controle que possam tirar proveito das possibilidades de sensoriamento e atuação remotos e distribuídos. Com a implementação de *microgrids* e GDs, diversos dispositivos controladores e inteligentes são implementados na infraestrutura. No entanto, caso a capacidade de comunicação deles não seja explorada, o equipamento fica subutilizado e o controle realizado não é feito da forma mais eficiente. O emprego de mecanismos de controle que sejam baseados em uma comunicação mais inteligente irá aumentar o desempenho de todo o sistema elétrico e seus componentes [166, 76]. Com isso, aumenta bastante a relação entre as redes de comunicação, o controle e os componentes do sistema de potência, o que exige que estudos sejam direcionados para a rede de comunicação. Tal relação é, em particular, mais crítica em sistemas transientes, onde o aumento do tráfego de comunicação durante eventos críticos de energia, gerados por processos de controle e monitoramento, podem dificultar o

desempenho da rede de comunicação e, por sua vez, interromper os esquemas de controle que dependem dele. Por exemplo, uma falta em um alimentador irá disparar uma série de mensagens oriundas dos vários dispositivos conectados a ele que observaram o aumento de corrente em diferentes locais (fisicamente relacionados) e enviarão informações para a rede. A inundação de mensagens irá influenciar na rede de comunicação que poderá sofrer com longos atrasos na comunicação, impedindo que possíveis ações de proteção possam ser tomadas a tempo [137]. Por esse motivo, como afirmam Moradi-Pari et al. [137], é muito importante o estudo das estratégias que serão usadas para controle distribuído ou centralizado em redes elétricas inteligentes. Os autores concordam que as tecnologias de comunicação precisam avançar para permitir uma implementação mais eficiente das redes elétricas inteligentes e ressaltam que a comunicação entre seus domínios pode melhorar bastante o desempenho das aplicações de energia. A necessidade do estudo e avaliação de tecnologias de comunicação avançadas para permitir um controle distribuído eficiente das redes elétricas inteligentes é bastante apontado pelos autores. O desempenho da comunicação, ainda segundo os autores, tem um efeito significativo no desempenho dos controladores que gerenciam o sistema elétrico. Apesar da análise motivadora, Moradi-Pari et al. apenas apresentam uma estratégia sob demanda, que descreve como a comunicação entre os sistemas poderia ser configurada para melhorar o desempenho das aplicações, apontam o que precisa ser comunicado e com essas informações constroem um simulador. No entanto, consideram que essa rede de comunicação com qualidade de serviço suficiente já exista e direcionam os esforços para o simulador desenvolvido.

O *framework* proposto nesta tese objetiva permitir que a rede de comunicação possa lidar com esses diferentes requisitos de comunicação de forma dinâmica provisionando a rede, de forma autonômica, de acordo com a qualidade de serviço demandada pela aplicação. Outro ponto importante, é que a característica citada por Lasseter [139] como necessária também é considerada, de forma que as funções sejam *plug-in-play*. Da mesma forma, não só o tráfego *multicast*, como as prioridades definidas em norma são parte dos requisitos do *framework*, como será visto adiante.

Muitas das aplicações de energia para redes elétricas inteligentes têm exigências rigorosas em termos de disponibilidade e atraso na comunicação [177]. A rede de comunicação não pode aumentar o tempo da atuação da proteção, por exemplo [116]. Nesse sentido, algumas iniciativas para definir valores de atraso aceitáveis nessas redes têm sido feitas. A norma IEC 61850-7 [80], de 2009, aborda a padronização da comunicação para os recursos de energia distribuídos usando o mesmo limiar temporal estabelecido para proteção e controle de subestações. Com isso, são recomendados para proteção valores de atraso de 3ms até 100ms de acordo com o tipo de mensagem utilizada. Também nesse sentido, o departamento de Energia dos Estados Unidos, em 2010, analisou os requisitos de comunicação para redes elétricas inteligentes e definiu valores de latência máximos de milissegundos e níveis de confiabilidade para cada aplicação [179]. Isso confirma a necessidade de implementação de uma rede de comunicação resiliente entre os dispositivos que compõem o

sistema, como também aponta o trabalho de Lin et al. [116]. Os autores apresentam um esquema de proteção de distância *backup* baseado em comunicação. Neste esquema, os IEDs proativamente comunicam-se uns com os outros para obter uma melhor visibilidade do sistema e tomar decisões coordenadas de proteção. Os resultados da simulação validam o esquema de proteção utilizado e mostram que o tempo de comunicação necessário para o perfeito funcionamento do esquema de proteção é menor que o limite, definido em 100ms para todas as ações de proteção necessárias, incluindo nesse valor o tempo de comunicação. Apesar dos autores apontarem novamente a importância da comunicação para a modelagem do sistema de energia, e testarem um estudo de caso para avaliar o uso inteligente da rede de comunicação, Lin et al. não apresentam estudos ou propostas para o avanço na comunicação. Levando em consideração esse mesmo cenário, no entanto com um esquema de proteção principal, sem *backup*, caso as mensagens de proteção e controle não sejam entregues ao destino devido a uma falha na rede de comunicação, os equipamentos de proteção não atuam, deixando o sistema desprotegido, o que pode resultar em falhas elétricas de enormes proporções. Nesse sentido, além de uma rede de comunicação com baixa latência, também é altamente recomendado que a rede de comunicação seja resiliente a falhas. Ressalta-se que os trabalhos apontados levam em consideração apenas o atraso na comunicação e não consideram que falhas na rede de comunicação possam ocorrer.

A necessidade de implementação de uma rede resiliente já é um problema bem conhecido em redes locais de subestação, tanto que muitos esforços têm sido feitos atualmente para garantir que falhas na rede de comunicação não afetem o sistema e controle e proteção de subestações [84]. Apesar dos avanços tecnológicos obtidos nessa área, a garantia de resiliência evitando que a comunicação fique fora por um tempo que afete o sistema ainda é um desafio. O *Rapid Spanning Tree Protocol* (RSTP) [110], amplamente utilizado na camada de enlace, tem tempos de recuperação de até alguns segundos, valor bastante distante dos limiares exigidos para redes elétricas inteligentes [169]. Apesar de existirem versões mais recentes do RSTP que apresentam tempos de recuperação da rede muito melhores, na casa dos milissegundos, estes são geralmente soluções proprietárias ou envolvem uma topologia muito específica e configurações manuais dos dispositivos [155]. Além disso, o RSTP usado em subestações usa um único caminho em caso de falha, já que foi idealizado apenas para uma rede em anel, e, portanto, não funciona para mais do que uma falha simultânea [169].

Outros dois protocolos que foram propostos para uso em redes de comunicação de subestações que apresentam um baixo tempo para recuperação em caso de falha são o *Parallel Redundancy Protocol* (PRP) e o *High-availability Seamless Redundancy* (HSR) [84], ambos da IEC. No PRP, o método consiste no envio duplicado do pacote por duas redes distintas e similares. Com isso, caso uma rede sofra uma falha, o pacote enviado pela outra rede chegará. O HSR funciona de forma similar, porém na topologia em anel. O dispositivo envia o pacote duplicado, um por cada sentido do anel, de forma que em caso de rompimento de um lado do anel, o outro pacote chegará. Dessa forma, considera-se

que o sistema não fica indisponível em caso de falha. No entanto, este tipo de solução não é escalável, sendo insuficiente para a introdução massiva dos recursos de geração distribuída e proteção em redes de distribuição elétrica [169]. A implementação de duas redes semelhantes e independentes entre todos os dispositivos deixa a solução cara, sendo economicamente viável apenas para subestações. Além disso, os IEDs precisam ter os protocolos PRP e HSR implementados, deixando a solução dependente de fabricantes que trabalhem com esses protocolos. IEDs que não tenham os protocolos implementados precisam ser trocados ou necessitam de um dispositivo intitulado RedBox (*Redundancy Box*). O RedBox é instalado entre o IED e a rede com a responsabilidade de duplicar a mensagem no envio e descartar a duplicata na recepção. Essa solução, além de cara, faz com que seja criado um ponto de falha após o IED, o que precisa ser repensado, já que os protocolos foram concebidos justamente para contornar falhas. No caso da falha do RedBox, o IED fica isolado, indo contra a ideia principal dos protocolos. Outro ponto importante é que os IEDs, elementos mais caros que os dispositivos de rede, são sobrecarregados por precisarem duplicar as informações e descartar duplicatas. Isso faz com que o tempo de vida útil destes equipamentos diminua, o que pode não ser interessante para a concessionária. Esse aumento do processamento do equipamento também pode aumentar o tempo para transmissão de mensagens de proteção e controle, interferindo no tempo total para atuação. Essas características implicam muitos problemas no uso das soluções, que tem como única vantagem o tempo de recuperação zero, caso a falha não seja no RedBox e seja em apenas uma das redes.

Tendo em vista a necessidade de resiliência, o alto tempo de recuperação do RSTP e as premissas e problemas para a instalação do PRP e do HSR, alguns autores [169, 155] propõem outras soluções. Selga et al. [169] propõem uma abordagem que estende os princípios do TRILL (*Transparent Interconnect of Lots of Links*), que é uma especificação que permite a implementação de multicaminhos em *data centers* e do SPB (*Shortest Path Bridging*), protocolo especificado no IEEE 802.1aq. Os autores propõem uma solução baseada na junção de ambos os métodos para aplicação em redes elétricas inteligentes. Porém, a solução é baseada no encapsulamento do quadro ethernet tradicional, o que imprime atraso na comunicação. Essa afirmação foi comprovada pelos testes realizados no trabalho, que mostraram que a proposta não pode lidar com os requisitos mais rigorosos definidos para as redes elétricas inteligentes. Como solução, os autores propõem uma solução baseada na combinação do método proposto com os princípios do PRP. No entanto, este recurso resulta nos mesmos problemas descritos para o PRP, inviabilizando o uso da proposta para o cenário em questão.

Realizando testes em redes reais com uma versão melhorada do RSTP, porém proprietária, Pustylnik et al. [155] fornecem uma análise detalhada do desempenho do RSTP juntamente com equações simples para estimar o tempo de recuperação da rede em caso de falhas. Os autores realizaram testes em um ambiente real e atestaram que o RSTP, conforme definido pelo IEEE 802.1D-2004, tem melhor desempenho do que sua versão

mais antiga com tempo de recuperação após uma falha de 89,71ms para 25 *switches*. Infelizmente, apesar de ter melhorado o tempo em comparação com sua versão mais antiga, o tempo encontrado ainda não alcança o tempo de recuperação exigido por esse cenário. Para que os autores alcançassem o tempo de 20 ms usaram um tipo de RSTP muito específico e proprietário (Siemens) [155]. Além disso, o limiar temporal exigido para algumas aplicações chega a 3ms, já que este é o valor mais rígido exigido nesse cenário (mensagem para comando de trip com GOOSE - IEC 61850), o que deixa 20ms fora do limiar necessário.

O *framework* proposto nesta tese objetiva manter a comunicação dentro da latência exigida mesmo em caso de falha na rede de comunicação. Além disso, a solução não é dependente da topologia, é capaz de recuperar a partir de um número variável de falhas de rede desde que haja pelo menos um caminho de comunicação físico disponível entre origem e destino, é transparente para o IED e não sobrecarrega os elementos finais nem a rede de comunicação.

Capítulo 4

Redes Definidas por Software

As redes de computadores usadas atualmente são complexas [60, 97]. São diversos tipos de equipamentos com funções diferentes para alcançar a qualidade de rede demandada. *Switches* e roteadores têm um *software* de controle distribuído e complexo, além de normalmente fechado e proprietário [60]. Esse *software* de controle distribuído, existente em cada dispositivo tradicional, constitui a parte responsável pela "inteligência" do dispositivo, pois é ele que decide como lidar com o tráfego na rede.

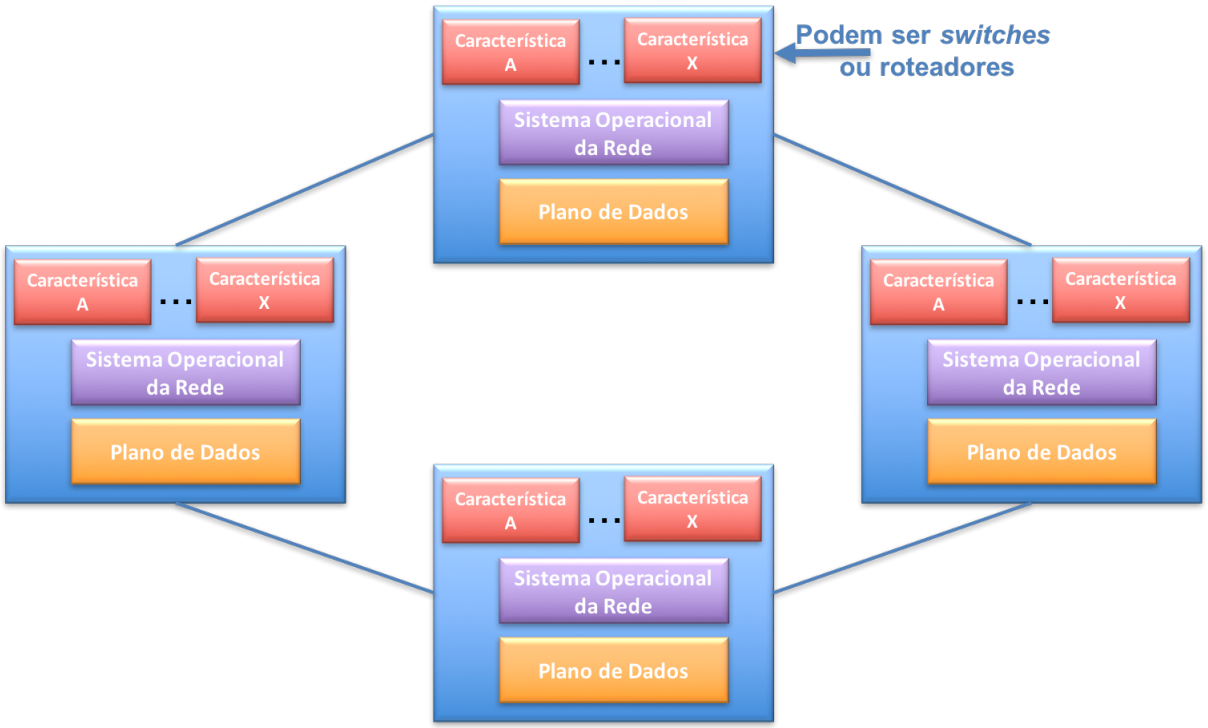


Figura 4.1: Arquitetura tradicional de redes onde o plano de controle reside em cada equipamento, exigindo a constante troca de informações de controle entre todos os dispositivos. Adaptada de [168].

De forma geral, o plano de controle define a regra, ou seja, como um pacote deve ser

tratado e por qual interface ele deverá ser encaminhado. O plano de encaminhamento é o responsável por lidar com os pacotes de acordo com essa regra. Essa arquitetura tradicional é ilustrada na Figura 4.1 onde o plano de controle e o plano de encaminhamento estão dentro do mesmo dispositivo. Os códigos dos protocolos, responsáveis pela realização de cálculos, como as rotas em protocolos de roteamento, são função desse plano de controle. Contudo, sua natureza distribuída exige que diversas informações de controle sejam trocadas pelos dispositivos de rede para que cada dispositivo se mantenha atualizado. As decisões são passadas do plano de controle para o plano de encaminhamento, através de uma API proprietária.

Essa união física entre o plano de encaminhamento e o plano de controle torna o gerenciamento da rede ainda mais difícil [97]. Os operadores da rede de comunicação normalmente configuram os dispositivos e provisionam os enlaces da rede de forma individual, usando interfaces de configuração que variam de fornecedor para fornecedor e até mesmo de modelo para modelo de um mesmo fornecedor. Embora algumas ferramentas de gerenciamento de rede ofereçam um ponto de vista central para configuração, estes sistemas ainda operam com mecanismos, protocolos e interfaces de configuração próprios. Este modo de operação diminui a inovação, aumenta a complexidade, o investimento e os custos operacionais da gerência de uma rede [60].

Ademais, o plano de controle implementa protocolos de rede que precisam passar por muitos anos de padronização e testes de interoperabilidade [60]. Isso se deve a infraestrutura de rede atual, que muitos pesquisadores consideram "ossificada", por não poder ser modificada [133]. Isso ocorre pois já existe uma base extensa e já instalada de equipamentos e protocolos em produção. Experimentar novas tecnologias em redes em produção não é uma prática comum, o que constitui muitos obstáculos para a implantação de inovações. Mckeown et al. [133] afirmam que na rede de comunicação tradicional não há praticamente nenhuma forma de se testar novos protocolos de rede, por exemplo, os novos protocolos de roteamento ou, alternativas ao IP, em ambientes suficientemente realistas para ganhar a confiança necessária para sua implantação generalizada. O resultado é que a maioria das novas ideias da comunidade de pesquisa não é devidamente testada e, por essa razão, acaba não sendo implementada nas redes em produção.

Além disso, cada vez mais, são demandados novos requisitos de rede, como o isolamento entre redes virtuais, um maior provimento de qualidade de serviço, uma maior velocidade de comutação em caso de falha, a mobilidade, etc. A comunidade de redes vem atendendo bem a essas crescentes demandas, porém, com soluções individuais, que não lidam com a arquitetura como um todo [20]. Portanto, encontram-se soluções bem definidas para casos específicos e isolados, porém alcançar a integração ainda é um desafio nas redes atuais.

Redes definidas por *software* (do inglês, *Software Defined Network* (SDN)) objetivam flexibilizar o provimento de novas funcionalidades em redes de forma estruturada, através da criação de um plano de controle via *software* que seja fisicamente separado do plano de

encaminhamento de pacotes. Com isso, o plano de encaminhamento continua residente nos equipamentos de rede, sejam eles *switches*, pontos de acesso ou roteadores, independente de fornecedor, porém com uma interface uniforme. O plano de controle fica externo ao equipamento de rede, podendo ser implementado de forma centralizada ou distribuída. Essa arquitetura, ilustrada na Figura 4.2, é considerada um modelo programável, pois permite que as características requeridas da rede sejam implementadas a partir de códigos, intitulados aplicações, que fazem parte do plano de controle.

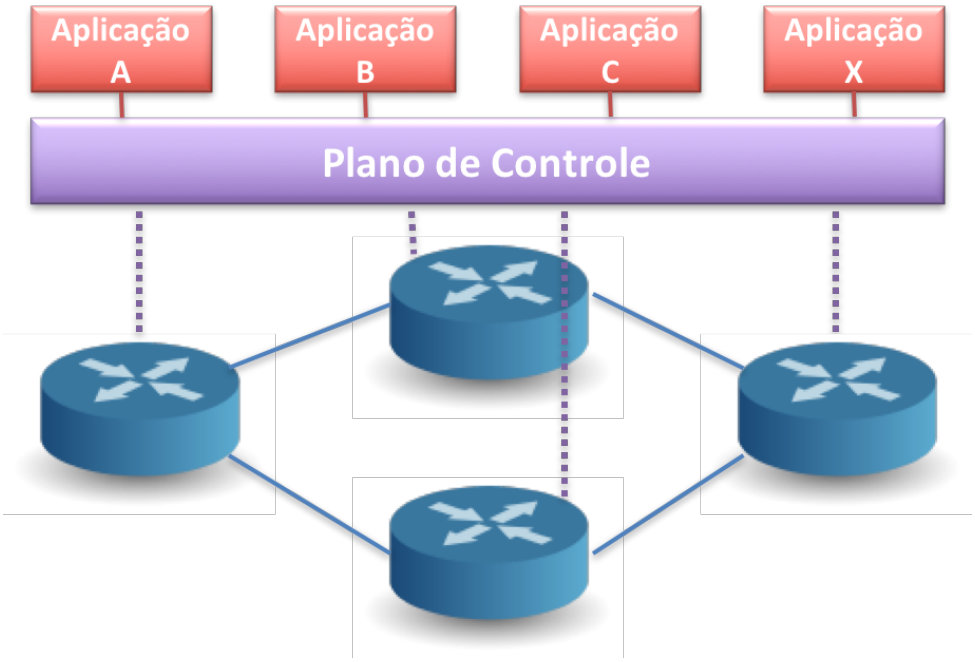


Figura 4.2: Arquitetura SDN com visão global da rede e modelo programável. Adaptada de [168].

Com o modelo programável, ilustrado na Figura 4.2, a implementação de aplicações de rede se torna mais fácil, pois é feita com base em uma visão centralizada e global da rede [61]. De fato, nesse novo modelo, o plano de controle pode ser implementado sobre servidores com uma interface de *hardware* aberta e amplamente utilizada no desenvolvimento de aplicações. Desse modo, mantém-se o alto desempenho no encaminhamento de pacotes em *hardware* aliado à flexibilidade de se inserir, remover e especializar aplicações em *software* [163].

Nas aplicações mais comuns de SDN, o plano de controle é abrigado em uma máquina física ou virtual, intitulada controlador SDN, de forma que se tem um novo elemento na rede, responsável pela tomada de decisão e confecção das tabelas de encaminhamento. Dentro desse elemento, reside o sistema operacional de rede, que é o *software* que oferece uma interface de programação simples e uma visão topológica da rede, o que simplifica as tarefas de engenheiros de rede [61]. A plataforma OpenFlow [133], proposta pela Universidade de Stanford, é o principal exemplo da aplicação do conceito de SDNs. O

funcionamento e principais características do OpenFlow são descritos na Seção 4.1.

Algumas das maiores empresas, incluindo Deutsche Telekom, Facebook, Google, Microsoft, Verizon, e Yahoo!, criaram a *Open Networking Foundation* (ONF) [21] para padronizar e promover as SDNs. A ONF é uma fundação sem fins lucrativos, que possui quase 100 membros, entre os quais estão: Alcatel-Lucent, Cisco, Dell, Extreme, HP, Huawei, IBM, Juniper, NEC, Nokia Siemens. Vários fornecedores já vendem produtos SDN, tais como *switches* e controladores [22, 21]. Em 2018, a empresa SEL lançou o que os mesmos intitulam o primeiro *switch* SDN de mercado projetado para ambientes agressivos, frequentemente encontrados no setor de energia*. O controlador comercializado pela empresa fornece uma engenharia de tráfego centralizada e permite que os fluxos sejam configurados de forma manual pelos usuários.

4.1 O OpenFlow

A plataforma OpenFlow [133], proposta pela Universidade de Stanford, é o principal exemplo da aplicação do conceito de SDNs. No OpenFlow, o plano de controle funciona em um servidor, capaz de se comunicar com todos os *switches* OpenFlow da rede, obtendo informações de estado e enviando comandos de configuração e encaminhamento. Com isso, a demanda pela validação de novas propostas de arquiteturas e protocolos de rede sobre equipamentos comerciais em uma rede em produção, incluindo as abordagens *clean slate*†, pode ser atendida. As atividades de gerência e configuração da rede são feitas em cima da abstração da rede. Com isso, ao invés de se configurar cada dispositivo separadamente, os administradores de rede precisam somente manipular o seu mapa lógico. A arquitetura também suporta uma série de APIs, que permitem a implementação de serviços de rede comuns como roteamento, *multicast*, políticas de acesso, engenharia de tráfego, QoS, entre outros.

O OpenFlow tem como objetivo ser flexível para atender aos seguintes requisitos [133]:

- Possibilidade de uso em implementação de baixo custo e de alto desempenho;
- Capacidade de suportar uma ampla gama de pesquisas científicas;
- Garantia de isolamento entre o tráfego experimental e o tráfego de produção;
- Consistência com a necessidade dos fabricantes não exporem o projeto de suas plataformas.

*Detalhes sobre o *switch* e o controlador são encontrados em https://selinc.com/pt/products/2740S/ e https://selinc.com/products/5056/, respectivamente.

†A abordagem *Clean slate* visa substituir toda a arquitetura atual por uma nova, totalmente reconstruída, tendo como principal objetivo direcionar como será efetuado o desenho da nova Internet [23].

Para isso, utilizam-se as tabelas já existentes nos *switches* atuais[‡]. Para fornecer uma forma aberta e padronizada para a comunicação entre o controlador e o *switch*, foi desenvolvido o protocolo OpenFlow. Ele especifica uma interface padronizada onde os administradores da rede podem determinar as ações de encaminhamento de pacotes, obter estatísticas da rede, entre outros [133]. Portanto, um *switch* OpenFlow precisa apresentar a capacidade de estabelecer um canal seguro com o controlador, permitindo que sejam trocados comandos e pacotes entre esses elementos [133] de forma segura. Para que a rede não sofra ataques de elementos mal intencionados, o canal seguro garante confiabilidade na troca de informações entre o *switch* e o controlador. A interface de acesso recomendada é o protocolo *Secure Socket Layer* (SSL), embora também seja possível fazer a conexão via *Transmission Control Protocol* (TCP) nas implementações atuais [6]. Um *switch* OpenFlow precisa também estar apto a trocar dados, aceitar configurações por meio do protocolo OpenFlow e, ainda, armazenar as configurações recebidas na(s) tabela(s) de fluxos [133]. A Figura 4.3 ilustra um exemplo de *switch* OpenFlow na versão 1.0 [6].

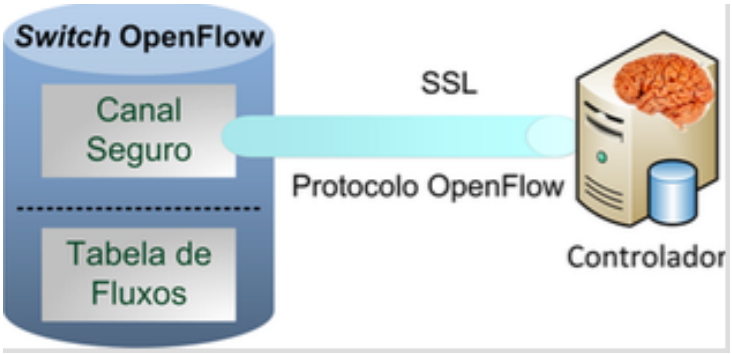


Figura 4.3: *Switch* OpenFlow. A Tabela de fluxos é controlada por um controlador remoto via o canal seguro. Adaptado de [133].

A arquitetura ilustrada na Figura 4.3 passou por melhorias e extensões com as novas versões do OpenFlow. A versão 1.1.0 [9], por exemplo, lançada em 2011, introduziu o conceito tabela de grupos. Além da inserção desta tabela de grupo, foi introduzido o conceito de *pipeline* de tabelas com múltiplas tabelas de fluxo. A Figura 4.4 mostra os principais componentes do *switch* OpenFlow a partir da versão 1.1.0.

Essas alterações permitem uma definição ainda mais completa dos fluxos e do conjunto de ações associadas [9]. Os principais componentes atuais dessa arquitetura, vantagens e funcionamento são detalhados nas seções que seguem.

[‡]A maioria dos *switches* Ethernet e roteadores modernos possuem tabelas de encaminhamento tipicamente construídas a partir de *Ternary Content Addressable Memory*s (TCAMs), que são utilizadas para implementar diferentes funcionalidades, como Qualidade de Serviço (QoS), *Firewalls*, *Network Address Translation* (NAT) e coleta de estatísticas.

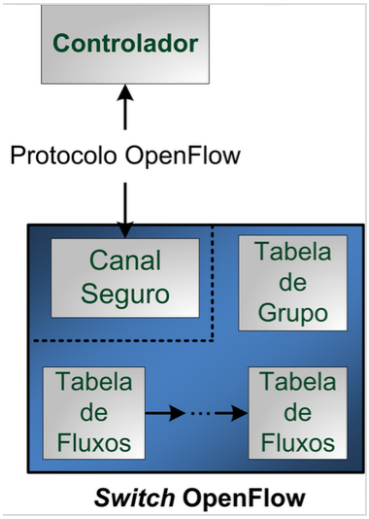


Figura 4.4: Componentes do *switch* OpenFlow versão 1.1.0 [10]

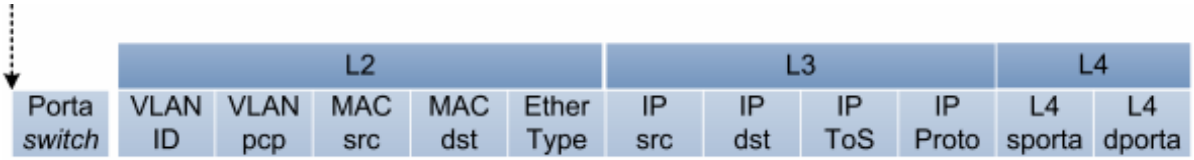
4.1.1 Tabela de Fluxos do OpenFlow 1.3

O principal objetivo de um *switch* é possibilitar a conexão de dispositivos em rede. Para isso, ele precisa encaminhar o pacote que entra para a interface de saída correta, a fim de que o pacote possa chegar ao seu destino [98]. Com isso, a lógica de encaminhamento de pacotes é feita com base em regras contidas em tabelas de encaminhamento. Se o pacote que entra no *switch* corresponde a determinada regra, ele sofre o comportamento associado a ela. Em geral, nas redes tradicionais, há uma tabela que associa uma porta (comportamento) a um endereço de destino (regra). Com isso, se o pacote tiver o endereço de destino descrito na regra, ele é enviado para a porta de saída descrita na tabela.

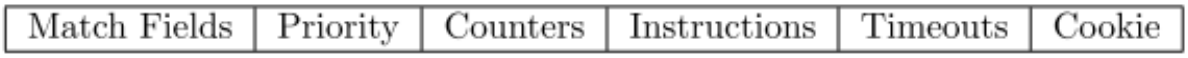
Uma das grandes vantagens da tecnologia SDN baseada em OpenFlow é a capacidade de construção de regras mais elaboradas. Além do uso de endereços de destino, todos os campos do cabeçalho, a porta de entrada e um campo opcional chamado metadados podem ser usados para a construção de uma regra em um *switch* OpenFlow. A versão 1.3 contém 13 campos para correspondência, ilustrados na Figura 4.5(a), que podem ser usados inclusive em conjunto. Desta forma, o fluxo de pacotes pode ser identificado através da combinação de qualquer um desses campos. Um exemplo poderia ser um pacote da VLAN 100, com Ethertype $0X88b8$ e MAC de destino 01:0c:cd:01:00:02. Com isso, todo pacote que atender a essa correspondência estaria de acordo com a regra. É importante observar que o *switch* OpenFlow opera usando campos de diferentes camadas, o que garante uma alta flexibilidade no encaminhamento de pacotes.

O comportamento associado a uma regra de encaminhamento é chamado de instrução e, junto com outros campos, constituem uma entrada de fluxo OpenFlow. A entrada de fluxo é formada pelos campos descritos a seguir e é ilustrada na Figura 4.5(b) [10]:

- match: são os campos de correspondência. Eles consistem na porta de entrada e nos



(a) Campos para formar a regra no OpenFlow 1.3 [10]



(b) Principais componentes de uma entrada de fluxo no OpenFlow 1.3 [10]

Figura 4.5: Cada regra pode ser formada por 13 campos do cabeçalho. Cada entrada de fluxo tem além da regra outros campos associados, dentre ele a instrução que indica o que deve ser feito com o pacote que corresponder a regra.

cabeçalhos de pacote e, opcionalmente, nos metadados especificados por uma tabela anterior.

- prioridade: marca a prioridade que a entrada de fluxo tem em comparação com as outras. Uma entrada que especifica uma correspondência exata é sempre a maior prioridade. Todas as entradas com campos coringas têm uma prioridade associada. Se várias entradas possuírem a mesma prioridade, o *switch* é livre para escolher qualquer ordem;

- contadores: atualizam as estatísticas dos fluxos. Mantêm, entre outros, um registro do número de pacotes e *bytes* referentes a cada entrada de fluxo, o tempo decorrido desde a última vez que um pacote desse fluxo foi identificado pelo *switch* e o tempo desde a instalação do fluxo. O contador não possui indicador de *overflow*, com isso a contagem é reiniciada automaticamente ao alcançar o valor máximo [6].

- instruções: descreve como o pacote será processado e/ou para onde será encaminhado quando coincidir com uma determinada regra. Uma instrução pode, por exemplo, modificar o processamento do *pipeline*, enviando um pacote para outra tabela, ou pode conter uma lista de ações para ser aplicada. Com isso, cada entrada de fluxo contém um conjunto de instruções que são executadas quando um pacote corresponde a essa entrada. Apenas dois tipos de instruções são obrigatórias em *switches* OpenFlow: `Write-Actions` e `Goto-Table`. As demais são opcionais [10]:

  - Obrigatórias:

    * `Write-Actions <actions>` - Mescla a ação especificada no *action set*[§] atual. Caso uma ação do mesmo tipo já exista no conjunto atual, essa instrução sobrescreve a ação, em caso contrário, adiciona. As ações são detalhadas na Seção 4.1.2.

[§]O *action set* é o conjunto de ações OpenFlow a ser aplicado a cada pacote.

    * `Goto-Table <next-table-id>` - Indica qual a próxima tabela a ser consultada. O campo `table-id` é o identificador da tabela atual, o `next-table-id` precisa ser maior que o `table-id`. Os fluxos da última tabela não podem conter essa instrução, ou seja, se um conjunto de instruções não tem `Goto` significa que acabou o *pipeline* e que irá executar o `action set`.

  – Opcionais:

    * `Meter <meter id>` - Envia o pacote direto para um *meter* específico. Um *meter* controla a taxa de transmissão dos fluxos que entram no *switch*. É usado para garantia de QoS.A "Meter Table" é uma tabela utilizada para limitar a banda por fluxo. Através das instruções contidas no fluxo os pacotes são enviados para essa tabela para serem processados por estruturadas chamadas *Band*. Cada *band* tem uma taxa limite e é acionado se o fluxo de pacotes. Como resultado, o pacote pode, inclusive, ser descartado.
    * `Apply-Actions <actions>` - Aplica as ações especificadas imediatamente sem modificar o *action set* a ser aplicado a cada pacote. Essas instruções podem ser usadas para modificar o pacote entre tabelas e realizar múltiplas ações do mesmo tipo.
    * `Clear-Actions` - Apaga todas as ações no *action set* imediatamente.
    * `Write-Metadata <metadata/mask>` - Escreve o valor de um metadado no campo `Metadados`. A máscara especifica quais *bits* do metadado devem ser modificados.

- *timeouts*: tempo que o fluxo fica ocioso antes de expirar.
- *cookie*: esse valor é escolhido pelo controlador para ser usado por ele para filtrar estatísticas, modificações e detecções de fluxo. Não é usado no processamento de pacotes.

Ressalta-se que uma entrada de fluxo é identificada pela regra e pela prioridade e, com isso, essa dupla precisa ser única [10].

A tabela do *switch* OpenFlow é constituída por várias destas entradas de fluxos, e, portanto, é conhecida como tabela de fluxos [133], como mostrado na Figura 4.6.

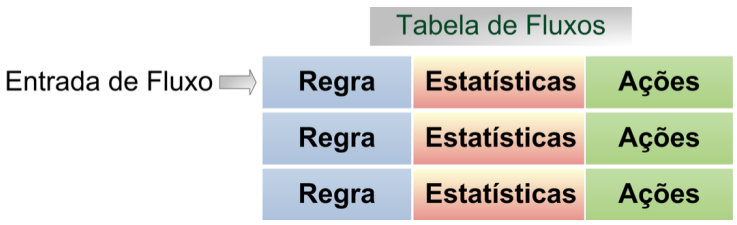


Figura 4.6: Tabela de Fluxos no OpenFlow 1.3 [10]

O *switch* OpenFlow precisa conter no mínimo uma tabela de fluxo, sendo mais simples se contiver apenas uma [11].

4.1.2 Ações e *Action Set*

O conjunto de ações que o pacote executa quando chega no final da linha de processamento é chamado *action set*. Ou seja, quando as instruções de uma entrada de fluxo não contêm a instrução `Goto-Table`, o processamento no *pipeline* de tabelas se encerra e as ações no *action set* são executadas. Se o *action set* está vazio, ou seja, não indica o que deve ser feito, o pacote é descartado. Esse conjunto é vazio por padrão [10]. O controlador, ao instalar uma entrada de fluxo na tabela, modifica esse conjunto usando a instrução `Write-Actions`.

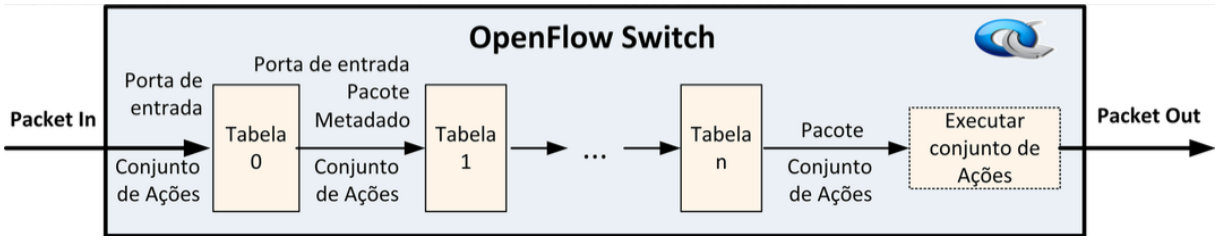
Assim como as instruções, nem todas as ações são obrigatórias. Inclusive, o controlador pode consultar o *switch* para saber quais ações opcionais ele suporta. As ações obrigatórias definidas no OpenFlow 1.3 são [10]:

- `Output` - Encaminha o pacote para uma porta OpenFlow específica. Os *switches* OpenFlow suportam o encaminhamento para os seguintes tipos de porta:
  - porta física - interface física do *switch*.
  - portas lógicas - abstrações de alto nível. Podem, por exemplo, estar associadas a várias portas físicas.
  - portas reservadas - portas definidas pela especificação OpenFlow para definir encaminhamentos genéricos:
    - `All` - todas as portas do *switch* que podem ser usadas para encaminhar um pacote específico. Só pode ser usada como porta de saída. Nesse caso, uma cópia do pacote é enviada para todas as portas exceto a de entrada e as configuradas para não participar da inundação.
    - `Controller` - representa o canal de controle com o controlador. Pode ser usada como porta de entrada, indicando que o pacote vem do controlador, ou saída. Quando usada como porta de saída, o *switch* encapsula o pacote ou apenas o seu cabeçalho em uma mensagem `Packet-in` e envia usando o protocolo OpenFlow.
    - `In-Port` - Envia o pacote para a porta de entrada.
    - `Normal` - Processa o pacote utilizando um encaminhamento tradicional.
- `Drop` - Não existe uma ação explícita para descartar o pacote. Ao invés disso, pacotes que não tiverem ações `Output` são descartados. Isso pode ocorrer, por exemplo, após uma instrução `Clear-Actions`.

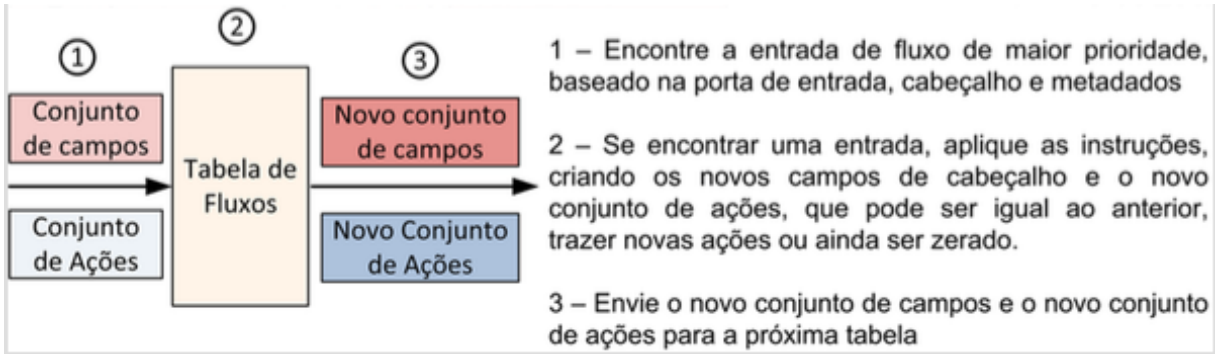
- `Group` - encaminha o pacote para um grupo específico. A exata ação vai depender do tipo de grupo, como será detalhado na Seção 4.1.4.

4.1.3 Processamento dos Pacotes no OpenFlow 1.3

As tabelas de fluxo do OpenFlow 1.3 são numeradas de 0 a n. O processamento do *pipeline* nos *switches* OpenFlow define como os pacotes interagem com as tabelas de fluxo, conforme a Figura 4.7 [9].



(a) Exemplo de processamento do *pipeline* nos *switches* OpenFlow [9].



(b) Processamento do Pacote por tabela [9, 61].

Figura 4.7: Fluxos de pacote através do *switch* OpenFlow [9].

Dessa forma, quando o pacote chega, se houver uma regra correspondente na primeira tabela, o pacote é processado ali, senão, se houver um link para outra tabela, esse pacote será encaminhado para a segunda tabela. O processamento sempre começa pela tabela de número 0. As outras tabelas são usadas de acordo com o resultado da correspondência feita na tabela anterior [9]. Se o fluxo encontrar uma regra configurada, as instruções para aquele fluxo serão aplicadas. O detalhamento desse processo é ilustrado na Figura 4.8.

Além disso, as entradas na tabela podem apontar para uma tabela de grupo. A tabela de grupo é projetada para realizar operações que são comuns a múltiplos fluxos. Dessa forma, ações são executadas para um grupo se for necessário, não apenas para um fluxo. Ações complexas de encaminhamento como múltiplos caminhos, agregação de enlaces e re-roteamento rápido são permitidas através desse mecanismo [112].

Com o OpenFlow, principalmente na versão 1.0 [6], o conhecimento global da rede no

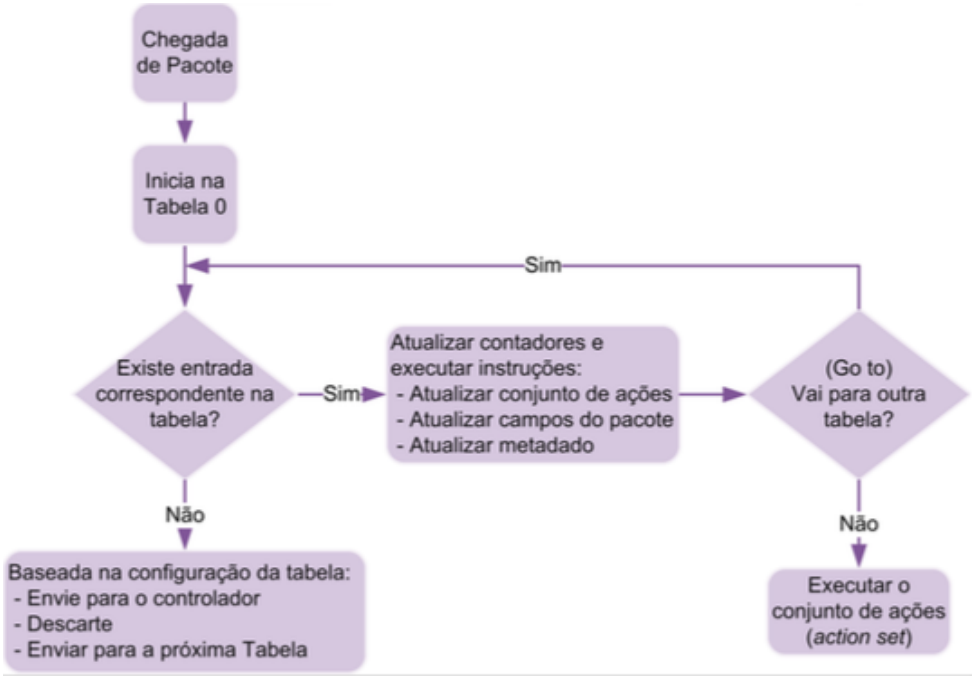


Figura 4.8: Fluxograma detalhando processamento dos fluxos através de um *switch* OpenFlow versão 1.1.0 [9].

plano de controle permite que um novo caminho seja instalado nos *switches*, em poucos milissegundos, depois da falha.

No entanto, a comunicação entre o plano de encaminhamento e o plano de controle é necessária para que a falha seja detectada e novos caminhos sejam calculados. Após o cálculo, as regras precisam ser configuradas nos *switches* para só então ser estabelecido um novo caminho. Todo esse processo adiciona uma latência entre a falha e o restabelecimento da rede. Desta forma, aplicações sensíveis ao atraso e que não podem sofrer perda acabam sendo afetadas por uma falha que deixa a rede um certo tempo "no escuro", fazendo com que os pacotes desse período sejam perdidos.

Assim, existe uma necessidade grande de que caminhos alternativos sejam pré-configurados nos *switches* sem que seja necessária uma comunicação com o controlador, fazendo com que seja perdido o mínimo de pacotes possíveis na rede. As tabelas de grupo do OpenFlow 1.3 [10] podem ser usadas com esse propósito, pois possuem um tipo de grupo intitulado *Fast-Failover*, que atende exatamente a esses requisitos.

4.1.4 Grupos OpenFlow e Tabela de Grupo

Um grupo OpenFlow é uma abstração que facilita as operações com pacotes mais complexos e específicos que não podem ser facilmente executadas através de uma entrada de tabela de fluxo. Cada grupo recebe os pacotes como entrada e executa uma ação. Um grupo não é capaz de executar instruções OpenFlow, então um grupo não pode, por exemplo, enviar

pacotes para uma tabela de fluxo. Portanto, o pacote deve ser tratado corretamente antes de entrar em algum grupo, pois os grupos não suportam *matching* nos pacotes, são apenas mecanismos para executar ações avançadas ou um conjunto de ações.

Uma tabela de grupos consiste em entradas de grupo. A capacidade de um fluxo apontar para um grupo permite que o OpenFlow adicione novos métodos de encaminhamento, onde cada entrada de grupo é associada a quatro campos, conforme a Figura 4.9 [9]:

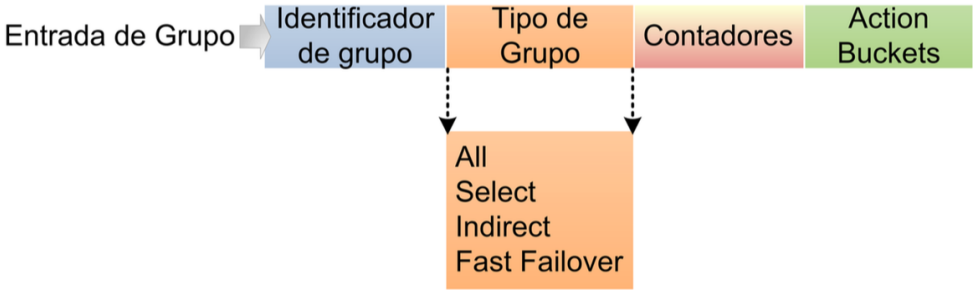


Figura 4.9: Tabela de Grupos. Uma entrada de grupo, no OpenFlow 1.1.0 ou superior, consiste nos campos identificador de grupo, tipo de grupo, contadores, e *action buckets* [9]
.

- Identificador de grupo: número que identifica unicamente o grupo.
- Tipo de grupo: determina que tipo de ações esse grupo pode tomar. Podem ser de quatro tipos: *all*, *select*, *indirect* e *fast failover*, detalhados a seguir.
- Contadores: contadores de pacotes atualizados a cada vez que um pacote é processado na tabela de grupo.
- *Action buckets*: lista ordenada de *action buckets*, onde cada *action bucket* contém um conjunto de ações para serem executadas.

Como mostra a Figura 4.10, um conjunto de ações é intitulado *bucket* e um grupo é formado por uma lista de *buckets*. Os parâmetros de um *bucket* são definidos de acordo com o tipo de grupo.

O tipo de grupo determina que tipo de ações o grupo pode tomar. Existem quatro tipos de grupo:

- *all*: Executa todos os *buckets* no grupo. O pacote é copiado para cada um dos *buckets*. Cada *bucket* pode possuir ações distintas o que permite que operações diferentes sejam executadas em cópias diferentes do pacote. É utilizado para o encaminhamento *multicast* e *broadcast*.
- *select*: Cada *bucket* tem um peso associado como parâmetro. Cada pacote que entra é enviado para um único *bucket* no grupo, baseado em algum algoritmo como *hash*

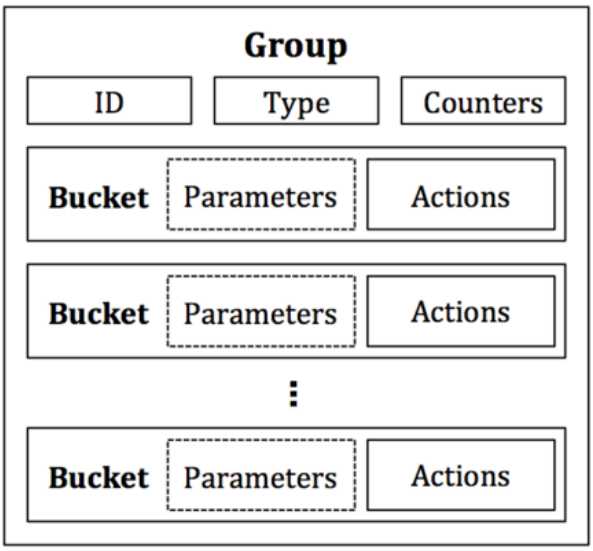


Figura 4.10: Componentes de um grupo e seus *buckets*. As ações em um *bucket* consistem de um conjunto de ações OpenFlow.

ou *round robin*. É utilizado para balanceamento de carga. Assim como o anterior, cada *bucket* pode conter uma lista de ações distintas.

- *indirect*: Só permite um único *bucket*. Tem como propósito ser usado como saída para diferentes entradas de fluxo de forma mais simples. Um exemplo seria um roteamento semelhante ao IP, aonde o bucket indicaria a porta de saída correta para uma rede ou um conjunto de redes. É usado para simplificar a implantação e reduzir o consumo de memória de um conjunto de fluxos similares.

- *fast failover*: criado para detectar e superar uma falha. Contém como parâmetro especial uma *watch port* e/ou *watch group*. Ambos os parâmetros ficam monitorando o estado da porta ou do grupo, ou seja, se ele está ativo ou não. Se o estado for considerado ruim, o *bucket* não é utilizado e é executado o primeiro *bucket* considerado ativo no grupo. Caso o *bucket* volte a ficar operante, este já poderá ser usado novamente. Ressalta-se que o *bucket* em uso não será alterado enquanto estiver ativo, só será descartado quando seu estado for passado para *down*. Esse tipo de grupo permite que o *switch* mude o encaminhamento sem a necessidade de comunicação com o controlador. Se não houver *bucket* ativo, o pacote será descartado. O tempo de comutação dependerá do tempo para procura do próximo *bucket*.

4.2 Considerações sobre o Estado da Arte em SDN

Para que seja possível a implementação de uma rede de comunicação resiliente para *smart grids*, alguns autores sugerem o uso de SDN. Akkaya et al. [30] discutem as vantagens do

uso de SDN para *smart grids*. Goodney et al. [64] apresentam uma proposta para uso com PMUs (*Phasor Measurement Unit*) e avaliam o atraso na rede. Os autores implementaram uma rede *multicast* para trafegar os dados com as medidas fasoriais e compararam a solução SDN com a abordagem convencional encontrando menor latência e melhor utilização de rede com o uso de SDN.

Cahn et al. [40] propõem o SDECN (*Software-Defined Energy Communication Network*) para uso em subestações e da mesma forma abordam a necessidade de desempenho. Os autores ressaltam o uso de IEC 61850 e o problema com o *multicast* de camada dois inundando a rede. Os autores afirmam terem implementado a proposta num cenário envolvendo 3 IEDs reais conectados em uma rede emulada com o mininet. No entanto, não apresentam os detalhes dos testes nem detalhes da arquitetura ou dos algoritmos utilizados. As informações da rede emulada, como tamanho ou topologia, não são citadas nem o tráfego gerado. Os autores afirmam que a contribuição está na verificação que o envio das mensagens *multicast* em camada dois não sofreu inundação e afirmam que a latência ficou abaixo de 4 ms.

Também para uso em subestações, Lopes et al. [120] propõem o SMARTFlow, também com o cenário envolvendo IEC 61850. Os autores descrevem a arquitetura, os módulos envolvidos e algoritmos propostos. A inundação com o uso do MAC *multicast* também foi abordada. Neste trabalho, os autores testam e avaliam a solução no emulador Mininet com um gerador de trafego GOOSE [126]. Foram avaliadas a carga na rede a carga de controle e a latência. Os resultados encontrados mostram que a forma reativa do OpenFlow não atenderia aos requisitos de atraso impostos pelo setor, mas a proposta proativa, atende bem ficando abaixo do limiar de 3 ms e com baixa carga de controle, além de não inundar a rede. Estes trabalhos não abordam recuperação de falha e têm enfoque apenas no tempo de atraso das mensagens.

Dorsch et al. [51] propõem o *SDN4SmartGrids* também com uma abordagem voltada para o IEC 61850, no entanto para a comunicação com MMS. Os autores avaliam a proposta com 4 *switches* emulados, um cliente e dois servidores para troca de tráfego MMS. O atraso de recuperação de falha ficou acima de 80 ms e os autores utilizaram o OpenFlow versão 1.0.

Pfeiffenberger et al. [152] abordam o uso de uma versão mais recente do OpenFlow, a 1.3, e com isso podem utilizar um mecanismo intitulado *fast-failover* para recuperação de falhas. Eles destacam as vantagens do *fast-failover* para realização de recuperação de falhas nas redes de comunicação para o setor elétrico. Entretanto, poucos detalhes são apresentados sobre algoritmos e lógica de controle e os autores não implementaram a proposta. Reitblatt et al. [159] propõem uma solução chamada Fattire para recuperação de falhas, mas não apresentam avaliações motivadoras já que os resultados não foram promissores. Os autores realizaram apenas um único teste com resultados na casa de segundos para se recuperar de uma falha. Ressalta-se que, apesar da abordagem com

multicast ser muito discutida, uma abordagem que envolva recuperação de falhas e árvores *multicast* é complexa.

Como demonstrado por Gyllstrom et al. [71], a recuperação de falhas ótima de uma árvore *multicast* centrada na origem é um problema *NP-hard*. Neste sentido, Gyllstrom et al. fazem a formulação do problema de otimização para a árvore *multicast* secundária. Ademais, propõem um mecanismo para detectar a falha com OpenFlow e os algoritmos aproximados para encontrar a árvore principal e backup. Abordam o uso do *IP multicast* e avaliam o algoritmo com o Mininet e o OpenFlow versão 1.0.

Com relação a investigação do uso de SDN para sistemas SCADA, Silva et al. [48] discutem que uma rede SCADA baseada em SDN pode facilitar a concepção e o desenvolvimento de aplicações de rede inteligente, tornando-as mais robustas e flexíveis. Os autores têm enfoque no uso de SDN para tornar os sistemas SCADA mais seguros, assim como a maioria dos trabalhos que relacionam SDN e SCADA [48, 153, 13]. Silva et al. afirmam que é possível ter uma visão global do sistema elétrico a partir de sistemas SCADA baseados em SDN, e com isso, podem coletar estatísticas de *switches*. A partir daí, com o auxílio de técnicas de aprendizado de máquina, podem detectar comportamentos anômalos no SCADA. O trabalho utiliza um dos primeiros protocolos usados para supervisão, o MODBUS [146]. Por ser extremamente simples e sem muitas funcionalidades, os fornecedores costumam modificar sua operação para implementar mais características que não estão incluídas no protocolo. É um protocolo difícil de interoperar, tem pouquíssimos recursos e tem sido substituído por protocolos como o *Distributed Network Protocol v.3* (DNP3) e IEC 60870-5, ambos dos anos 1990 [118], e mais recentemente, pelo protocolo MMS – IEC 61850 [86]. Silva et al., em seu trabalho anterior [13], também utilizaram o Modbus para estudos de segurança para o SCADA com o uso de SDN. Espera-se que trabalhos propondo o uso de SDN avaliem soluções com protocolos mais atuais como os da norma IEC 61850, que estão sendo indicados para comunicação em *smart grids*. Nesse sentido, Pigossi e Lopes [153] utilizam o protocolo MMS, da norma IEC 61850, para a avaliação proposta no artigo. Os autores discutem os ganhos para tornar as redes SCADA mais seguras quando são utilizados mecanismos de autenticação. A proposta inclui o uso de SDN e MMS e foi implementada com o emulador Mininet.

Ressalta-se que os trabalhos têm enfoque no aumento da segurança em redes SCADA e não abordam a possibilidade de utilização do SCADA como ator na decisão de provisionamento da rede de comunicação, nem interações relacionadas às aplicações de energia. Os trabalhos utilizam os conceitos de SDN para captura de pacotes de forma a aplicar as respectivas técnicas propostas.

Portanto, o uso de SDN para redes elétricas inteligentes ainda apresenta muitos desafios. O OpenFlow [133], que é o principal padrão de comunicação em uma arquitetura SDN, se implementado como a maioria de suas aplicações (de forma reativa), não atende aos requisitos das *smart grids*, como já foi inicialmente analisado em [120]. O funcionamento

de uma rede elétrica inteligente baseada em SDN é ainda um desafio tratado na literatura. Isto ocorre, pois o cenário das redes elétricas inteligentes é bastante diferente do cenário comumente empregado para as soluções SDN. Outro ponto é que, como mostrado em [120], o simples uso de SDN não garante que os requisitos de qualidade de serviço sejam atendidos.

Outras propostas encontradas na literatura abordam questões específicas como o balanceamento de carga, mas não abordam o conjunto das redes elétricas inteligentes. Com isso, a implementação isolada destas soluções pode não atender, de fato, às redes elétricas inteligentes, já que apresentam limitações em pontos essenciais, como na qualidade de serviço [135, 64, 50], na segurança [176, 39, 64, 156, 51], no encaminhamento inteligente [135, 176, 39, 40, 156, 50], dentre outros. Ressalta-se que, até onde é conhecimento da autora deste trabalho, as propostas da literatura não abordam a interação com o supervisório para permitir o desenvolvimento de novas aplicações de energia que utilizem uma descoberta automática de dispositivos/topologia no supervisório e a modificação dinâmica dos recursos de rede, o que é uma das motivações principais para o desenvolvimento desta tese. Da mesma forma, não foi encontrado um *framework* que seja autonômico por interagir com os IEDs e configurar cada fluxo de forma individual, garantindo as características encontradas no IEDs como acontece com o ARES.

Essas características são resumidas na Tabela 4.1, que relacionada as características levantadas no estado da arte com os trabalhos mencionados.

Tabela 4.1: Propostas para redes elétricas inteligentes baseadas em *smart grid*. "✓" indica que o tópico foi abordado mesmo que parcialmente e "–" que não foi abordado.

Aspectos	Goodney et al. [64]	Cahn et al. [40]	Lopes et al. [120]	Dorsch et al. [51]	Molina et al. [135]	Sydney et al. [176]	Byun et al. [39]	Qin et al. [156]	Kim et al. [93]	Dong et al. [50]	Pfeiffenberger et al. [152]	Reitblatt et al. [159]	Gyllstrom et al. [70]	Pigossi e Lopes [153]	Silva et al. [48]
Domínio	PMU	SE	SE	SG	SG	SG	SG	SG	SG	SG	SG	SG	SG	SE	SG
Monitoramento da Rede/Sistema	–	✓	✓	✓	✓	✓	✓	✓	–	✓	–	–	–	–	–
Descoberta de Dispositivos	–	–	✓	✓	–	–	–	–	–	–	–	–	–	✓	–
Balanceamento de Carga	–	✓	–	–	✓	✓	✓	–	–	–	–	–	–	–	–
Qualidade de Serviço	–	–	✓	✓	–	✓	✓	✓	–	–	–	–	–	–	–
Segurança	–	✓	–	–	✓	–	–	–	–	✓	–	–	–	✓	✓
Recuperação de Falhas	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	–	–

Phasor Measurement Unit (PMU). *Smart Grid* (SG). Subestações (SE)

Capítulo 5

A Proposta ARES

O desenvolvimento de um *framework* para comunicação autonômica e resiliente para as redes elétricas inteligentes é fundamental para que novas aplicações de energia sejam desenvolvidas e para que as que estão sendo propostas na literatura possam ser, de fato, implementadas. Geralmente, as soluções são propostas levando em consideração que todas as informações estarão disponíveis o tempo todo nos dispositivos de interesse e que a rede de comunicação responderá em tempo real quando necessário [162, 153, 144, 33, 89, 129, 99, 72, 182, 188, 167, 12, 41, 66, 178, 16, 15].

Esta tese propõe o *framework* ARES, que traz como principal contribuição um novo paradigma para a área de redes elétricas por permitir interação entre o sistema supervisório e a configuração automática da rede de comunicação visando autonomia na configuração dos fluxos da rede e flexibilidade. A configuração autonômica pode ser realizada tanto com participação do plano de gerenciamento ARES quanto de forma direta, através do plano de controle do ARES.

A proposta permite que os sistemas supervisórios possam alocar recursos de comunicação sob demanda, a partir de informações do supervisório, ou de forma autonômica a partir dos *datasets* configurados nos dispositivos finais. Com isso, a infraestrutura de comunicação de uma *microgrid*, por exemplo, pode ser alocada dinamicamente de forma automática a partir do sistema supervisório. A partir da necessidade de implementação de comunicação entre veículos elétricos, medidores ou GDs, por exemplo, o sistema pode avaliar seus recursos, e, se existentes, alocar e configurar a rede de comunicação de forma automática a partir da aplicação de energia, do plano de controle ARES ou do comando de um operador. Da mesma forma, caso não existam recursos disponíveis, eventos de falha são enviados com informações sobre o "não provisionamento do enlace". Esta solução traz escalabilidade para as redes elétricas inteligentes, já que a necessidade de configuração manual da rede de comunicação a cada nova implementação faz com que o seu avanço seja muito custoso e lento.

A proposta também objetiva prover informações importantes para as aplicações de

energia deixando o sistema de controle e supervisão mais eficiente. Com o ARES, o sistema de supervisão e controle pode automaticamente e dinamicamente mapear os recursos de energia distribuídos e cargas do sistema assim que estes iniciem seu funcionamento. Quando um medidor inteligente, um painel fotovoltaico, uma carga, etc. forem ligados à rede de comunicação, o ARES coletará informações e as disponibilizará para as aplicações de energia para que estas possam fazer os mapeamentos automaticamente.

Além disso, o ARES também trata da resiliência da rede de comunicação usada para interligar os dispositivos que exijam requisitos temporais rígidos de comunicação. Nesse sentido, o ARES deverá garantir que falhas na rede de comunicação não interfiram em aplicações de energia críticas, como as de proteção e controle. Da mesma forma, é importante que a rede seja configurada de forma mais eficiente. Alguns protocolos que estão sendo propostos para comunicação em redes elétricas inteligentes, como o GOOSE e o SV (detalhados na Seção 3.4), além de possuírem uma restrição temporal rígida, têm características que podem sobrecarregar a rede de comunicação. Esses protocolos funcionam diretamente sobre a camada de enlace e utilizam o modelo publicador-assinante com um endereço de destino MAC *multicast*. Por padrão, os *switches* não reconhecem esse endereço e, para garantir que a mensagem vai chegar ao destino, a encaminham por todas as portas. Como esses protocolos já têm características de tráfego elevado, precisam ser tratados de uma forma mais inteligente, com a configuração de árvores *multicast* de camada 2. O ARES objetiva prover uma rede de comunicação mais eficiente para tratar esse tipo de tráfego, além do tráfego *unicast* (cliente/servidor) gerado por sistemas supervisórios.

É importante ressaltar que os protocolos de comunicação propostos para uso em redes elétricas inteligentes não possuem características de segurança em sua concepção. Mecanismos de autenticação e autorização, por exemplo, não fazem parte da estrutura desses protocolos [121]. No entanto, normas e iniciativas como a IEC 62351 [46] e a *North American Electric Reliability Corporation* (NERC) *Critical Infrastructure Protection* (CIP)* têm estudado formas de mitigar as vulnerabilidades encontradas nesses protocolos e estão sendo constantemente discutidos pelo setor elétrico, e principalmente pelo Comitê Internacional de Produção e Transmissão de Energia Elétrica (CIGRE). Como o *framework* proposto visa permitir que dispositivos sejam automaticamente mapeados no supervisório e os protocolos utilizados não levam em consideração mecanismos de segurança, é pré-requisito para implementação do *framework* ARES que os padrões sejam levados em consideração e que as características de segurança sejam observadas. Apesar de segurança estar fora do escopo desta tese, a autora reconhece e ressalta esta necessidade que será coberta em trabalhos futuros.

O segundo pré-requisito para a implementação do ARES é a utilização da modelagem da Norma IEC 61850 [177]. Para garantia de interoperabilidade entre os dispositivos da rede elétrica inteligente, o ARES é desenvolvido de acordo com a modelagem IEC 61850. Essa

*O plano NERC CIP consiste em 9 padrões visando cobrir a segurança para infraestruturas críticas. Disponível em: www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

escolha é devida à dificuldade que o setor elétrico passa ao usar tecnologias proprietárias ou diversos padrões não interoperáveis. Muitas das vantagens das redes elétricas inteligentes são devidas ao enorme aumento da comunicação entre dispositivos. Quando as empresas precisam lidar com diferentes tecnologias de comunicação, as dificuldades técnicas, custos de implementação e manutenção aumentam. Ademais, as concessionárias e fabricantes reconhecem a crescente necessidade de ter um padrão internacional que defina as interfaces de comunicação e controle para todos os dispositivos [80]. Assim, uma implementação padronizada para medidores inteligentes, DERs e todos os equipamentos envolvidos na comunicação da rede elétrica inteligente torna a solução mais simples, interoperável e flexível.

E por fim, o uso de redes definidas por *software*, é também pré-requisito para implementação do ARES. Com SDN, mais especificamente o OpenFlow, o provisionamento da rede de comunicação pode ser feito de forma dinâmica e em tempo real, de forma transparente para os outros serviços. Como o ARES possui módulos de provisionamento de acordo com o serviço em questão, uma tecnologia que permita o tratamento do tráfego de comunicação de acordo com seus requisitos de QoS e de forma dinâmica é essencial para a implementação da proposta. Por esse motivo, o *framework* ARES é baseado no OpenFlow.

5.1 Requisitos de Comunicação para as Aplicações de Energia de Nova Geração

A característica multifuncional dos dispositivos exige que a rede de comunicação seja pensada de acordo com a QoS exigida por cada domínio. Além disso, a quantidade de dispositivos para serem configurados no supervisório aumenta exponencialmente. Soluções que dependam de configurações manuais, tanto da rede de comunicação, quanto dos dispositivos e do supervisório, passam a parecer inviáveis. Com isso, o mapeamento automático desses dispositivos no supervisório passa a ser extremamente desejável. Da mesma forma, o mapeamento da função do dispositivo (gerador ou carga, por exemplo) também é necessário. Além desse, outros requisitos de comunicação são demandados para permitir não só a comunicação entre dispositivos, mas também a implementação de novas aplicações de energia.

Recentemente, têm sido propostas diversas aplicações de energia para o sistema supervisório das redes elétricas inteligentes. Essas aplicações levam em consideração a capacidade de comunicação bidirecional de sensores e atuadores na rede, a disponibilização de informação para o supervisório, além da inserção de medidores inteligentes, VEs, DERs, etc. Apesar desse cenário trazer diversas oportunidades, as aplicações de energia pouco têm explorado as possibilidades que esta rede de nova geração pode viabilizar.

Para a construção de um *framework* para comunicação inteligente em uma rede elétrica de nova geração é necessário entender quais requisitos de comunicação são necessários para as redes elétricas inteligentes. Da mesma forma, para um entendimento melhor do que as aplicações de energia de nova geração, chamadas nesta tese de SCADA-NG, são capazes, é essencial que seja realizado o levantamento do que a rede de comunicação pode prover para as aplicações de nova geração para o sistema elétrico. A ideia engloba o levantamento das características de comunicação entre dispositivos inteligentes e entre eles e o sistema supervisório.

De fato, uma das contribuições desta tese é o levantamento desses requisitos e o que é demandado da rede de comunicação para permitir não só a comunicação entre dispositivos, mas também a implementação de novas aplicações de energia.

5.1.1 Requisitos de Desempenho da Rede de Comunicação

A comunicação nas redes elétricas inteligentes tem duas características fortes e distintas: comunicação entre dispositivos inteligentes e comunicação entre eles e o supervisório. Essas características, já bastante conhecidas em subestações, fazem com que a natureza da comunicação seja bastante diferente. No primeiro caso, os dispositivos inteligentes se comunicam diretamente para tomar decisões importantes e, geralmente, essas decisões englobam a proteção e controle do sistema elétrico. No segundo caso, os dispositivos trocam informações com o supervisório para monitoramento e controle remoto, como comandos, corte/religamento e medições. Com isso, há dois cenários de comunicação bastante distintos com requisitos diferentes. Nesta tese, a comunicação entre dispositivo e supervisório será intitulada comunicação vertical, e a comunicação entre dispositivos sem a interferência de um supervisório será intitulada comunicação horizontal, nomenclaturas já utilizadas em subestações. A compreensão dos requisitos de qualidade e disponibilidade dessas duas formas de comunicação [124] é essencial para o desenvolvimento do *framework* ARES, que visa provisionar automaticamente os enlaces de comunicação para as redes elétricas inteligentes.

5.1.1.1 Comunicação Vertical

Essa forma de comunicação é caracterizada pela troca de mensagens entre o supervisório e os dispositivos inteligentes, apresentando uma restrição temporal pouco rígida. Geralmente, são aceitos entre 100 ms e 1000 ms de atraso [179, 177] de acordo com o tipo de aplicação. Os protocolos utilizados estão na camada de aplicação e geralmente utilizam o modelo cliente/servidor com endereço de destino *unicast* para comunicação. Essa comunicação, usada para monitoramento e controle, já é bem conhecida desde a década de 1970 com a utilização do protocolo MODBUS [146]. Com o decorrer do tempo, novos protocolos foram propostos com novas funcionalidades, como o DNP3 [7] e o MMS [3].

A comunicação vertical tem estreita ligação com o provimento de facilidades para o supervisório, como descrito na Seção 3.3. Dentre as novas funcionalidades, o processo de auto-descrição (*self-description*) do MMS é um dos mais motivadores. O *self-description* já aponta uma iniciativa na área para tornar a configuração do supervisório mais automatizada e dinâmica. Ressalta-se que os protocolos utilizados para essa comunicação, geralmente, estabelecem conexão com cada dispositivo inteligente na rede, o que, dependendo da escala da rede, pode não ser possível. Esse cenário sugere que a conexão seja realizada para um concentrador ao invés da forma individual.

5.1.1.2 Comunicação Horizontal

Por ser utilizado na proteção da rede, o enlace de comunicação horizontal deve atender a restrições temporais muito fortes. Neste caso, um atraso na comunicação é crítico, podendo causar acidentes devido a uma atuação atrasada.

Os protocolos usados na comunicação horizontal são mapeados diretamente sobre a camada de enlace. Não usam mecanismos de confirmação de entrega de mensagem e, por esse motivo, usam mecanismos de retransmissão da informação para garantir a entrega do dado[†]. Essa característica já mostra que a carga na rede pode se tornar uma preocupação, já que as mensagens horizontais são enviadas para endereços MAC multicast e, como já foi explicado, isso leva a inundações na rede. Ressalta-se, ainda, que as mensagens horizontais, usualmente, possuem alta prioridade, o que pode se tornar um outro complicador, em caso de a rede estar saturada com essas mensagens.

Os protocolos de comunicação horizontal, na sua maioria, utilizam um modelo publicador/assinante para comunicação. Os principais protocolos que se enquadram nesse caso são o GOOSE e o SV, ambos da norma IEC 61850.

5.1.2 Requisitos Funcionais para a Rede de Comunicação

A Tabela 5.1 resume as características das comunicações horizontais e verticais. Com as características de comunicação levantadas, as funcionalidades desejáveis da rede podem ser mapeadas.

Com relação à comunicação horizontal, que se dá entre os dispositivos, o aumento do tráfego de comunicação durante eventos críticos de energia, gerados por esquemas de proteção, controle e monitoramento, podem dificultar o desempenho da rede de comunicação e, por sua vez, interromper os esquemas de proteção e controle que dependem dele. Como a comunicação entre dispositivos é feita em camada dois com endereçamento de destino MAC multicast, o consumo de banda pelo tráfego de dados em redes compostas por

[†]Considera-se que o uso de uma camada de transporte, ou ainda, que a espera por uma confirmação antes de reenviar uma mensagem perdida trazem atrasos inviáveis à aplicação de proteção.

Tabela 5.1: Características da comunicação para redes elétricas inteligentes.

Característica	**Comunicação**	
	HORIZONTAL	VERTICAL
Restrição de Atraso	$\leq$ 3 ms, 4ms, 10ms, de acordo com o tipo da mensagem (Tabela 3.2)	$\leq$ 100 ms, 500 ms, 1000 ms, de acordo com o tipo da mensagem (Tabela 3.2)
Necessidade de Autonomia no SCADA	Não se aplica	Alta
Carga na Rede	Alta	Média
Número de fluxos simultâneos	Alto	Alto
Exemplo de Protocolos	GOOSE, Sampled Values	Modbus, DNP3, MMS

switches típicos é alto. Para que isso não aconteça e a rede não fique sobrecarregada com mensagens desnecessárias, uma árvore *multicast* em camada dois precisa ser implementada, idealmente de forma transparente para os dispositivos finais[‡].

Outro ponto crítico na comunicação entre dispositivos é a restrição temporal crítica que requer redes mais eficientes e confiáveis. A indisponibilidade da rede não pode afetar os esquemas de proteção e controle. A restrição temporal mais rígida levantada foi a de 3 ms [179, 177]. Esse é o tempo total que uma mensagem deve levar de dispositivo de proteção a outro, logo, o tempo de recuperação total da rede, incluindo o tempo para a detecção da falha de comunicação, não pode ultrapassar esse valor. Ressalta-se que é desejável que o tempo de recuperação se aproxime de zero já que esse limiar é relacionado ao atraso na rede e não ao tempo em que a rede fica indisponível. Idealmente, a solução precisa oferecer um tempo de recuperação total baixo de forma que uma indisponibilidade na rede de comunicação não afete o sistema elétrico.

Com relação à comunicação vertical, entre dispositivo inteligente e supervisório, a ideia abrange a disponibilidade de funcionalidades que tornem o SCADA mais automático com configurações mais facilitadas. A necessidade de um SCADA mais autonômico também foi apontada por autores que afirmam que a escala das redes elétricas inteligentes não pode ser gerenciada pelos SCADAs atuais [113]. A configuração manual do SCADA já é desafiadora quando limitada a subestações. Esse desafio é ainda maior se relacionado a todas as áreas das redes elétricas inteligentes. Também é importante ressaltar que configurações manuais podem resultar em erro de configuração, atraso de configuração e, algumas vezes, em maiores custos com fornecedores e equipe. O sistema SCADA precisa ser mais autonômico

[‡]Métodos que montam árvores *multicast* geralmente precisam que os dispositivos implementem mecanismo de *join* e *leave*, para entrada e saída da árvore. Isso, além de gerarem uma certa carga de controle na rede, exigem que os dispositivos inteligentes implementem essa funcionalidade.

para incorporar um sistema elétrico e de comunicação que se torna mais dinâmico.

A necessidade de um sistema dinâmico para permitir que um DER se registre em um cliente SCADA, especificado apenas com seu endereço IP, já foi apontada na literatura [56]. A ideia engloba que as características, as propriedades e a capacidade disponível da DER pudessem ser disponibilizadas de forma automatizada para o SCADA. Essa característica mostra que as funções dos dispositivos precisam ser mapeadas de forma automática no supervisório. Da mesma forma, a alteração de funções em dispositivos multifuncionais também precisa ser relacionada. Para que isso seja possível, os dispositivos precisam se associar na rede automaticamente, sem necessidade de configuração por um operador.

Como detalhado em [121], segurança é um ponto crítico em redes elétricas inteligentes, tanto na comunicação para o supervisório quanto na comunicação entre dispositivos. Propostas que objetivam deixar o sistema mais dinâmico e automatizado precisam levar em conta, ao menos, requisitos básicos de segurança.

Um ponto chave no levantamento realizado é a possibilidade de configuração e provisionamento da rede de comunicação a partir do sistema supervisório de forma autonômica. Com o mapeamento automático de dispositivos e funções, caso seja possível o mapeamento automático também da rede de comunicação, o sistema supervisório, com base nos recursos de rede necessários informados pelas aplicações de energia, pode provisionar de forma automática a sua rede de comunicação. Isso significa que, ao implementar uma AMI ou uma *microgrid*, os recursos de comunicação podem ser alocados de acordo com a necessidade definida pela aplicação de energia e a função esperada dos dispositivos. O mesmo se encaixa para subestações, esquemas de resposta à demanda, gerenciamento de VEs, etc. Por exemplo, caso a aplicação de energia precise ser composta por GDs se comunicando entre si para trocar informações de controle e proteção, a alocação dos recursos de rede poderia ser feita de forma automática levando em consideração a funcionalidade dos dispositivos envolvidos e a característica do tráfego. Nesse caso, seriam alocados recursos para o tráfego *multicast* de mensagens GOOSE e SV na comunicação entre dispositivos, além dos recursos de comunicação *unicast* para o supervisório. Essas necessidades levantadas são resumidas na Tabela 5.2.

Tabela 5.2: Funcionalidades desejáveis para comunicação para redes elétricas inteligentes.

Necessidades	**Comunicação**	
	HORIZONTAL	VERTICAL
Tratamento de Endereços Multicast camada 2	Crítica	Não se aplica
Recuperação de Falhas	<3ms	<100ms
Mapeamento Automático de Dispositivo	Não se aplica	Desejável
Mapeamento Automático de Função	Não se aplica	Desejável
Provisionamento Automático de Enlaces	Desejável	Desejável
Segurança	Crítica	Crítica

Com a implementação de um *framework* que tenha como base os requisitos apontados

na Tabela 5.2, o sistema supervisório tradicional pode ser aperfeiçoado para incorporar novas características e funcionalidades, permitindo o desenvolvimento de um supervisório de nova geração.

Nesta tese, entende-se que as aplicações de energia que estão sendo criadas podem integrar o sistema supervisório fazendo parte de um plano de gerenciamento, descrito na Seção 5.2. Essa integração permite desenvolvimentos mais interoperáveis e inteligentes. O supervisório de subestações atual, por exemplo, seria uma aplicação de energia que faz parte do plano de gerenciamento. Com a oferta das funcionalidades apontadas na Tabela 5.2, espera-se que possam ser criadas aplicações de energia com serviços mais inteligentes e autonômicos. A possibilidade de configuração da rede de comunicação de forma automática traz muitos ganhos nesse desenvolvimento. Do mesmo modo, a possibilidade de desenvolvimento de aplicações com base em um *framework* único torna o sistema mais interoperável e flexível.

Portanto, o *framework* proposto visa permitir que as aplicações de energia de nova geração sejam implementadas em um SCADA aperfeiçoado, intitulado, nesta tese, como SCADA-NG.

5.2 Arquitetura do *framework* ARES

O *framework* ARES, proposto para atender aos requisitos do SCADA-NG, tem a arquitetura ilustrada na Figura 5.1, que mostra a interação entre os cinco planos que constituem a proposta.

No plano superior, intitulado ARES-based Management Plane, é onde estão localizadas as aplicações de energia das redes elétricas inteligentes. Neste trabalho, propõe-se o SCADA *Next Generation* (SCADA-NG) que estende o SCADA atual para incluir as novas aplicações de energia que interagem automaticamente com a rede de comunicação. Além do monitoramento remoto, controle e das funções tradicionais do SCADA, o SCADA-NG é capaz de configurar e provisionar os recursos de comunicação da rede elétrica inteligente através da API ARES. Além disso, recursos já configurados nos IEDs podem ser liberados para funcionamento através de comandos. Assim, o SCADA-NG interage com todo o sistema, incluindo IEDs, medidores inteligentes, DERs, veículos elétricos, etc. Para que a solução possa atender a diferentes necessidades e para que a concessionária possa utilizar apenas as aplicações de energia em que tenha interesse, o SCADA-NG deve ser modular. Sistemas de gerenciamento pelo lado da demanda, supervisão e controle de subestações, gerenciamento de *microgrids*, carga e descarga de veículos elétricos, gerenciamento da proteção adaptativa, dentre outros, são exemplos de aplicações de energia. A modularidade do SCADA-NG também permite que as aplicações de energia sejam desenvolvidas separadamente mesmo que utilizem os mesmos recursos. É importante ressaltar que os requisitos foram levantados para que o ARES possa disponibilizar as

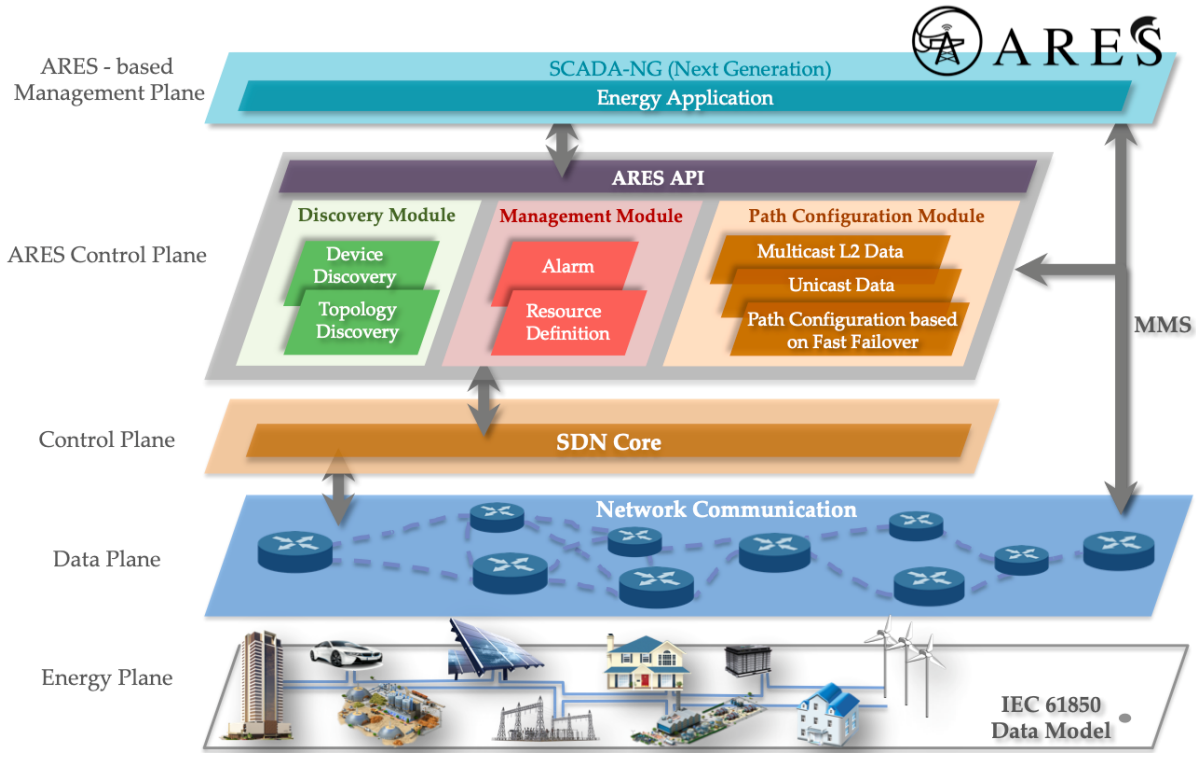


Figura 5.1: Visão geral da arquitetura do ARES com a interação entre os cinco planos.

funcionalidades que podem ser interessantes para aplicações de energia de nova geração.

Interagindo com o SCADA-NG está o ARES Control Plane, que oferece a API ARES, detalhada na Seção 5.4, e é composto por três módulos e seus componentes. Como pode ser visto na Figura 5.1, a ARES API funciona como uma *north bound* API para o plano de controle do ARES. Todas as funcionalidades disponibilizadas pela API se baseiam em três módulos principais, que constituem o núcleo do plano de controle ARES, sendo eles o *Management Module* com os componentes *Alarm* e *Resource Definition*; o *Discovery Module* com os componentes *Device Discovery* e *Topology Discovery*; e o *Path Configuration Module* com os componentes *Multicast L2 Data*, *Unicast Data* e *Path Configuration based on Fast Failover*. Os três módulos e seus componentes são detalhados na Seção 5.3. Ressalta-se que o plano de controle ARES possui uma comunicação MMS com os dispositivos finais (IEDs) de forma a coletar informações necessárias para a configuração autonômica e também para liberar ou não a comunicação de determinado elemento/fluxo na rede.

A API ARES é responsável pela interação entre as aplicações de energia do SCADA-NG e os módulos ARES. Esta API recebe as chamadas das aplicações de energia e traduz em entradas para os componentes ARES, que, por sua vez, podem alterar a rede de comunicação. Além disso, as informações geradas pelos componentes, como por exemplo quais recursos de geração distribuída entraram ou saíram da rede, também são traduzidas para as aplicações de energia através desta API.

Dentre suas funcionalidades, a API disponibiliza para as aplicações de energia do SCADA-NG serviços de detecção de cargas, tais como DERs, veículos elétricos, baterias, medidores inteligentes, etc. Assim, as aplicações podem automaticamente mostrar em tela para os operadores do sistema os dispositivos usados por aquela aplicação, sem a necessidade de configuração manual. Com isso, cargas e DERs, além de IEDs e *switches* poderão ser mostrados dinamicamente no supervisório. Entradas e saídas de dispositivos oriundas tanto de novos comissionamentos como também de falhas no sistema poderão ser automaticamente reportadas para o SCADA-NG. Isso torna as aplicações de energia mais escaláveis e flexíveis permitindo que o SCADA execute aplicações de energia em tempo real.

A API ARES provê serviços de comunicação para o SCADA-NG, como o provisionamento de enlaces, o mapeamento de dispositivos e da rede de comunicação e o monitoramento de eventos. Com isso, os enlaces são configurados de acordo com o tipo de tráfego demandado e a QoS necessária. Permite também o desenvolvimento e implementação de novas aplicações de energia que precisem ou possam lidar com o suporte da rede. Esta é uma das principais inovações da proposta, já que as aplicações SCADA tradicionais apenas se apoiam em uma rede que interconecta dispositivos e não possuem a possibilidade de configuração automática. A proposta ARES provê serviços autonômicos que podem melhorar consideravelmente o desempenho e a eficiência das aplicações de energia das redes elétricas inteligentes. Os componentes ARES e a API ARES podem ser implementados em qualquer controlador SDN e, visando maior robustez, também podem ser implementados em mais de um controlador de forma distribuída.

Abaixo do ARES Control Plane, encontra-se o Control Plane da rede SDN. Este plano contém o núcleo do controlador SDN, que é capaz de se comunicar com o Data Plane, usando o OpenFlow [11]. Os recursos desse plano permitem que os módulos do plano superior sejam desenvolvidos. Recursos como a descoberta de *switches* e a criação de grupos ou de caminhos (calculados pelo plano ARES Control Plane) já são capacidades que o *framework* herda por ser baseado em SDN.

O Data Plane compreende a comunicação entre todos os dispositivos da rede de comunicação, que é configurada de forma automática e eficiente. Como será visto adiante, os elementos de rede na modelagem ARES são dispositivos intitulados *datapaths* do tipo *switch* OpenFlow, por exemplo.

Por fim, o plano mais baixo é onde estão localizados os dispositivos de energia. Nesse plano, intitulado Energy Plane, localizam-se os medidores inteligentes, os relés e o Controlador Lógico Programável (CLP), os DERs, os VEs e qualquer dispositivo que seja considerado uma carga, um gerador, um item de armazenamento, um sensor ou um atuador, ou ainda um controlador, desde que se comunique com a rede. Uma característica importante é que os dispositivos devem seguir a modelagem IEC 61850 para que o *framework* ARES possa ser totalmente implementado. Com isso, todos esses

dispositivos são considerados IEDs, e de forma mais específica, dispositivos físicos, de acordo com a modelagem IEC 61850. Como será visto adiante, esses dispositivos são intitulados *datapaths* do tipo IEDs na modelagem ARES.

Dentre os requisitos mapeados para o SCADA-NG, está a operação e gerência eficiente de dispositivos de energia usando o protocolo MMS-IEC 61850. Para que isso seja possível, a API ARES, os componentes e os módulos ARES deverão ser implementados para prover esses recursos para o SCADA-NG. Com isso, três características são importantes na proposta e implementação do ARES: rede de comunicação com dispositivos SDN, dispositivos do plano de energia de acordo com a norma IEC 61850, implementação de mecanismos de segurança como autenticação, etc. Esta tese engloba a descrição de todo o *framework* para permitir que as aplicações de energia do SCADA-NG sejam criadas com um uso mais inteligente dos dispositivos e recursos da rede. No entanto, as aplicações de energia são diversas e não fazem parte do escopo deste trabalho. Tanto o desenvolvimento de módulos de segurança, quanto as diversas aplicações de energia possíveis, são trabalhos futuros promissores.

5.3 Os Componentes e Módulos ARES

Os componentes ARES são baseados em configurações de rede reativas, proativas e híbridas usando OpenFlow. Na configuração proativa, o controlador define regras automaticamente assim que um *datapath* é ligado. Na configuração reativa, o controlador responde a um evento específico, como a conexão ou desconexão de um DER. Assim, um evento desencadeia automaticamente ações reativas. Contudo, com o objetivo de proporcionar uma maior velocidade de configuração, pode também ser utilizada uma configuração híbrida.

Uma vantagem grande, que traz ganhos no desempenho da rede, é que o cálculo inicial para estabelecimentos dos caminhos é realizado proativamente, durante a inicialização da rede, evitando, assim, a necessidade de cálculos de rotas ou de mensagens de controle durante o funcionamento da rede. Essa é uma das diferenças básicas para os componentes nativos[§] do OpenFlow, que têm um funcionamento reativo. Ressalta-se que o funcionamento proativo, apesar de pouco implementado em *data centers* ou na Internet, pode ser implementado em redes de comunicação usadas para automação do sistema de energia, pois elas possuem um padrão comportamental bem definido. É essa característica que difere muito as redes de comunicação para automação do sistemas elétrico das redes corporativas, por exemplo. Redes de comunicação para o sistema elétrico utilizam protocolos bem definidos e serviços específicos, com cada fluxo muito bem conhecido, assim como cada

[§]Entende-se, nesta tese, por componentes nativos do OpenFlow, as aplicações de controle OpenFlow já disponibilizadas pelos controladores mais utilizados, tais como POX [75], NOX [67], RYU [47], entre outros.

endereço de origem e destino envolvido. Essas característica torna possível a implementação de novos módulos como os propostos nesta tese.

O ARES é composto de três módulos, conforme ilustra a Figura 5.2:

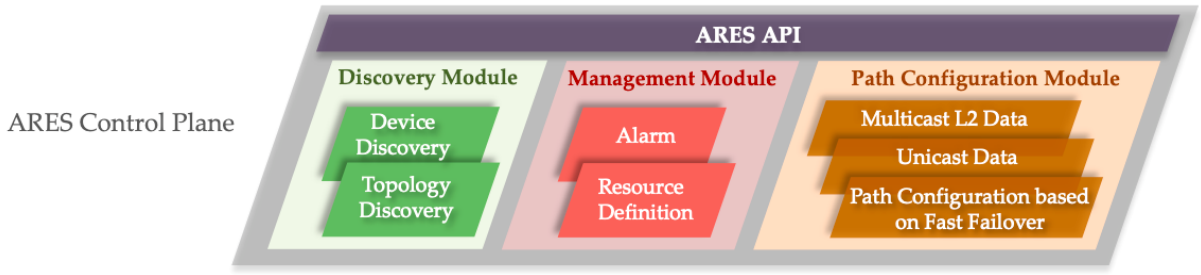


Figura 5.2: `ARES Control Plane` composto por 3 módulos: `Management, Discovery` e `Path Configuration`.

- `Discovery Module`: responsável pelo mapeamento e descoberta de elementos do sistema; detalhado na Seção 5.3.1;
- `Management Module`: O módulo é responsável por prover informações necessárias ao provisionamento e por monitorar os eventos de rede; detalhado na Seção 5.3.2;
- `Path Configuration Module`: responsável por toda a configuração da comunicação, incluindo métodos para recuperação de falhas, rotas *unicast* e árvores *multicast* de camada 2; detalhado na Seção 5.3.3.

5.3.1 `Discovery Module`

Este módulo é composto por dois componentes que são responsáveis por fazer o mapeamento de forma automática do `Energy Plane` e do `Data Plane`, desde que os dispositivos já tenham sido autenticados[¶]. Por mapeamento, entende-se que, quando os equipamentos forem ligados e tentarem se comunicar, poderão automaticamente ser mapeados pelo *ARES Control Plane*. Adicionalmente, podem reportar qualquer tipo de mudança na rede. Os componentes do módulo de descoberta são:

- `Topology Discovery`: Responsável por fazer a descoberta e mapeamento da topologia de rede. Este tipo de componente geralmente é nativo dos controladores SDN e é essencial para o funcionamento dos outros componentes do ARES. Após autenticados, os *switches* trocam informações com o controlador para estabelecer conexão. Nesse momento, o controlador já sabe quais *switches* existem, suas informações (como versão do *firmware* e modelo do *switch*) e que interfaces possuem. No entanto,

[¶]A forma de autenticação dos dispositivos pode variar de aplicação para aplicação, por isto o ARES não define um método de autenticação.

não sabe como estão conectados. Uma das formas para inferir os enlaces e consequentemente a conexão é executar algum protocolo para descoberta de vizinhança, como o *Link Layer Discovery Protocol* (LLDP) [26], também nativo na maioria dos controladores SDN.

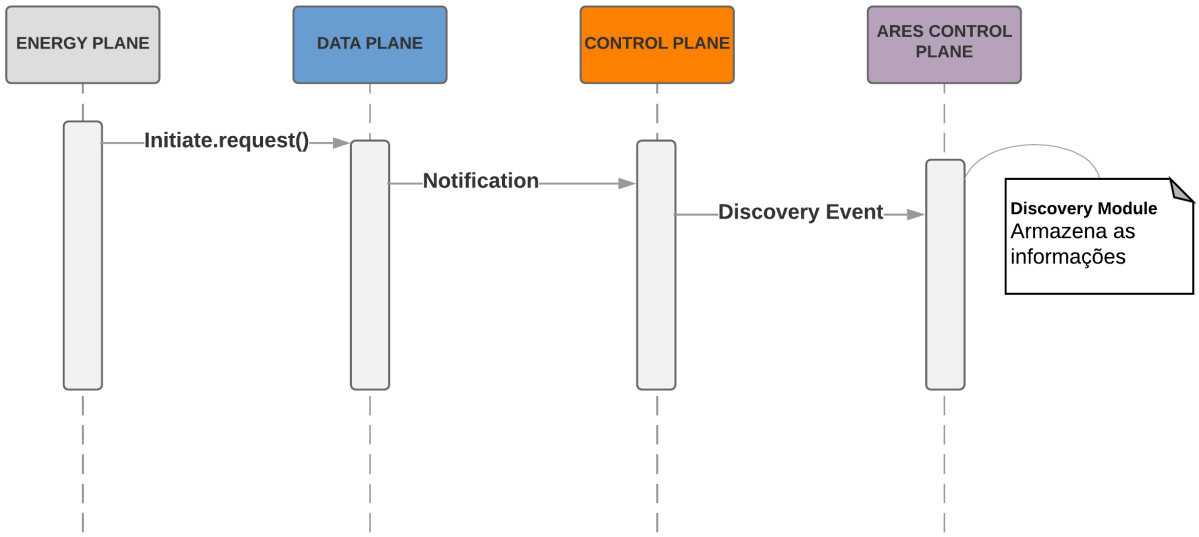


Figura 5.3: Diagrama de sequência do módulo `Device Discovery ARES`. O dispositivo no plano de energia inicia o serviço `Initiate.Request` do MMS para ser registrado na rede.

- `Device Discovery`: Este componente é responsável por fazer o mapeamento automático dos dispositivos do `Energy Plane` conectados aos *switches* que não executam protocolos para descoberta de vizinhança, como o LLDP. Sejam esses dispositivos postos de cargas de VEs, medidores inteligentes, *microgrids*, ou qualquer outro equipamento com capacidade de comunicação [‖], ao serem ligados, eles passam à etapa de autenticação. Depois de autenticados, tentam estabelecer conexão com o supervisório usando o protocolo MMS. A primeira mensagem MMS é enviada e o primeiro equipamento de rede a receber essa mensagem ainda não tem nenhuma regra de encaminhamento configurada pelo controlador ARES. Isso faz com que o equipamento de rede envie uma mensagem para o controlador SDN. Com isso, os atributos do novo dispositivo, que estão descritos no cabeçalho do pacote, passam a ser conhecidos e armazenados pelo controlador. Entre os dados coletados no cabeçalho do pacote MMS, destacam-se o MAC e o *Internet Protocol* (IP). Os dados do novo dispositivo são armazenados, assim como a quais portas e equipamentos de rede ele está ligado. Esse processo está ilustrado na Figura 5.3. Cada vez que um equipamento é acrescentado ou retirado da rede, esse componente atualiza essa lista. O componente proposto monitora os eventos da rede e mantém a lista atualizada. Após essa captura, o `Device Discovery` utiliza o serviço de *self-description* do MMS para coletar as informações relativas a configuração dos equipamentos. Logo, todos

[‖]Caso esses equipamentos tenham um *switch* com capacidade de enviar LLDP, serão descobertos pelo módulo *Topology Discovery*.

os *datasets* IEC 61850 dos dispositivos são mapeados, e além das informações citadas, as características de cada fluxo (como prioridade, identificador, destino e tipo de fluxo) são coletadas.

5.3.2 `Management Module`

O módulo é composto de dois componentes:

- `Resource Definition`: O componente é responsável requerer informações necessárias ao provisionamento e prover essas informações ao *Path Configuration Module*. Dados os nós de origem e destino informados, ele informa os equipamentos de comunicação aos quais os *hosts* de origem e destino estão diretamente conectados. Cabe observar que o destino pode ser *multicast* ou *unicast*, o que significa que um ou mais equipamentos de rede de destino podem ser informados. Além disso, para o provisionamento da qualidade de serviço, esse componente também retorna a prioridade necessária para a criação da comunicação entre origem e destino. Portanto, o componente utiliza:

  1. os parâmetros passados no provisionamento solicitado pelas aplicações de energia do SCADA-NG, onde as informações de tipo de mensagem, prioridade, origem e destino são passadas;
  2. os dados do `Discovery Module`, inclusive as informações de configuração (*datasets* IEC 61850).

  É importante ressaltar que as características para provisionamento do enlace devem estar de acordo com a aplicação em questão. A ideia é que seja definida uma ou mais prioridades para garantia de QoS para definição da regra a ser configurada. A prioridade será definida com base no tipo de mensagem, ou ainda com a prioridade nativa do fluxo. Os detalhes do algoritmo deste componente são descritos na Seção 5.3.4.

- `Alarm`: O componente é responsável por monitorar os eventos da rede que venham a prejudicar serviços que já estejam provisionados. Além disso, o controlador também gerencia a vivacidade das conexões regularmente com verificações periódicas e com eventos de falha, caso estas ocorram. Estes eventos podem ser notificações de falha no enlace/*datapath*/interface, alterações em fluxos, como sobrecarga de enlace, comutação para caminho *backup*, dentre outros. Como será visto na Seção 5.4, os alarmes também são acessados pelo serviço `Event` da API ARES. Com isso, o operador do SCADA-NG tem uma visão unificada do sistema com a indicação de qual função do sistema elétrico foi afetada por uma falha ou qual serviço foi afetado, ou ainda poderá ficar indisponível devido a uma falha de comunicação. Suponha uma mensagem GOOSE, sendo esta um *trip* (tipo 1A), enviada do IED A para o

IED B como prioridade 4 relacionada à função de proteção da linha de transmissão. O retorno de uma falha em um enlace que prejudique a função de proteção de linha de transmissão seria conforme a Tabela 5.3. Ressalta-se que este componente notifica os eventos de rede que ocorrem com funções/serviços que já estão em funcionamento e, para tanto, já tiveram seus objetos criados no SCADA-NG para provisionamento do enlace.

Tabela 5.3: Exemplo de retorno de falha no enlace que afeta a função de proteção de linha

Objeto IED3GOOSE1	
Atributo	**Valor**
source	*MAC Address* de origem (exemplo: 00:22:19:fe:8a:90)
destination	*MAC Address Multicast* de destino (exemplo: 01:0C:CD:01:00:04)
type	Tipo da mensagem definida na norma IEC 61850 (exemplo: Tipo 1A)
prio	Prioridade definida no campo Prio da camada 2 (exemplo: 4)

5.3.3 `Path Configuration Module`

O módulo `Path Configuration` interage com os dois módulos anteriores e é composto de três componentes que são responsáveis por configurar os recursos de rede de forma eficiente. Os componentes são:

- `Path configuration based on Fast Failover`: O componente tem como objetivo instalar as regras de fluxos de dados, dando suporte à recuperação de falhas na rede. Essa recuperação de falhas, dentro da concepção proposta pelo ARES, deve ser transparente para os dispositivos finais. Para isso, o componente usa um conceito intitulado *fast failover* de forma que as opções de encaminhamento *backup* em caso de falha já fiquem configuradas no *switch* previamente para o fluxo com interesse em usar a rede de comunicação. Os caminhos primário e *backup* são configurados com uma prioridade. Como o *switch* executa o caminho ativo de maior prioridade primeiro, caso o caminho principal sofra uma falha, o *switch* imediatamente encaminhará o pacote para a saída descrita na próxima opção ativa (caminho *backup*). O componente, de forma geral, descobre um caminho principal e um caminho *backup* usando pelo menos uma porta de saída diferente para cada opção. Sempre que ocorre uma falha, o caminho de *backup* é automaticamente escolhido e, em seguida, o componente `Multicast L2 Data` ou o `Unicast Data`, dependendo das aplicações que usavam o enlace com falha, são chamados novamente para criação de um novo caminho de *backup*. Os detalhes desse processo são descritos na Seção 5.3.4.

- `Unicast Data`: O componente é responsável por calcular os caminhos *unicast* da comunicação, como por exemplo, os usados por mensagens MMS de supervisão e

controle. Geralmente, os protocolos de controle e supervisão utilizados em redes elétricas inteligentes utilizam endereços *unicast* [86] para estabelecer conexão com os controladores dos dispositivos e concentradores/*gateways*. Ressalta-se que outros protocolos, como o SV, podem ter uma opção para uso de endereço *unicast*. Logo, o componente `Tráfego Unicast Data` é o responsável por definir o caminho para as aplicações de energia que utilizem endereçamento *unicast*. Dessa forma, o componente é capaz de achar o caminho mais curto entre origem e destino quando chamado pelo componente `Path configuration based on Fast Failover`.

- `Multicast L2 Data`: Este componente calcula as árvores de cobertura para os grupos *multicast* de camada dois, necessários para a comunicação horizontal, como por exemplo mensagens de proteção usando GOOSE e SV. O componente utiliza como entrada os *Datapath* de origem e destino passados pelo componente *Resource Definition*, assim como a visão unificada da rede. Com isso o componente calcula as árvores *multicast* para cada grupo na rede de forma a viabilizar a configuração da árvore.

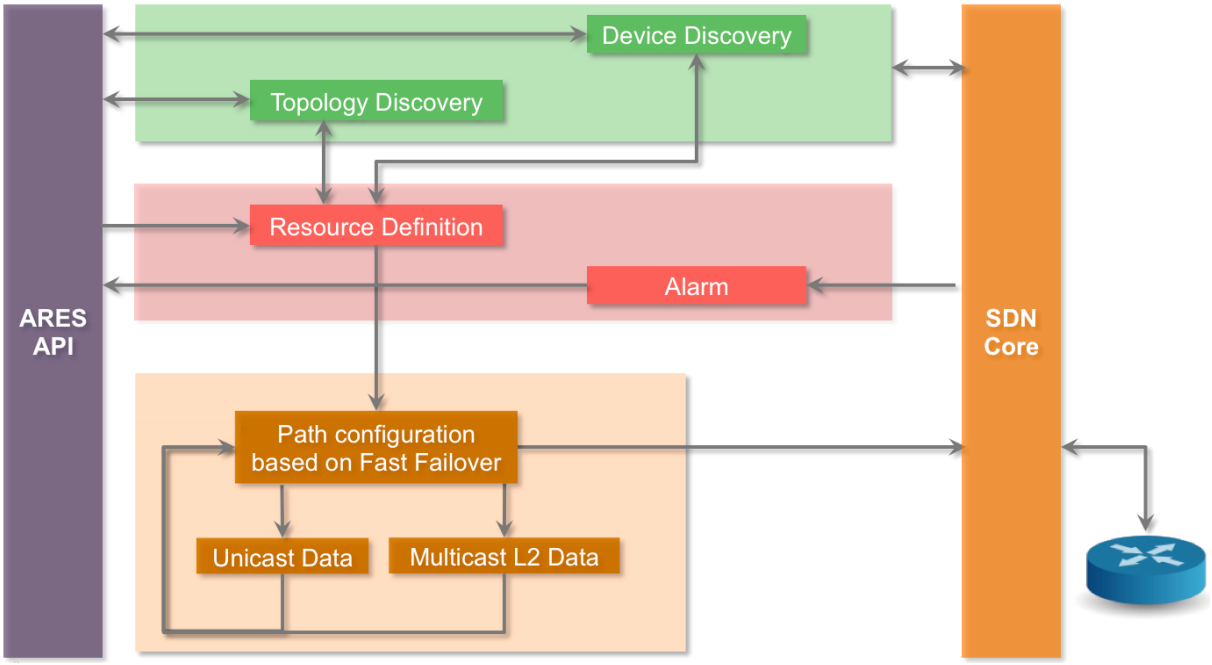


Figura 5.4: Fluxo mostrando a interação entre os módulos ARES.

A interação entre os três módulos ARES e os componentes descritos é ilustrada na Figura 5.4.

As configurações de caminho são realizadas de forma proativa após a primeira mensagem MMS enviada pelo dispositivo. Isto é especialmente importante para mensagens GOOSE e SV que trabalham com endereçamento de destino *multicast* de camada dois e possuem alta sensibilidade a atrasos. Com isso, a configuração proativa impede que a entrega das mensagens seja atrasada pela consulta reativa ao controlador. Desta forma, tem-se

uma rede que realiza o cálculo antecipado de árvores *multicast*. Como consequência, os quadros de enlace são apenas transmitidos ao grupo de interesse, por uma árvore *multicast* bem definida, evitando que o tráfego seja enviado para toda a rede desnecessariamente, evitando a sobrecarga na rede e nos dispositivos finais.

5.3.4 Algoritmos ARES

O módulo `Discovery`, que inclui os componentes `Device` e `Topology Discovery`, é capaz de retornar a visão completa da rede incluindo os dispositivos já autenticados do `Energy Plane`. Além disso, a classe *Path* do ARES retorna a origem, o destino, a prioridade e o tipo de mensagem que irá precisar de recurso (esta classe está descrita na Seção 5.4). Essas informações têm os valores recebidos pelos serviços MMS conforme o diagrama da Figura 5.5.

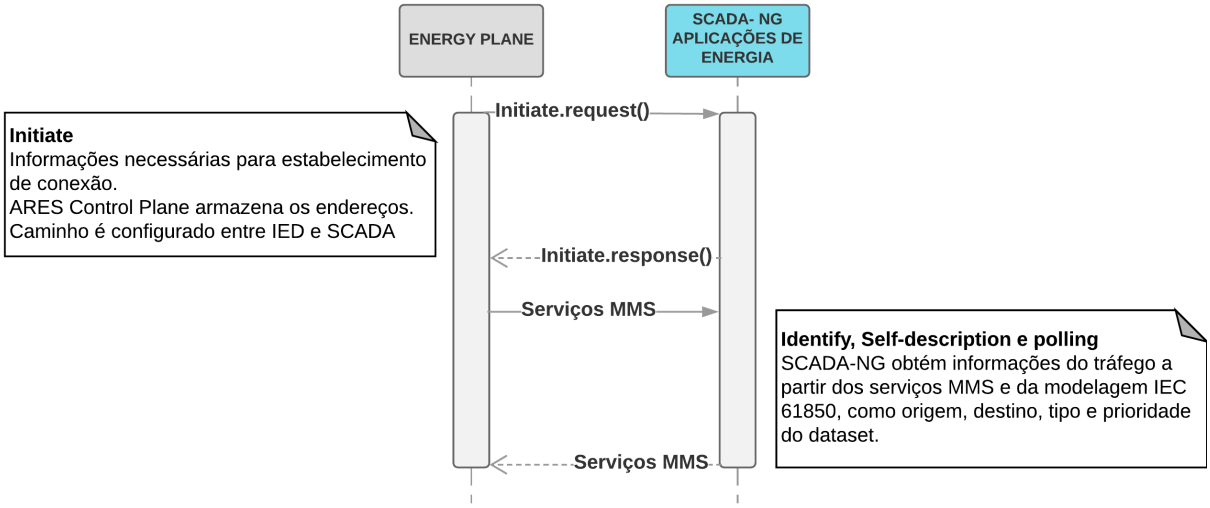


Figura 5.5: Fluxo mostrando a inicialização da comunicação entre o dispositivo IED e o SCADA-NG, que em seguida faz o mapeamento do IED com os serviços MMS.

Após estabelecida esta conexão, a aplicação de energia é capaz de ter os dispositivos mapeados através da API, que será detalhada na Seção 5.4. Através dos componentes Openflow, as informações relacionadas a rede são passadas. Através do protocolo MMS, as informações do tráfego que será enviado pelos dispositivos físicos (IEDs), e as informações destes próprios dispositivos são passadas.

Com isso, os enlaces podem ser provisionados de acordo com o tráfego que será requerido (*datasets* coletados através dos serviços MMS diretamente pelo módulo de descoberta) e/ou de acordo com a necessidade das aplicações de energia. Os componentes ARES envolvidos no provisionamento dos enlaces são o *Resource Definition* e todos os componentes do módulo *Path Configuration*. O componente *Resource Definition* é responsável por prover informações necessárias ao provisionamento. Para isso, conforme o Algoritmo 1, tem-se as seguintes entradas:

- os objetos da classe *Path* (definida na Tabela 5.7, na Seção 5.4), enviados para serem provisionados. Essa classe contém os atributos origem, destino, tipo e prioridade do fluxo a ser definido;
- saídas do `Módulo Discovery`: uma lista de todos os enlaces (E) e nós da rede (N), um dicionário mapeando todos os endereços MAC com as suas respectivas portas e *datapaths* conectados (*mac_map*)
- as informações dos *datasets* que precisam de fluxo configurado.

Algoritmo 1: Algoritmo do componente `Resource Definition`.

Input: $Path$, E, N, mac_map,$info\_dsets$
Output: dp_src,dp_dst,$prio$

```
1  dp_src = descobre_dp(mac_map, path.src)
2  for dst in path.dst do
3  |   dp_dst = descobre_dp(mac_map, path.dst, info_dsets)
4  |   dps.append(dp_dst)
5  |   dps_dst = remove_redundancias(dps)
6  end
7  for path.type in path do
8  |   prio = path.prio
9  |   if prio_nao_definida then
10 |   |   prio = define_prio(E, N, path.type, info_dsets)
11 |   end
12 end
13 return dp_src,dps_dst,prio,type
```

A função *descobre_dp*, na linha 1, com base no *map_mac* e no *path.src*, descobre qual o *switch* que está conectado no nó de origem da requisição de provisionamento. Para cada endereço de destino na lista de dispositivos de destino solicitados pela aplicação de energia, a função *descobre_dp*, na linha 3, também retorna o *switch* que está conectado ao endereço de destino. A lista *dps_dst*, na linha 5, contém os *switches* de destino, com as respectivas portas. Caso seja um caminho *unicast*, ele retorna um item.

Para cada tipo de mensagem com essa origem e destino, a prioridade é definida como sendo o valor do atributo prioridade da classe Path, linha 8. Caso a mensagem não tenha prioridade definida, a função *define_prio* retorna a prioridade para o tipo de mensagem em questão. A prioridade é retornada obedecendo os tipos de mensagem da norma IEC 61850, de acordo com a Tabela 3.2, e a aplicação de energia envolvida.

Com isso, este componente retorna os *datapaths* de origem (*dp_src*) e o(s) de destino (*dps_dst*) conectados nos dispositivos finais que possuem o endereço de origem e destino passado para provisionamento. O componente também retorna a prioridade daquele fluxo que deve ser usada para configurar o enlace. O tipo do fluxo (GOOSE, SV, MMS, mensagem de sincronismos, etc) também é retornado para fazer parte das regras configuradas.

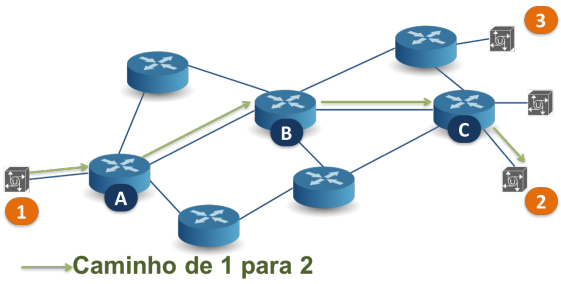
Algoritmo 2: Algoritmo do componente `Multicast L2 Data`.

Input: *dp_src*, *dps_dst*, E, N
Output: *arvore_multicast*
1 **for** *dp_dst* ***in*** *dps_dst* **do**
2 | $melhor\_caminho = calc\_unicast(dp\_src, N, E, dp\_dst)$
3 | $caminhos\_arvore.append(melhor\_caminho)$
4 **end**
5 $arvore\_multicast = remove\_redundancias(caminhos\_arvore)$
6 **return** *arvore_multicast*

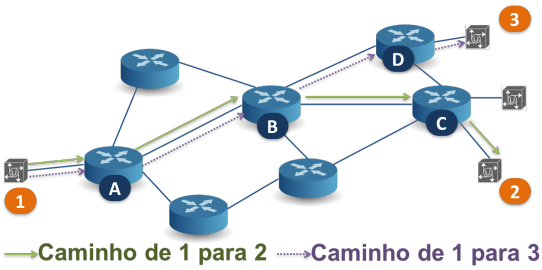
A descrição detalhada do componente `Árvore Multicast L2 Data` é dada no Algoritmo 2 e ilustrada na Figura 5.6. Os enlaces e nós da rede, o *dp_src* e a *dps_dst* são as entradas desse algoritmo. Suponha que o nó 1 precisa se comunicar com os nós 2 e 3 (Figura 5.6(c)). Neste cenário, o *dp_src* desta árvore é o *datapath* A e os de destino, D e C. Com essas informações, conforme linha 1, para cada destino do grupo, a função *calc_unicast* retorna o menor caminho da origem ao destino unicast. A lista *caminhos_arvore*, linha 3, guarda esses caminhos. Nas Figuras 5.6(a) 5.6(b), respectivamente, tem-se o caminho $A \rightarrow B \rightarrow C$ para chegar no *datapath* C e o caminho $A \rightarrow B \rightarrow D$ para chegar em D. Para que se calcule a árvore *multicast* a fim de evitar a configuração desnecessária de fluxos, a lista *caminhos_arvore* é processada para remoção de redundâncias com a função *remove_redundancias*, linha 5, que exclui qualquer caminho repetido na lista. No exemplo, a função retorna $A \rightarrow B \rightarrow (C, D)$, conforme 5.6(c). Assim, o componente retorna a *arvore_multicast* do grupo em questão.

Este componente é usado pelo componente `Path Configuration` para calcular os caminhos *multicast* da rede. A função *calc_caminho* será responsável por chamar esse componente ou o `Unicast Data`. Tanto o caminho *unicast* quanto o *multicast* são provisionados com a tentativa de um caminho *backup* e observando o *label* descrito pelo componente `Resource Definition`. Essas ações são efetuadas pelo componente `Path Configuration`, que faz o cálculo e configuração de caminhos *backup* para o fluxo seguir em caso de falha na rede de comunicação. Ressalta-se que o cálculo das árvores *multicast backup* que visam minimizar algum aspecto, como sobrecarga de sinalização do plano de controle, é um problema pelo menos *NP-hard* [71]. Logo, o algoritmo apresentado é uma solução para encontrar uma árvore principal e uma backup viáveis. A definição de uma árvore *backup* otimizada não é escopo desta tese.

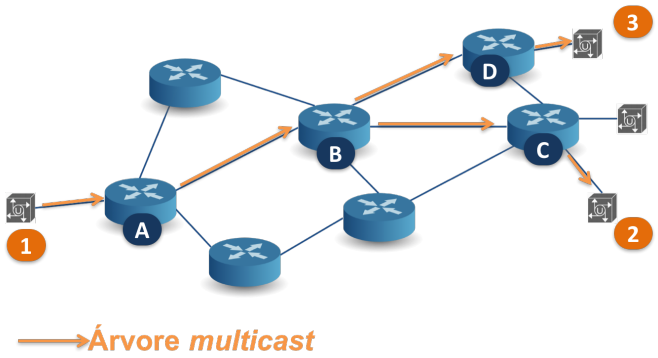
Como ilustrado na Figura 5.7, para cada possível falha na árvore *multicast*, o componente calcula os fluxos *backup*. Para isso, ele considera cada possível falha no caminho, retira os enlaces envolvidos e o próximo *datapath* e recalcula os caminhos. Por fim, tem-se as regras para cada *datapath* considerando cada falha e apenas os *datapaths* envolvidos na rota são configurados. O Algoritmo 3 recebe como entrada a lista de todos os enlaces (E) e nós da rede (N), o *switch* de origem no caminho (*dp_src*), o(s) de destino (*dps_dst*), e a



(a) Cálculo da rota mais curta do nó 1 até o 2



(b) Cálculo da rota mais curta do nó 1 até o 3

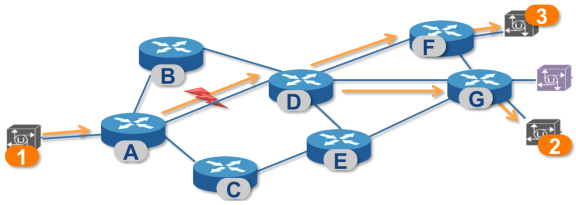


(c) A função *remove_redundancias* remove os enlaces repetidos.

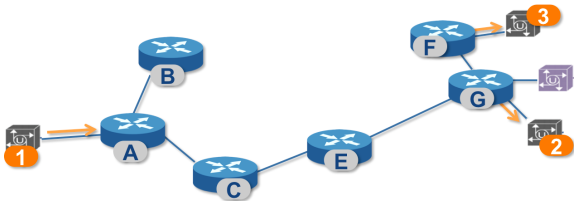
Figura 5.6: Cálculo da árvore *multicast* para o grupo composto pelos assinantes 2 e 3 e publicador 1.

prioridade que deve ser usada para a definição da QoS (*prio*). Ao final do procedimento, todas as regras de encaminhamento, incluindo os caminhos de recuperação de falhas, são inseridos nos *datapaths*.

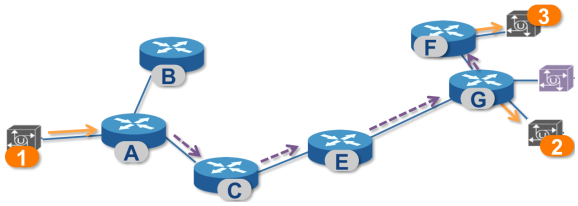
No Algoritmo 3, a função *calc_caminho*, na linha 1, calcula os fluxos dos *datapaths* do caminho utilizando os componentes `Unicast Data` e `Multicast L2 Data`. Em seguida, como descrito a partir da linha 2, para cada *datapath* no caminho principal, ele escolhe um fluxo. A função *remove_dp_E* remove a porta de saída escolhida na topologia (linha 3) e o próximo *datapath* no caminho, simulando uma falha que ocorra no enlace, porta ou *datapath* associado a essa porta de saída. Ele recalcula o caminho, caso ele exista, a partir daquele *datapath*, com a função *calc_caminho*, linha 4, conforme ilustrado na Figura 5.7(c). Se existir caminho, ele cria as regras necessárias naquele *datapath* com a *prio* solicitada pelo componente *Resource Definition*, tanto para o caminho principal como para o *backup*, linha 6. Conforme linha 8, ele retorna uma indicação de que o caminho pode ser provisionado com sucesso, `OK`, e as informações do *datapath* associado. Caso o caminho não exista, ele tenta o cálculo retirando apenas o enlace e mantendo o *datapath*, já que a falha pode ocorrer apenas na porta ou não no enlace, e não necessariamente no caminho. Se ele encontrar caminho (linha 13), salva as regras para essa opção e retorna



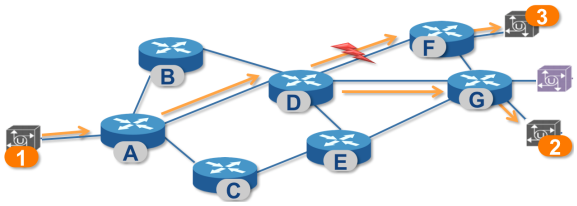
(a) Considera-se possível falha no enlace $A \rightarrow D$.



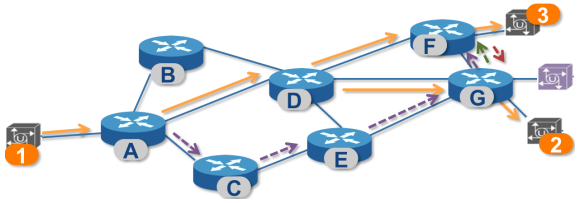
(b) Remove enlace e próximo *datapath* (se possível)



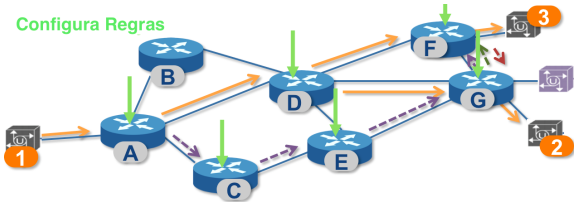
(c) Caminho *backup* é calculado passando saindo por C.



(d) Repete para cada enlace no caminho.



(e) Regras *backup* para cada possível falha no caminho.



(f) *Datapaths* envolvidos são configurados

Figura 5.7: Componente `Path Configuration based on Fast Failover`

um `WARNING` informando quais recursos não estão disponíveis e o *datapath* associado. Se não conseguir caminho ele retorna `NOT OK`, com as informações do erro (linha 19). Com isso, tem-se os fluxos criados para cada *datapath* e a função *remove_redundancias* trata as redundâncias removendo entradas ambíguas antes de configurar cada *datapath* no caminho (linha 23). O *status* do provisionamento é enviado para API ARES.

Uma consideração importante é que o componente calcula e instala as regras na tabela dos *datapaths* antes que o caminho principal falhe. A recuperação é rápida pois é feita de forma proativa. Quando o caminho principal falha, o caminho *backup* já está instalado. No entanto, no caso da árvore *multicast*, isso pode se tornar um problema, especialmente no caso em que a árvore de *backup* e a árvore primária têm enlaces de saída diferentes, como mostra a Figura 5.8, em "G". Em "G" caso o tráfego seja oriundo da árvore principal, linha cheia laranja, o enlace de saída é apenas para o destino "2". Caso o fluxo seja oriundo da árvore backup, linha tracejada roxa, tem-se mais de um enlace de saída, neste caso, tanto para "F" quanto para "2". Se o fluxo não puder ser diferenciado, independentemente de tráfego principal ou secundário, "G" vai encaminhar o fluxo para ambos os enlaces. Isto pode resultar em pacotes encaminhados erroneamente no *datapath* usando a árvore de *backup* antes de ocorrer uma falha ou ainda encaminhando pacotes incorretamente usando a árvore primária após a falha no enlace.

Algoritmo 3: Algoritmo do Componente `Path Configuration based on Fast Failover`.

Input: E,N, dp_src, dp_dst, $prio$
$caminho\_principal = calc\_caminho(E, N, dp\_src, dp\_dst)$
for dp ***in*** $caminho\_principal$ **do**
  $topo\_temp = remove\_dp\_E(E, N)$
  $caminho\_backup = calc\_caminho(dp\_src, topo\_temp, dp\_dst)$
  if $len(caminho\_backup) > 0$ **then**
    $regras[dp\_src] = cria\_regra(caminho\_backup, caminho\_principal, prio)$
    $arvore\_regra[dp\_src : dp\_dst] = regras[dp\_src]$
    return OK, dp
  end
  else
    $topo\_temp = remove\_E(E, N)$
    $caminho\_backup = calc\_caminho(dp\_src, topo\_temp, dp\_dst)$
    if $len(caminho\_backup) > 0$ **then**
      $regras[dp\_src] = cria\_regra(caminho\_backup, caminho\_principal, prio)$
      $arvore\_regra[dp\_src : dp\_dst] = regras[dp\_src]$
      return $WARNING$, dp
    end
    else
      return $NOT\ OK$, dp
    end
  end
end
$arvore\_regras = remove\_redundancias(arvore\_regra)$
$install\_regras(arvore\_regras)$

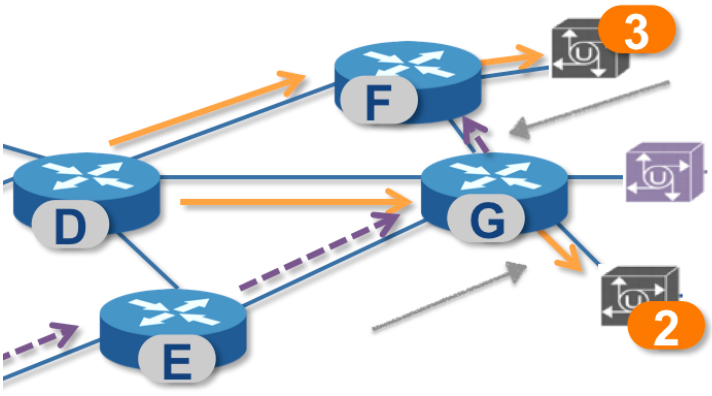


Figura 5.8: Árvore de *backup* e a árvore primária com enlaces de saída diferentes no *datapath* G

Para contornar esse problema, o componente `Path Configuration` atribui uma identificação (*tag*) no fluxo enviado para a árvore de *backup*. Dessa forma, o fluxo pode ser identificado como participante da árvore *backup* ou primária. A regra no *datapath*, correspondente à árvore primária, não usa a *tag*. A regra correspondente à árvore *backup*

utiliza a *tag*. A função *cria_regra*, linhas 7 e 15, é responsável por acrescentar essa *tag* no caminho backup calculado. A regra pode, por exemplo, mandar escrever o id da árvore backup no campo *dl_src* do pacote e usar esse mesmo campo para correspondência dos fluxos. Assim, o *datapath* encaminha os fluxos usando presença ou ausência da *tag*:

1. quando a árvore de *backup* for ativada, o fluxo tem a identificação *dl_src* indicando que esses pacotes devem ser disseminados pela árvore *backup* e não pela primária.
2. enquanto a árvore de *backup* permanecer sem uso, o fluxo não sofre marcação.

A regra é marcada com a "prioridade da regra" pela função *cria_regra*, linhas 7 e 14. A regra correspondente à árvore *backup* é prioritária. Isso faz com que o *datapath* primeiro confira se o pacote tem *tag*. Se ele encontrar, isso indica que o *datapath* encontrou uma correspondência na tabela e envia o pacote para a árvore *backup*. Se não tiver *tag*, ele não encontra correspondência e passa para a próxima regra na prioridade, que será a árvore principal.

5.4 API ARES

A API ARES oferece um conjunto de rotinas e padrões de programação para acesso à rede de comunicação das redes elétricas inteligentes através do uso de SDN. Com isso, torna-se possível realizar a comunicação entre as aplicações de energia do SCADA-NG com o controlador SDN em uso de forma a compartilhar suas rotinas, ferramentas, padrões e protocolos.

A intenção da API ARES é permitir que desenvolvedores das aplicações de energia possam criar seus produtos associados aos serviços prestados pela API ARES. Através da API, as aplicações de energia podem, por exemplo, se comunicar umas com as outras sem conhecimento ou intervenção dos operadores do SCADA-NG. Além disso, com os serviços prestados pela camada de controle do *framework ARES* o SCADA-NG poderá possuir aplicações de energia que, através do conhecimento da rede e possibilidade de interação em tempo real, são capazes de tomar decisões mais inteligentes.

Para exemplificar, suponha uma aplicação de energia para controle das GDs. Esta aplicação faz parte das aplicações de energia de nova geração. Sem o uso de um *framework* inteligente, as GDs apenas são ligadas e participam do sistema elétrico. Desta forma, os problemas oriundos dessa entrada só podem ser tratados posteriormente, quando ocorrerem, e não evitados. Uma aplicação de energia baseada no ARES pode decidir por essa liberação, de forma rápida e automática, ou ainda de forma mais lenta com o auxílio do operador do SCADA-NG, e tomar ações que possam impedir estes problemas antes da entrada desta GD. Igualmente importante a GD deverá ter seus recursos provisionados de forma correta. A Figura 5.9 ilustra de forma simplificada este pedido de provisionamento. A

ideia é proporcionar, de maneira ágil, a integração entre os sistemas supervisórios e os controladores SDN. Quando esta aplicação de energia executa um comando para liberar o funcionamento de determinada GD, uma mensagem MMS `Write` é enviada. No entanto, para que esta GD possa participar da rede de comunicação os seus recursos precisam estar configurados e de acordo com a QoS pedida pela aplicação de energia. Logo, antes do comando de liberação, é realizada uma chamada para a API ARES solicitando o provisionamento dos enlaces relacionados a esta comunicação. Desta forma, a conexão com o controlador é estabelecida e, através dos componentes ARES, os enlaces são provisionados.

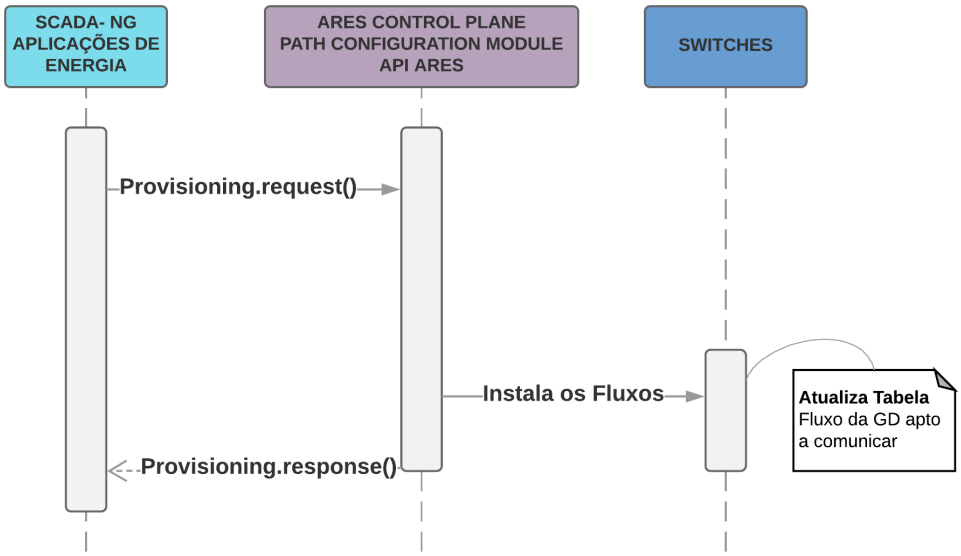


Figura 5.9: Serviço de provisionamento de enlaces da API ARES. Representação simplificada.

Outro ponto importante é que a API permite que funcionalidades específicas de uma aplicação de energia sejam utilizadas em outra sem que isso cause qualquer dificuldade. Imagine que a aplicação de energia de gerenciamento de veículos elétricos disponibilizou o mapeamento de todos os veículos com intenção de exportar energia para a rede elétrica. Essas informações podem ser utilizadas pelas aplicações de resposta à demanda para otimizar seus algoritmos para tarifação em determinado momento.

O detalhamento da API ARES e seus parâmetros são descritos a seguir. São definidos três serviços, que se relacionam com os módulos ARES conforme a Figura 5.10:

1. `Discovery`: para mapeamento da rede. Se relaciona com os componentes do Módulo `Discovery`;

2. `Provisioning`: para provisionamento de recursos. Se relaciona com o módulo de gerenciamento para requisitar o provisionamento do enlace e com o módulo de configuração para receber as respostas sobre a solicitação feita;

3. `Event`: para gerenciamento dos eventos de comunicação que ocorrem na rede. Se relaciona com o módulo de gerenciamento quando ocorrer eventos na rede de comu-

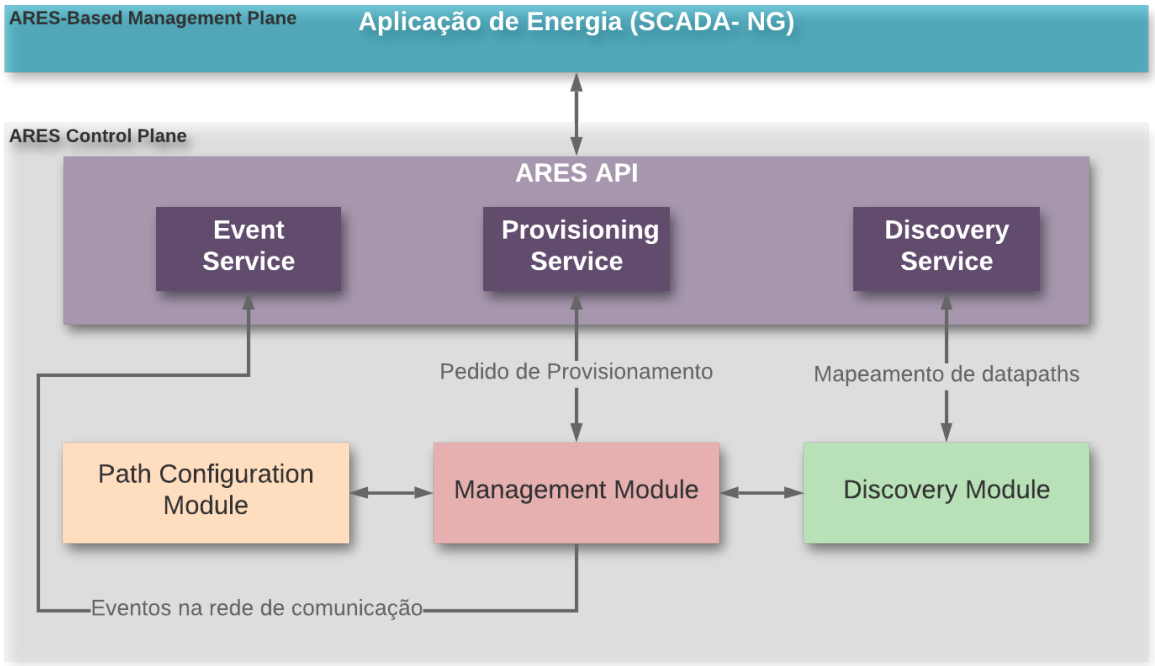


Figura 5.10: Relação dos serviços da API ARES com os módulos ARES.

nicação. Ressalta-se que, quando um novo caminho *backup* for reconfigurado após uma falha, essa informação é atualizada pelo serviço de provisionamento.

5.4.1 Serviço *Discovery* da API ARES

O serviço de mapeamento da API ARES é intitulado `Discovery`. Utilizando este serviço, as aplicações de energia podem, por exemplo, mapear todos os dispositivos da rede no supervisório de forma automática, deixando esta visualização disponível para o operador. Com o auxílio das informações da modelagem, como por exemplo localização do dispositivo (latitude, altitude, etc), modelo do dispositivo, endereços de rede, etc, os dispositivos podem ser alocados em um mapa mostrando, além da sua localização, suas informações.

Para tanto, a API ARES possui o serviço *Discovery* que fornece como retorno uma lista de objetos da classe *Datapath* do ARES, descrita na Tabela 5.4. Nesta tese, considera-se que cada dispositivo da rede é um objeto da classe *Datapath*, seja este um IED ou um *switch*. Assim todos os elementos da rede, sejam dispositivos SDN ou não, são mapeados na classe *Datapath*. O *framework* ARES foi modelado tanto para ser transparente para os dispositivos finais, quanto para considerar que estes dispositivos também fazem parte da estrutura SDN da rede, no caso do IED conter um switch SDN internamente**.

O diagrama de classes, ilustrado na Figura 5.11, descreve esta classe e suas interações

**Observe que um IED que tem a opção de comunicar em um anel de IEDs, ou ainda possui duas portas para *failover*, possui um *switch* interno. Este *switch* interno pode ser um *Datapath* SDN.

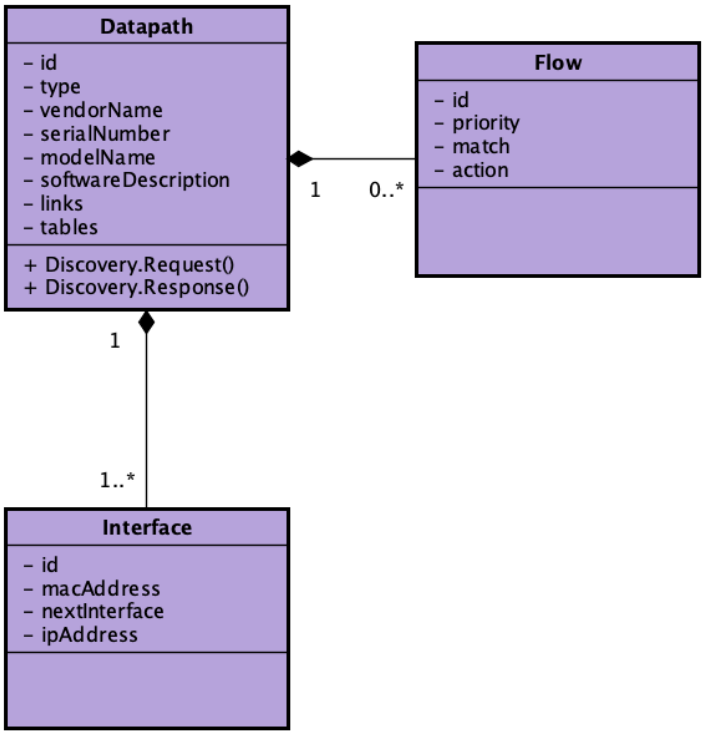


Figura 5.11: Diagrama de Classes da API ARES. Serviço `Discovery`

com outras classes da API ARES. Cada *Datapath* tem, no mínimo, uma interface de rede e pode ou não ter fluxos configurados. Um IED, por exemplo, é um objeto da classe *Datapath* que pode ter apenas uma interface (ou duas) e não contém fluxos configurados.

Tabela 5.4: Descrição da Classe *Datapath* do ARES

Classe Datapath		
Atributo	**Descrição**	**M/O**
id	ID do dispositivo	Opcional
type	tipo do dispositivo	Opcional
vendor name	Fornecedor do equipamento	Opcional
serial number	Número de série do equipamento	Opcional
model name	Descrição do *hardware*.	Opcional
software description	Descrição do *software*	Opcional
links	Lista de objetos da Classe *Interface* (Tabela 5.5)	Mandatório
tables	Lista de objetos da Classe *Flow* (Tabela 5.6)	Opcional

A Tabela 5.4 descreve a classe *Datapath*. O atributo `id` identifica o dispositivo. A definição do tipo de *datapath* é feita no atributo `type`, que pode ser desde "tipo veículo elétrico até tipo "*switch*, por exemplo. Essa representação é relacionada a aplicação de energia que estiver em uso. O nome do fornecedor do equipamento é descrito pelo atributo `vendor name` e seu número de série pelo atributo `serial number`. O atributo `model name` é relacionado a descrição mais especifica de hardware do equipamento, como o seu modelo e o `software description` a descrição mais específica do software, como por exemplo

versao do *firmware*. Para *switches* SDN os atributos poderiam, por exemplo, assumir os seguintes valores:

1. `id`: “1”;
2. `type`: “switch SDN”;
3. `vendor name`: “Nicira”[††];
4. `serial number`: “None”;
5. `model name`: “Open vSwitch”;
6. `software description`: “2.3.90”.

Para IEDs:

1. `id`: ”001”;
2. `type`: “IED”;
3. `vendor name`: “*Schweitzer Engineering Laboratories* (SEL)”[‡‡];
4. `serial number`: “2008285094”;
5. `model name`: “SEL-751A”;
6. `software description`: “R419”.

Além desses atributos, a classe *Datapath* contém o atributo `links` e o `tables`. O primeiro é composto por uma lista de objetos da classe *Interface*, conforme Tabela 5.5, e descreve cada interface dos equipamentos. O segundo por uma lista dos objetos da classe *Flow* que contém as regras dos fluxos.

Tabela 5.5: Descrição da Classe *Interface* do ARES

Classe *Interfaces*		
Atributo	**Descrição**	**M/O**
id	Descrição/nome da interface	Opcional
mac address	Endereço MAC Address da interface	Mandatório
next interface	Interface Próximo Salto	Opcional
ip address	Endereço IP da interface	Opcional

Na classe *Interface*, cada objeto tem um identificador, seus endereços IP e MAC e um próximo salto. Esse último indica qual é o próximo *datapath* que ele está conectado e em

[††]Nicira é uma empresa focada em SDN e virtualização de rede.
[‡‡]A SEL é uma empresa focada em equipamentos para o setor elétrico.

que interface desse próximo salto. Com essa informação, pode-se mapear os *links* da rede e as características da conexão entre eles. Logo tem-se a visão unificada da topologia da rede.

Tabela 5.6: Descrição da Classe *Flow* do ARES

Classe *Flow*		
Atributo	**Descrição**	**M/O/C**
id	Identificador	Mandatório
match	Campos usados para correspondência do fluxo	Mandatório
priority	prioridade da regra	Mandatório
action	Conjunto de instruções que o fluxo contém	Mandatório

Além desta visão, a API também permite que as tabelas contendo as regras dos *switches* sejam consultadas. Para isso, é definida a classe *Flow*, conforme a Tabela 5.6, onde o fluxo possui um identificador e suas características. De forma geral, as características envolvem uma regra (`match`), a prioridade daquela regra (`priority`) e a ação correspondente (`action`).

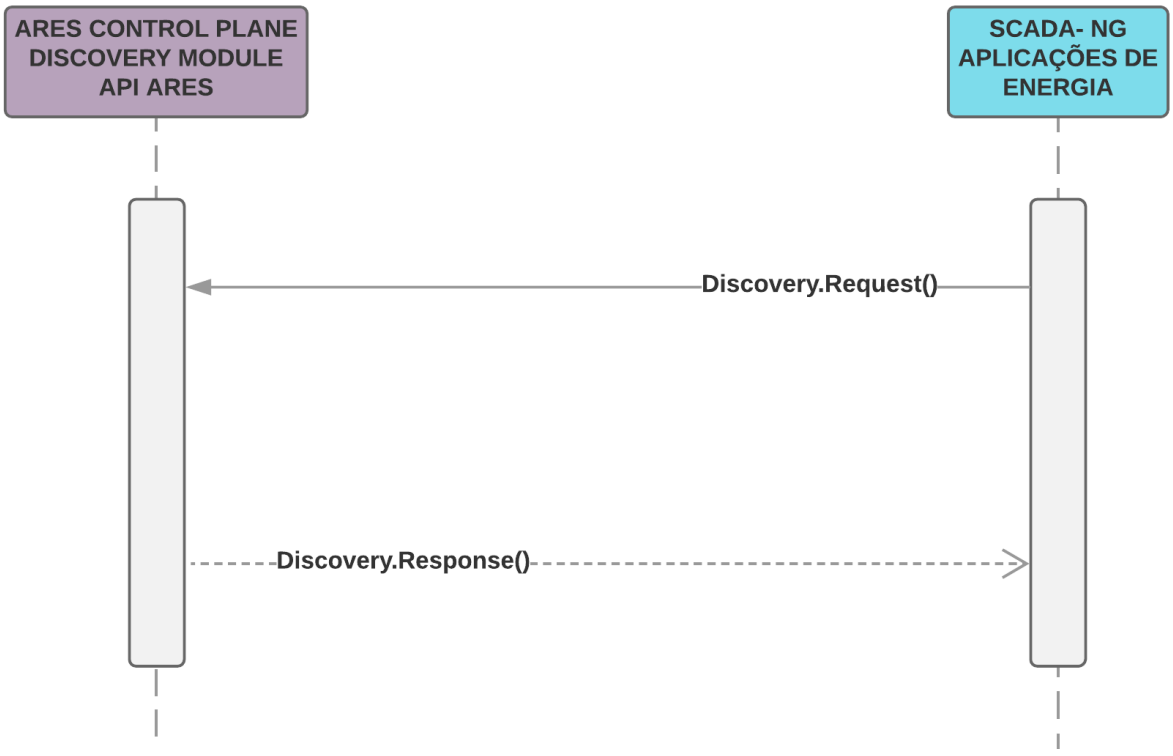


Figura 5.12: Serviço de mapeamento da API ARES, *Discovery*.

Definidas essas classes, a Figura 5.12 ilustra o serviço *Discovery*. As aplicações de energia enviam uma requisição *Discovery.Request* para o controlador ARES de forma a obter as informações para mapeamento da rede de comunicação. O `Discovery.Request()` requisita os objetos *Datapath* para o `ARES Control Plane`. Caso não sejam definidos os parâmetros, a resposta contém todos os objetos da classe *Datapath*. É importante ressaltar

que os parâmetros de entrada da Discovery.Request são opcionais. Assim, a requisição pode ser feita sem parâmetros, retornando todas as informações de topologia disponíveis, ou ainda, com algum parâmetro, especificando quais informações são necessárias, por exemplo, apenas o conjunto de *links*, os vizinhos de um nó, as informações de um único *Datapath*, etc. Os componentes do `ARES Control Plane` são responsáveis por manter, em tempo real, as informações dos dispositivos e da topologia da rede. Com isso, pode-se inferir a topologia disponível desde o núcleo até os IEDs do plano de energia.

5.4.2 Serviço *Provisioning* da API ARES

O segundo serviço da API ARES é relacionado ao provisionamento dos enlaces de comunicação. Como anteriormente descrito, as aplicações de energia podem solicitar o provisionamento dos enlaces de acordo com a QoS exigida pela aplicação. Nesse sentido, o serviço `Provisioning` é responsável por realizar a configuração dos recursos da rede. Para isso, a aplicação de energia precisa realizar a requisição de provisionamento passando como parâmetros os objetos da classe *Path*, conforme a Tabela 5.7.

Tabela 5.7: Descrição da Classe *Path* da API ARES

Classe *Path*		
Atributo	**Descrição**	**M/O**
id	identificador do caminho	Opcional
source	nó de origem na comunicação	Mandatório
destination	nó(s) de destino na comunicação	Mandatório
type	lista de tipos de mensagem definidos na norma IEC 61850 a serem trafegadas. Caso não definida na norma, o tipo pode ser representado pelo próprio protocolo	Mandatório.
prio	prioridade definida para o fluxo na configuração do equipamento	Opcional

Supondo a configuração de um caminho de “a” para “b”, os parâmetros do fluxo que vai trafegar nesse caminho são enviados na mensagem *Provisioning.request()*. O restante das ações são de responsabilidade dos módulos ARES descritos na Seção 5.3. São os componente ARES que se encarregam de decidir quais são os recursos necessários, caminhos possíveis e calcular as tabelas e fluxos que devem ser configurados em todos os dispositivos envolvidos no caminho de “a” até “b”, com prioridade “x” do tipo “y” . Com relação ao atributo `prio`, caso aquele fluxo de mensagens já tenha uma prioridade definida pelos equipamentos finais, essa pode ser requisitada. Caso contrário, pode-se usar o atributo `type`, para que essa prioridade seja definida de acordo com o tipo de mensagem definida na norma IEC 61850. Como detalhado na Seção 5.5.2, esses atributos são enviados e armazenados no estabelecimento de conexão (MMS) do plano de controle ARES ou do SCADA-NG com o dispositivo do *Energy Plane*. Ressalta-se que o destino pode incluir

mais de um dispositivo (no caso de *multicast* ou *broadcast*) e que o módulo ARES `Path Configuration` sempre tenta encontrar e configurar caminhos *backup*.

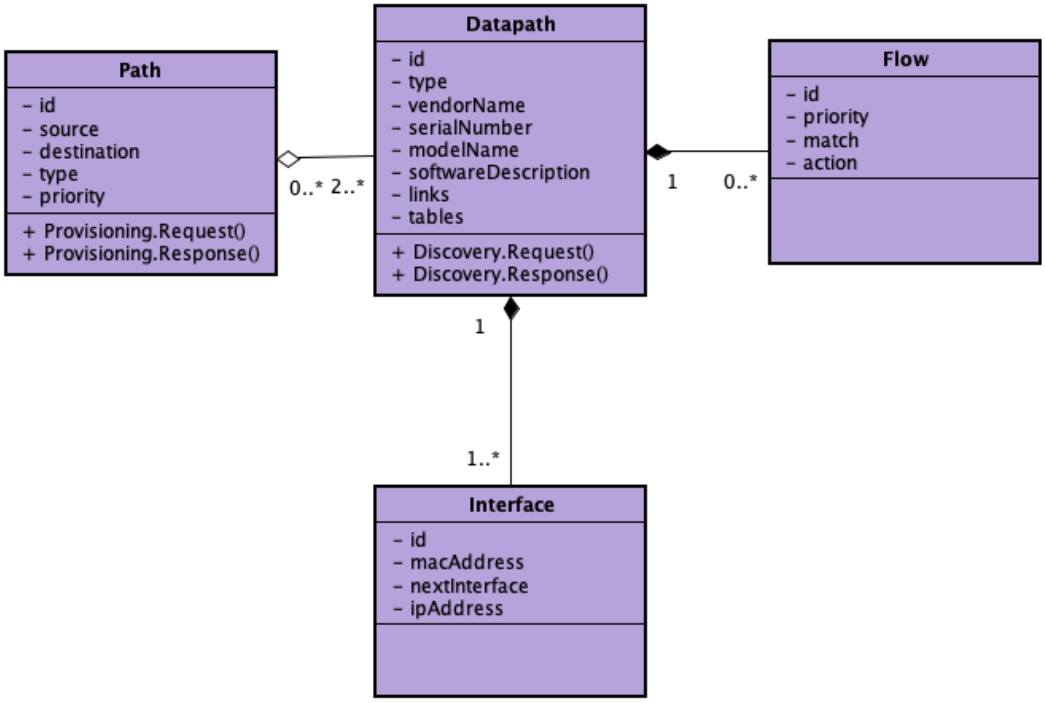


Figura 5.13: Diagrama de Classes da API ARES. Serviço `Provisioning`

O diagrama de classes, ilustrado na Figura 5.13, descreve a relação da classe *Path* com a classe *Datapath*. Para que um objeto da classe *Path* seja criado ao menos dois *Datapaths* têm que existir, origem e destino. Para destinos *broadcast* e *multicast* são possíveis vários *Datapaths*. Com essas informações o provisionamento do caminho pode ser solicitado. A Figura 5.14 ilustra essa solicitação.

A aplicação de energia baseada no ARES solicita um provisionamento com o serviço `Provisioning.Request()` e os parâmetros são definidos pela classe *Path*. O `ARES Control Plane` se encarrega do provisionamento. Em seguida, se necessário, o controlador instala os fluxos definidos pelo `ARES Control Plane`. Se todos os recursos conseguiram ser implementados com sucesso, o serviço retorna uma mensagem "OK" com os parâmetros da classe *Datapath*. Dessa forma, sabe-se exatamente o que foi provisionado, inclusive os caminhos *backup*. Caso o `ARES Control Plane` encontre apenas recursos escassos, mas ainda assim consiga provisionar o enlace, ele vai retornar um "warning", informando o que foi provisionado e motivo deste "warning", indicando onde o recurso está escasso.

5.4.3 Serviço *Event* da API ARES

O terceiro serviço da API ARES, diferentemente dos anteriores, é assíncrono. O serviço *Event* informa os eventos da rede de comunicação assim que estes ocorrem. Estes eventos

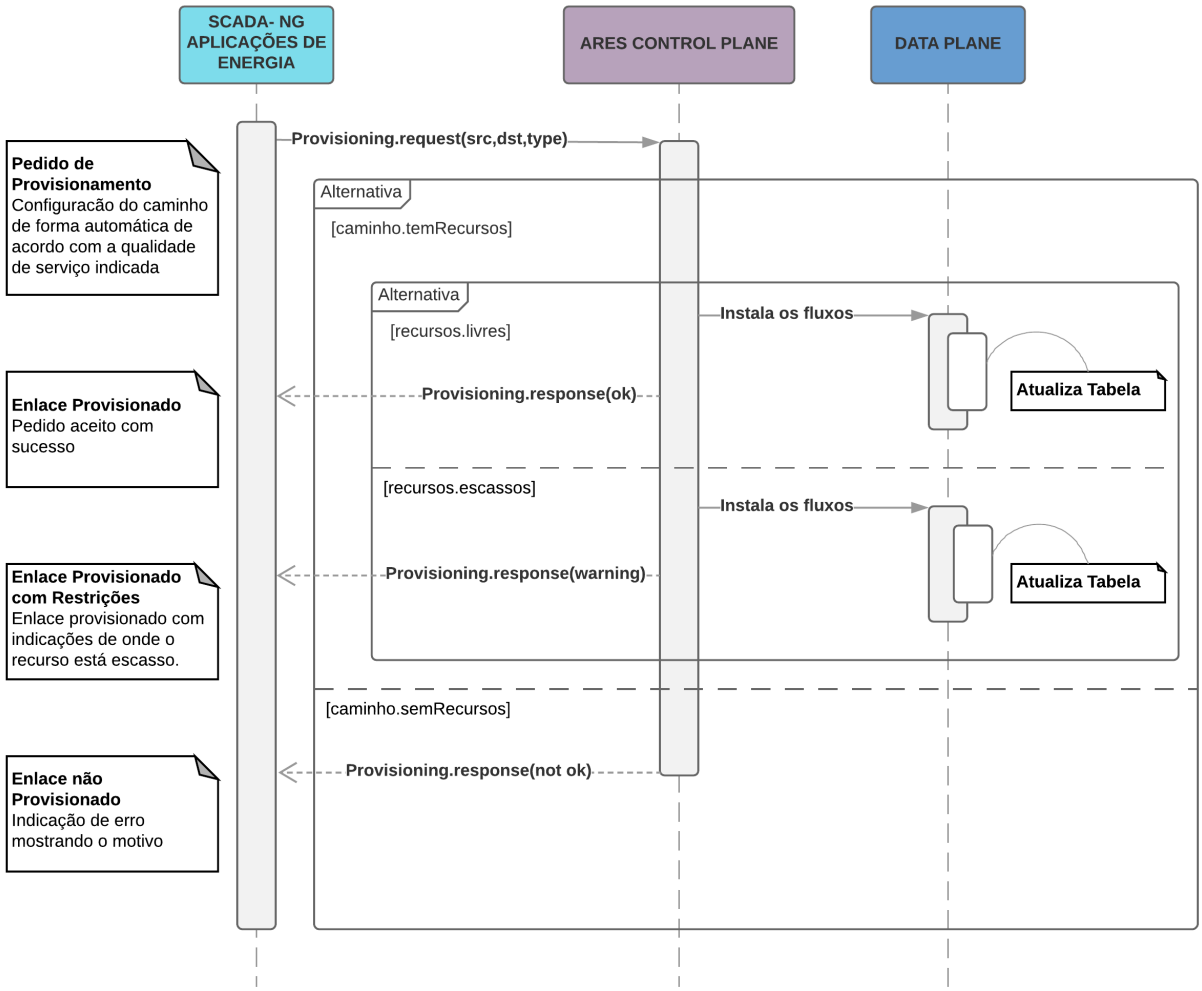


Figura 5.14: Provisionamento completo

podem ser:

1. notificações de falha em um enlace, ou *datapath* ou interface;
2. notificações de que os fluxos foram alterados. Quando por exemplo, um novo caminho é provisionado após uma falha, essa alteração nos fluxos também é notificada;
3. notificações de sobrecarga. Quando um fluxo começa a ser descartado por estar ultrapassando um limiar pré-estabelecido.

Com essas informações, além do gerenciamento da notificação a aplicação de energia consegue relacionar qual função/serviço do sistema elétrico foi afetado por aquele evento. Por exemplo, caso seja notificada uma sobrecarga no fluxo "1" do *datapath* "A", a aplicação de energia consegue relacionar qual função é afetada por esse fluxo e avisar que as mensagens estão sendo descartadas.

Suponha uma mensagem MMS sendo enviada do IED A para o supervisório. Exemplos de mensagens são as leituras de medidas analógicas, as leituras de variáveis digitais,

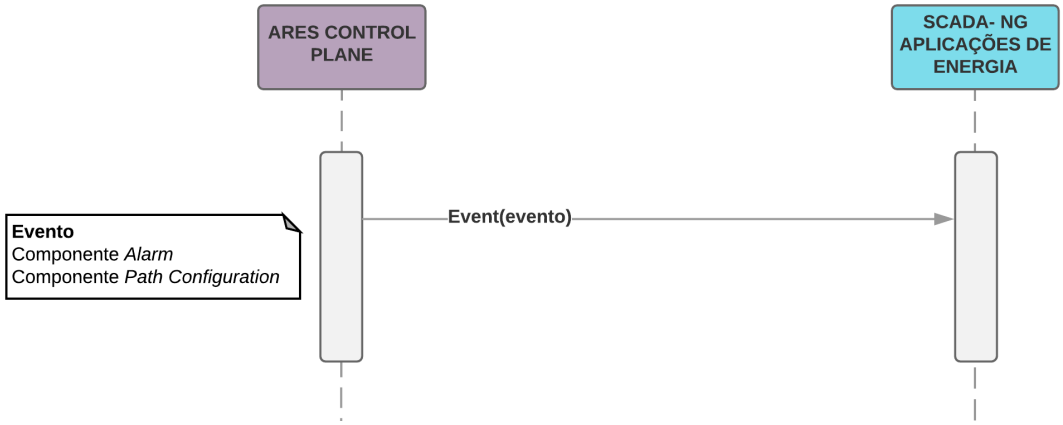


Figura 5.15: Serviço *Event* da API ARES

comandos para alteração de parâmetros. Esses atributos ou objetos podem estar agrupados em *datasets* MMS específicos, por possuírem prioridades diferentes por exemplo. Neste caso, os fluxos podem ter sido provisionados em caminhos diferentes. Logo, esses fluxos são independentes e podem estar sendo afetados de formas diferentes.

Caso este fluxo esteja sofrendo descarte por qualquer razão (ultrapassou determinado limiar de banda definido para o fluxo, sobrecarga na fila, etc) este evento é recebido pelo componente *Alarm* do módulo *management*. O serviço *Event* da API é acionado notificando sobre o evento, conforme ilustra a Figura 5.15. Com o auxílio do *framework* e da modelagem IEC 61850, que será apresentada na Seção 5.5.2, a aplicação de energia consegue inferir qual serviço está sendo afetado. Com isso, a API ARES, através do serviço *Event* informa a falha nesse fluxo e caso o fluxo seja pertencente à leitura de medidas analógicas, apenas esse serviço é marcado como afetado pela aplicação de energia.

Os parâmetros enviados pelo serviço são objetos da classe *Event*, conforme descrito na Tabela 5.8 e ilustrado no diagrama de classe da Figura 5.16. A classe *Event* possui o atributo `id`, que identifica o evento, e o atributo `status` que retorna qual tipo de evento ocorreu. O atributo `datapaths` é formado por um ou mais objetos da classe *Datapath*. O atributo `paths`, pode retornar nulo ou com a identificação que o evento ocorreu especificamente com um objeto da classe *Path*, que pode ocorrer, por exemplo, quando um fluxo é reprovisionado.

Tabela 5.8: Descrição da Classe *Event* da API ARES

Classe *Event*		
Atributo	**Descrição**	**M/O**
id	Identificador do evento	Opcional
status	Falha |Alteração |Sobrecarga	Mandatório
datapath	lista de objetos da classe *datapath* afetados	Mandatório
paths	lista de objetos da classe *Path*	Opcional

Por fim, o diagrama de componentes conceitual do plano de controle do ARES é

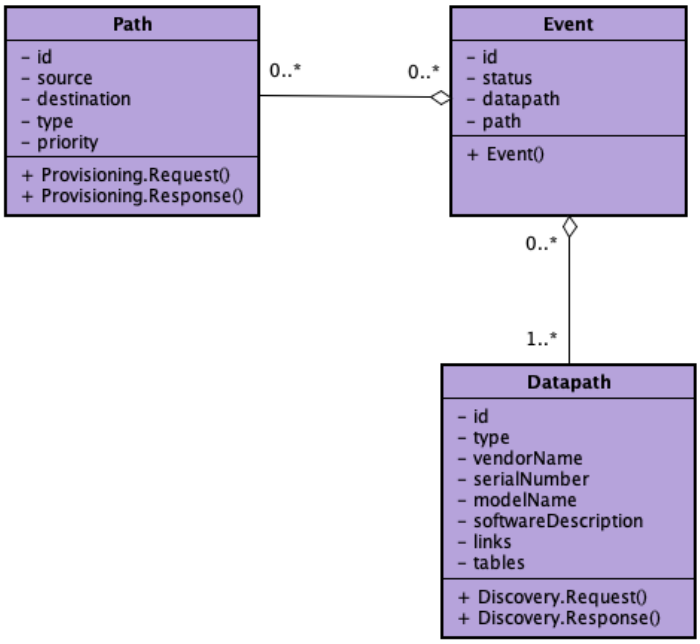


Figura 5.16: Diagrama de Classes da API ARES. Serviço `Event`

apresentado na Figura 5.17. O diagrama detalha os serviços da API ARES e a relação entre os componentes e módulos ARES.

Os componentes *Topology Discovery* e *Device Discovery* provêm as informações como topologia e fluxos configurados nos IEDs através do serviço *Discovery* da API. As informações dos *datasets* são requisitadas pelo componente *Device Discovery* através dos serviços MMS. Os módulos do *discovery* também provêm estas informações para o componente *Resouce Definition* que é responsável por definir quais recursos serão necessários na rede de comunicação com base na visão unificada da rede e na configuração presente nos IEDs.

O componente *Path Configuration*, é responsável por calcular os caminhos, com auxílio dos serviços prestados pelos componentes *Unicast* e *Multicast*. A requisição de cálculo de caminho é feita pelo componente *Resource Definition*. O serviço *Provisioning* é o responsável por fazer as solicitações dos provisionamentos oriundas da aplicação de energia para o componente *Resource Definition*. Ressalta-se que assim que o componente *Resource Definition* recebe um novo *dataset* (fluxo) do componente *Device Discovery* este também calcula os recursos e solicita o caminho sem interação com a API ARES.

Eventos na rede de comunicação, que podem ser de falha, alteração ou sobrecarga são reportados pelo componente *Alarm*, que provê essas informações para o serviço *Event* da API ARES. Da mesma forma, quando um evento ocorre, este componente prove essa informação para o componente *Resouce Definition* para que este analise a necessidade de reconfiguração de caminhos.

Um exemplo de diagrama de componentes de implementação ARES contendo plano de controle (*SDN core*) e plano de gerenciamento é apresentado no Apêndice A.

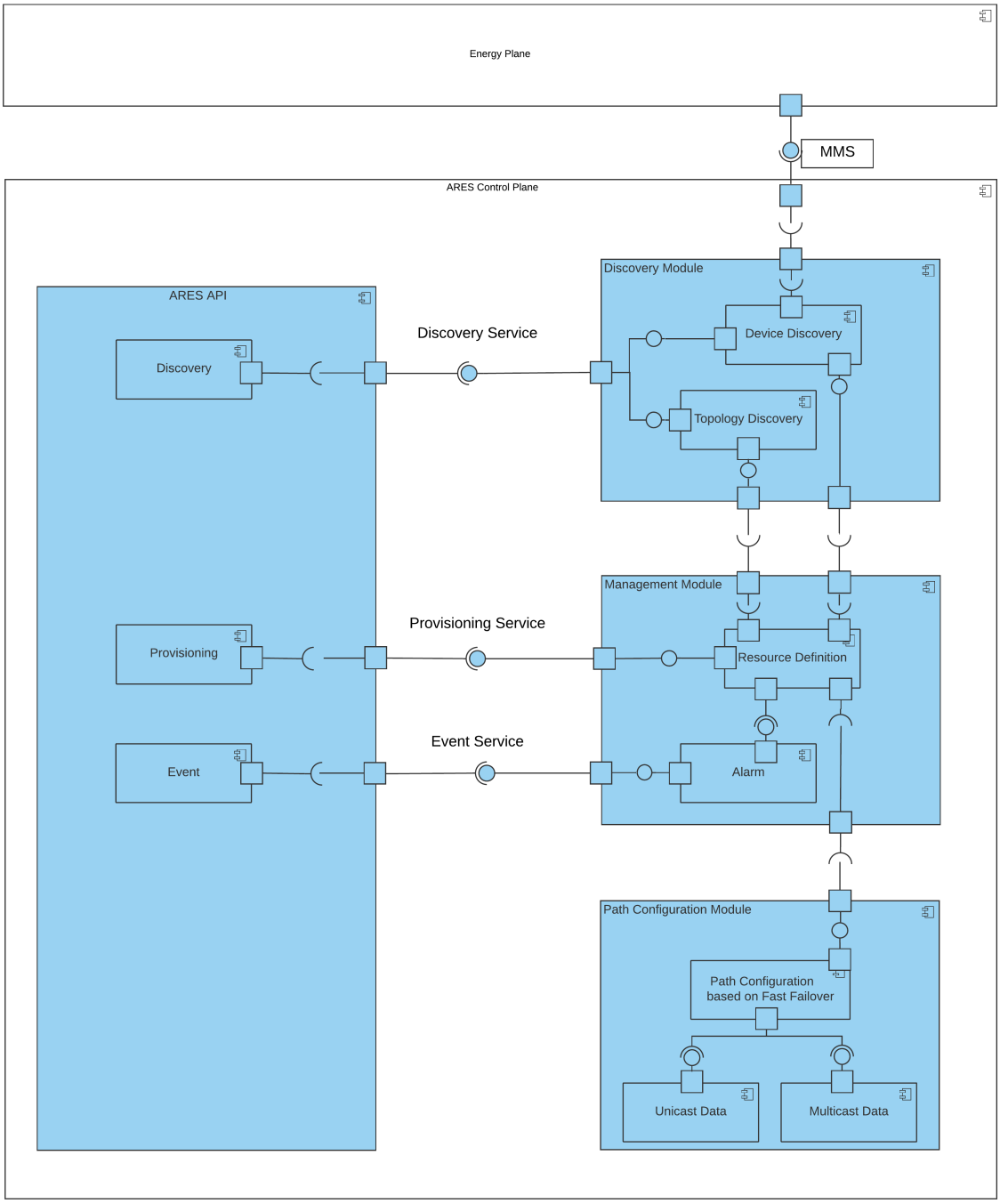


Figura 5.17: Relação dos serviços da API ARES com os componentes e módulos ARES.

5.5 Uso do ARES pelo SCADA-NG

Durante o desenvolvimento desta tese, algumas características foram levantadas para definição de um *framework* de comunicação com capacidade de interação em tempo real com a rede de comunicação. É desejável que:

1. o dispositivo do plano de energia possa solicitar, depois de autenticado, a entrada na rede de comunicação de forma automática. Alguns autores na literatura, como Etherden et al. [56] já citam que essa é a principal limitação do sistema SCADA atual. Os autores comentam que o ideal seria que o sistema fosse dinâmico para permitir que um DER se registre em um SCADA específico com apenas o endereço IP deste SCADA.

2. IEDs possam mudar sua parametrização de acordo com o cenário. Entradas e saídas de dispositivos do plano de energia, como GDs, geram mudanças nas características observadas pelo sistema elétrico. A entrada de equipamentos, se reportada, pode permitir que a parametrização das lógicas de proteção dos IEDs sejam ajustadas com base na alteração do sistema.

3. alterações na característica do tráfego do equipamentos resultem em provisionamento da rede de comunicação de forma autonômica. Caso um equipamento mude sua funcionalidade, os mesmo apenas determinado fluxo de um equipamento, o tráfego gerado pode sofrer alterações, tanto com relação à QoS demandada, quanto à característica do tráfego, incluindo destinos da mensagem, forma de disseminação da mensagem, dentre outros.

4. no estabelecimento da comunicação, as informações necessárias para o provisionamento da rede de comunicação sejam coletadas da forma mais automática possível. Isso é devido à característica autonômica do *framework*, trazendo simplicidade para o operador do SCADA-NG e minimizando a possibilidade de erro humano para sua configuração.

Para o Item 1, dos protocolos SCADA atuais, o que mais se aproxima desta ideia é o MMS. Apesar dos serviços IEC 61850, mapeados sobre o MMS, não abordarem essa característica [86], a ISO 9506 [3], que descreve este protocolo, permite que esse tipo de implementação seja realizada. Segundo a ISO 9506, após a conexão (serviço `Initiate`), qualquer um dos nós pode assumir a condição de cliente ou servidor.

Para o Item 2, o protocolo MMS também possui um serviço, chamado `write`, capaz de comandar uma ação nos equipamentos. Com uso desse serviço, desde que a rede de comunicação já esteja pronta pra receber esse tráfego, a característica pode ser viabilizada.

Com relação ao Item 3, um serviço MMS chamado *Report* pode ser utilizado. Para tanto, a modelagem IEC 61850 e as considerações feitas na Seção 5.5.2 devem ser observadas.

A auto-descrição, Item 4, é realizada pelo serviço MMS `Get`, que busca os atributos dos dispositivos, sendo complementado pelo serviço `Read`, que lê o valor destes atributos.

Mesmo com a implementação dos serviços MMS, é necessário que o dispositivo tenha a informação a ser reportada ou coletada. Nesse sentido, a modelagem da norma IEC 61850 precisa ter uma extensão, viabilizando essa implementação. Ressalta-se que, como detalhado a seguir, existem opções na modelagem IEC 61850 que podem ser utilizadas na implementação do *framework* quando a modelagem estendida não estiver disponível.

As características relacionadas ao protocolo MMS são detalhadas na Seção 5.5.1 e a extensão proposta para a modelagem da norma IEC 61850, na Seção 5.5.2.

5.5.1 Proposta de uso do MMS com o ARES

Devido às suas características, principalmente aos serviços de identificação do dispositivo, da auto-descrição, dos *reports bufferizados* e a modelagem de dados padronizada pela norma IEC 61850, o protocolo de supervisão e controle proposto para ser usado pelo SCADA-NG é o MMS. A Seção 3.3 comparou esses protocolos e a Tabela 3.1 resumiu as características.

Apesar de ser o protocolo mais indicado para uso pelo SCADA-NG, algumas características devem ser observadas. A partir do estudo para implementação deste protocolo com o ARES, verificou-se que:

- assim como todos os outros protocolos SCADA, o MMS não tem criptografia nativa nem outras características para garantir segurança.
- o serviço de identificação já existente, ilustrado na Figura 3.4, não possui a identificação de funcionalidade do dispositivo, nem informações referentes ao tipo de mensagem trafegada, prioridade, dentre outros.
- a conexão com o supervisório é geralmente iniciada no SCADA. Apesar da ISO 9506 permitir outra relação, a norma IEC 61860 adota a ideia de cliente SCADA.

Com relação à falta de mecanismos de segurança, mesmo que nenhum outro protocolo SCADA implemente nativamente mecanismos de segurança, essa característica dificulta sua implementação em larga escala, inclusive em medidores inteligentes. Apesar de não ser escopo desta tese, a autora reconhece e destaca a vulnerabilidade que tanto o MMS quanto os outros protocolos SCADA sofrem. Nesse sentido, a norma IEC 62351 [46] e a a NERC CIP foram desenvolvidas para lidar com essa e outras questões, como mecanismos de autenticação em infraestruturas críticas. Essas iniciativas têm estudado formas de mitigar as vulnerabilidades encontradas nesses protocolos e estão sendo constantemente abordadas pelo setor. Logo, é pré-requisito para implementação do *framework* ARES que os padrões

sejam levados em consideração e que as características de segurança sejam observadas. O *framework* ARES considera que os dispositivos, antes de iniciar a comunicação com o SCADA-NG, estejam autenticados.

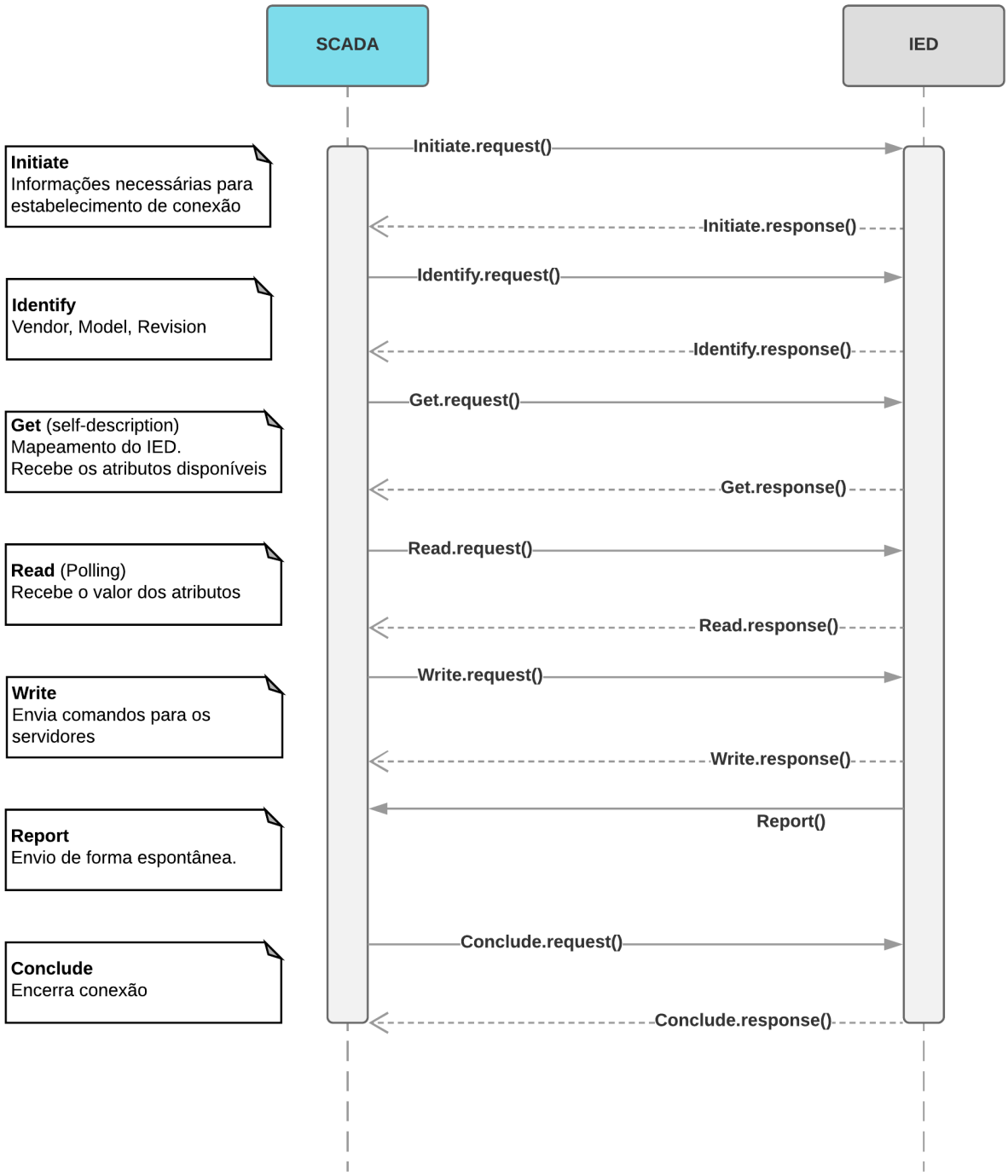


Figura 5.18: Diagrama de sequência de uma implementação tradicional do MMS.

Com relação ao serviço `Identify`, apesar de ser possível uma extensão no protocolo para que as informações fossem passadas como parâmetros deste serviço, nesta tese, optou-se pela extensão na modelagem IEC 61850. Já que, devido a outras características abordadas na Seção 5.5.2, a extensão é necessária, optou-se por manter compatibilidade

com os serviços já implementados pelo protocolo MMS.

Para enviar informações de um dado que sofreu alteração, assim que essa ação tenha ocorrido, é usado o serviço `Report`. Este serviço permite que uma característica do IED, como a mudança de funcionalidade, possa ser reportada para o SCADA assim que ocorra.

O fato da conexão ser iniciada sempre pelo supervisório exige que os dispositivos sejam previamente cadastrados no SCADA, que utiliza o serviço `Initiate` para iniciar a conexão e o `Conclude` para encerrar, como detalha o diagrama da Figura 5.18. Esse é um exemplo padrão de comunicação MMS. Ressalta-se que o serviço `identify` é opcional e que os demais serviços não têm uma ordem certa para ocorrer, são chamados de acordo com a necessidade do SCADA ou do IED.

Nesse tipo de implementação, o SCADA permanece como cliente durante todo o tempo de vida da associação, e os IEDs como servidores. Como a conexão é iniciada pelo SCADA, os dispositivos precisam ser previamente cadastrados no SCADA, o que vai de encontro à ideia de um SCADA autonômico com mapeamento automático de dispositivos.

É importante ressaltar que, segundo a ISO 9506, após a conexão ser estabelecida, cada nó pode assumir a condição de servidor ou cliente, independente de qual iniciou a conexão [2]. A ISO 9506 permite que o sistema real possa adotar a função de cliente ou servidor ou ambos durante o tempo de vida da associação [3]. Com isso, esta tese propõe que a conexão MMS seja iniciada pelo IED, mesmo que ele passe a maior parte da associação como servidor. O diagrama de sequência da Figura 5.19 ilustra essa característica.

Com a conexão iniciada pelo dispositivo (já autenticado) no sistema, tem-se um ambiente muito mais dinâmico e flexível, pois o estabelecimento da comunicação não precisa aguardar a configuração manual no SCADA tradicional para ser iniciada. Com o aperfeiçoamento deste protocolo e com a implementação completa do ARES, as aplicações de energia podem implementar novas possibilidades até então não exploradas.

Ressalta-se que, antes que o dispositivo possa efetuar o `Initiate` este já deve ter sido autenticado. E, da mesma forma, após o SCADA ter aceito a conexão está pode ser encerrada ou simplesmente continuar, de acordo com a implementação. O diagrama da Figura 5.19 ilustra, de forma mais completa, uma situação em que após o pedido de `Initiate` a comunicação continua com os demais serviços do MMS. Geralmente, essa é a sequência padrão, onde após a conexão, o SCADA solicita as informações de identificação, faz o processo de *self-description* e dá início ao *polling*. Em qualquer momento pode haver um comando, ou ainda um *report*. A sequência ilustrada é um exemplo, no entanto depende da implementação.

Exemplos de características que poderão ser implementadas:

- GDs e cargas poderão se associar as aplicações de energia com o serviço `Initiate`. Esse caso refere-se à primeira vez que o dispositivo participa do sistema.

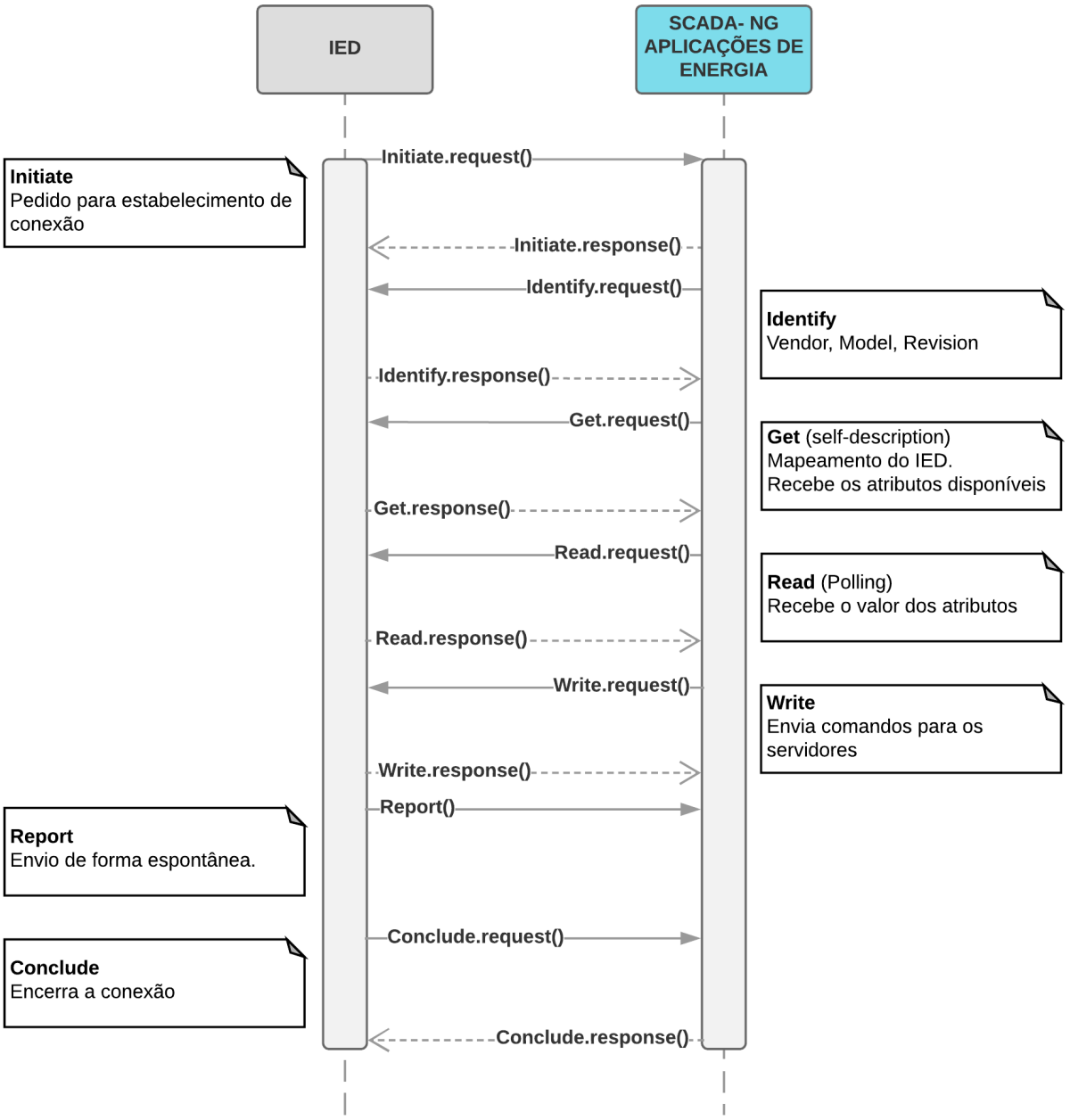


Figura 5.19: Diagrama de sequência da proposta para implementação do MMS com conexão iniciada pelo IED.

- Mudanças de funções serão reportadas para o SCADA com o serviço `Report`. O mesmo ocorre para qualquer alteração de informação/medição no IED.
- Comandos para alteração da parametrização do IED serão enviados com o serviço `Write`.
- O serviço *Identify, Get, Read* continuam com as suas características padrão, onde identificam o dispositivo, obtêm os atributos disponíveis, e em seguida os seus valores.

De forma geral, as aplicações de energia utilizam as informações enviadas por *Report*, ou solicitadas pelo `Read`, para monitorar e mapear o conteúdo dos dispositivos. No entanto,

apenas os serviços descritos não são suficientes para que as novas funcionalidade propostas para o SCADA-NG sejam viáveis. A extensão na modelagem da norma IEC 61850, conforme Seção 5.5.2, é necessária para permitir a viabilidade do *framework*. No entanto, opções podem ser utilizadas para manter compatibilidade com o modelo atual.

5.5.2 Modelagem IEC 61850 e o ARES

As informações principais que precisam estar modeladas pela norma IEC 61850 para o funcionamento do *framework* ARES são relacionadas às seguintes características:

1. a prioridade do dispositivo (carga/gerador): essa característica é relacionada à prioridade que o dispositivo do plano de energia tem em comparação com os outros. Exemplos de prioridades para cargas são hospitais com prioridade alta e residências com prioridades mais baixas. Postos de carga podem ser prioritários quando abastecendo uma ambulância, mas não prioritários se abastecendo um carro de passeio que já está com 80% da bateria carregada. Essa informação pode ser usada pela aplicação de energia para tomar determinadas ações no sistema, como liberar ou não para carga um veículo elétrico.
2. prioridade do fluxo de comunicação: usada para garantia de QoS necessária para a configuração da rede de comunicação.
3. tipo de mensagem IEC 61850 que o dispositivo vai trafegar: a norma IEC 61850 define 9 tipos de mensagem que podem estar relacionadas ao *trip*, amostragem de valores, sincronismo, comandos, etc (Tabela 3.2).
4. endereços de origem e destino do fluxo de comunicação.
5. status do fluxo: se o fluxo de comunicação (associado a um *dataset*) pré configurado está ativo ou não: com isso a API ARES pode saber se precisa configurar determinado fluxo ou não.

Na presença de DERs, além das características descritas acima tem-se:

1. função que aquele dispositivo exerce no sistema. Exemplos são os veículos elétricos, que ora estão suprindo a necessidade de demanda da residência, ora estão carregando e ora estão exportando energia. Generalizando, tem-se:
   - Carga: dispositivo está apenas consumindo energia;
   - Gerador: dispositivo está gerando energia e exportando pra rede;
   - Neutro: dispositivo não consome energia e não gera. Essa situação é comum quando a quantidade de energia gerada é consumida localmente sem a necessidade de uso da rede de distribuição de energia.

Nesta tese, propõem-se que os dispositivos do plano de energia (detalhado na Seção 5.2), sejam modelados como dispositivos físicos. Isso permite uma maior integração entre os dispositivos que compõem o sistema. Além disso, como a norma provê uma forma de mapear dispositivos não IEC 61850, a proposta pode ser utilizada mesmo que os dispositivos não utilizem o IEC 61850. Para tal, a norma provê formas de descrever um equipamento externo simplesmente tornando o dispositivo físico IEC 61850 um *gateway*. Com isso, tem-se um contêiner com as informações desse dispositivo externo. Detalhes sobre a composição destas classes e estruturas são descritas nas partes 7-1, 7-2 da norma [85, 81].

Os dispositivos físicos (*physical devices* nos IEDs) contêm os objetos criados com base nas classes IEC 61850. Logo, os atributos da IEC 61850 possuem os valores de interesse dos dispositivos do plano de energia. Esses valores vão desde uma medida analógica de corrente até a indicação de falha na abertura de um disjuntor que compõe o conteúdo das mensagens trafegadas. As informações de registro e algumas de configuração também são salvas nesses atributos. Como seria muito dispendioso montar um pacote para cada valor de envio, a norma considera que os atributos podem ser agregados em um conjunto de dados (*datasets*). O *dataset* contém os valores que compõem o *payload* da mensagem.

A norma define blocos de controle que se associam a esses datasets. Como qualquer característica da norma, os blocos e controle são definidos em classes, chamadas *Control Block*. Informações como endereço, prioridade, ou se aquele conjunto de dados configurado para envio está ou não habilitado, são atributos dessa classe de controle.

As classe dos blocos de controle são definidas na parte 7-2 [81] de acordo com a aplicação:

- GOOSE: a classe *GOOSE Control Block* (GoCB) é referente ao bloco de controle para a GOOSE;
- MMS: a classe *Buffered Report Control Block* (BRCB) é referente ao bloco de controle para *reports* buferizados e a *Unbuffered Report Control Block* (URCB) para *reports* não buferizados;
- SV: a classe *Multicast Sample Value Control Block* (MSVCB) é referente ao perfil *multicast* de comunicação SV e a *Unicast Sample Value Control Block* (USVCB) para o perfil *Unicast*.

A importância dos blocos de controle é relacionada ao fluxo de comunicação. As informações que forem referentes a determinado *dataset* são associadas a um bloco de controle e, consequentemente, a um fluxo de comunicação. Um conjunto de atributos GOOSE, por exemplo, tem o seu endereço de destino salvo no bloco de controle GOOSE. Logo, os atributos ARES, relacionados especificamente ao fluxo, devem ser definidos em blocos de controle.

A Tabela 5.9 descreve os novos atributos propostos neste trabalho para a norma IEC 61850, de forma a viabilizar as novas aplicações de energia descritas para o SCADA-NG. Na tabela, a primeira coluna indica o "atributo ARES". A coluna "item" relaciona cada atributo com as descrições das características discutidas acima. Um possível mapeamento desses atributos em atributos disponíveis na modelagem IEC 61850 atual é discutido na terceira coluna. A quarta coluna descreve um exemplo de que atributo utilizar para manter compatibilidade com os dispositivos atuais que já utilizem a norma. Os atributos `Priority`, `TypeDSet`, `MacAddress` e `FlowEna` são referentes ao fluxo, e portanto são definidos no bloco de controle. O atributo `PrioPhyDev` é relacionado ao dispositivo físico, e o `DER Function`, ao nó lógico que representa determinado recurso de geração distribuída (DER).

Tabela 5.9: Mapeamento dos Atributos ARES na modelagem IEC 61850

Atributo ARES	**Item**	**Mapeamento para Norma IEC 61850**	**Classe**	**Exemplo de uso mantendo compatibilidade com o modelo atual**
PrioPhyDev	1 - prioridade para os dispositivo	Não possui mapeamento direto. Pode ser usado um nó lógico genérico da norma	*Device Name Plate* (DPL) Class	GGIO.ISCSO.stVal
Priority	2 - prioridade para os fluxos	O atributo **PhyComAddr**, definido na na parte 7-2 [81] da norma, representa os campos da camada de enlace. Portanto pode assumir os valores do MAC *address* de origem e destino, além dos campos de **prioridade** e VLAN. Como esse tipo é utilizado nos blocos de controle GOOSE e SV, pode-se considerar o seu uso pelo *framework*. A prioridade definida é relacionada a cada fluxo GOOSE ou SV.	GoCB *Class* | BRCB *class* |URCB *Class* | MSVCB *Class*| USVCB	GSE.Address, type="VLAN-PRIORITY"

TypeDSet	3 - tipo de mensagem	Não possui mapeamento direto na norma. Como o tipo de mensagem precisaria ser definido por fluxo, este atributo precisaria estar em um bloco de controle. Devido a essa característica, não possui adaptação. Para contornar essa questão, o *framework* ARES utiliza apenas a prioridade definida no fluxo. Caso não esteja definida, o fluxo é tratado sem prioridade	GoCB *Class* | BRCB *class* |URCB *Class* | MSVCB *Class*| USVCB	GSE.Address, type="VLAN-PRIORITY"
IpAddress	4 - identificação dos endereços de rede	A Tabela 132 da Parte 8-1 da norma define o endereçamento para dispositivos que usem o perfil de aplicação (*Application Profile*). Logo, o endereço IP e máscara de rede do dispositivo é salvo no item **ConnectedAP** e pode ser utilizado para mapear o IP Nativo do dispositivo físico que pediu conexão no SCADA. Esse endereço é relacionado ao Dispositivo Físico.	BRCB *class* |URCB *Class*	ConnectedAP.Address, type="IP"

MacAddress	4 - identificação dos endereços de rede	O atributo **PhyComAddr**, definido na na parte 7-2 [81] da norma, representa os campos da camada de enlace. Portanto pode assumir os valores do **MAC *address*** de origem e destino, além dos campos de prioridade e VLAN. Como esse tipo é utilizado nos blocos de controle GOOSE e SV, pode-se considerar o seu uso pelo *framework*. Este endereço é relacionado a cada fluxo GOOSE ou SV.	GoCB *Class* | MSVCB *Class* | USVCB *Class*	GSE.Address, type="MAC-Address"
FlowEna	5 - status do fluxo	Os blocos de controle da norma, tanto GOOSE, como SV como MMS tem um atributo que indica que aquele DataSet está ativo para funcionamento ou não [81]. A classe GoCB é referente ao bloco de controle para a GOOSE, a BRCB para *report* MMS buferizado, a URCB para *report* MMS não buferizado, a MSVC para o perfil *multicast* de comunicação SV e o USVCB para o perfil *Unicast* da SV.	GoCB, BRCB, URCB, MSVCB, USVCB [81]	BRCB.RptEna

DerFunction	1–DER	O modelo genérico de dados para descrever as características elétricas de qualquer unidade ou sistema DER independente do seu tipo são descritas na parte 7-420 da norma [80]. Exemplo de classe que pode ser usada, é a *DER controller status* (DRCS) que é a classe de controle do estado da DER. Essa classe possui o atributo modOnAval para indicar que a DER está ligada e disponível para conexão, o modOffUnav para indicar que a DER está ligada porém indisponível para conexão e o modOnUnav para DER desligada e indisponível para conexão.	DRCS Class [80]	DRCS.modOnAval | DRCS.modOffUnav | DRCS.modOnUnav

Os dois atributos que não possuem mapeamento direto para a modelagem da norma são o *PrioPhyDev* e o *TypeDSet*. Como descrito na Tabela 5.9, os dispositivos sem a extensão da modelagem podem utilizar o *framework* com o exemplo descrito. No entanto, para uma solução mais completa, propõe-se que os dois atributos sejam incorporados à norma.

O nó lógico da norma, relacionado as características dos dispositivos físicos, é o *Physical Device Information* (LPHD). A classe LPHD, possui a identificação do dispositivo físico no atributo `PhyNam`. Este atributo é descrito pela classe DPL. Logo, como a prioridade, neste caso, é relacionada ao equipamento físico, propõe-se que o atributo *PrioPhyDev* seja acrescido aos objetos da classe DPL.

O atributo *TypeDSet* é relacionado a determinado dataset. Com isso, propõe-se que as classes dos blocos de controle incorporem esse atributo: GoCB, BRCB, URCB, MSVC, USVCB. Dessa forma, pode-se relacionar cada fluxo de informação com os tipos de mensagem da norma.

O diagrama da Figura 5.20 ilustra a sequência de ações que envolvem uma mudança de parâmetro ou função do IED e sua relação com os blocos de controle. Para exemplificar, imagine que uma residência com painel solar está gerando energia para suprir a demanda da residência. O medidor da residência, intitulado IED nesta tese, iniciou conexão com o SCADA-NG (veja os detalhes no diagrama da Figura 5.19). Após efetuados os serviços MMS, o SCADA tem as informações de controle de cada *dataset* configurado no equipamento.

Os fluxos ativos têm o valor *true* no bit `FlowEna`. No exemplo, considere que as informações de medição do cliente estão sendo monitoradas através de um *dataset* associado a um *report* não buferizado. Com isso, o atributo URCB.RptEna está em *true* e os outros permanecem em *false*.

O atributo que indica que a DER está ligada porém indisponível para conexão (DRCS.modONUnav) e os outros atributos da classe DRCS, se encontram dentro desse *dataset* que está sendo gerenciado. Quando esse painel solar tem a geração excedendo a demanda, ele passa a ter interesse em exportar energia. Com isso, o atributo DRCS.modONUnav recebe o valor *false* e o DRCS.modONAval o valor *true*, o que gera um *report* para o SCADA-NG.

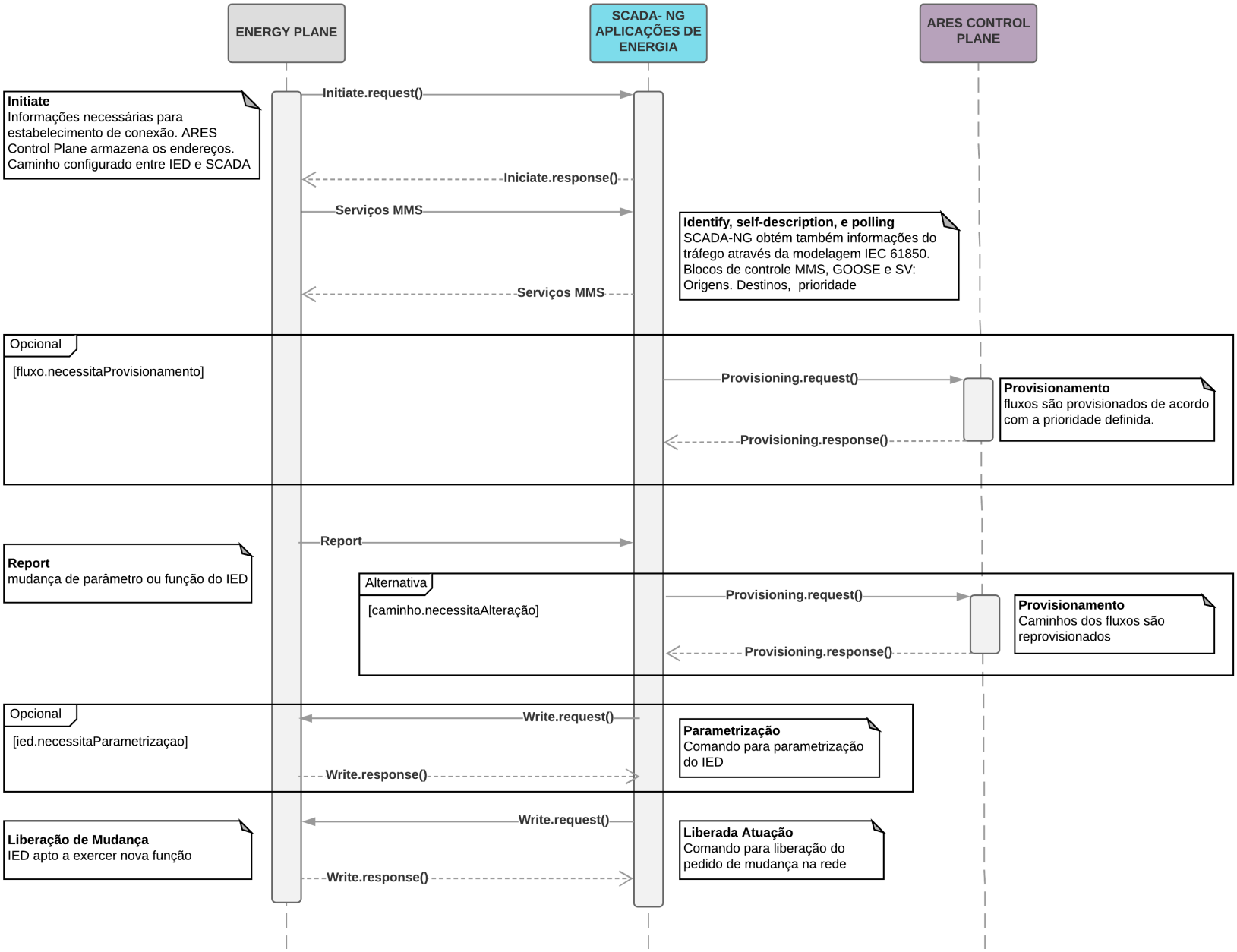


Figura 5.20: Diagrama de sequência quando acontece uma mudança de função.

Quando a mensagem do *report* é enviada para o SCADA-NG, os atributos do *control block* são enviados em conjunto. O SCADA-NG reconhece que o dispositivo está solicitando mudança de função (DRCS.modOnAval em *true*) e precisa ter seu enlace provisionado. Essa alteração faz com que um *dataset* GOOSE seja necessário na rede, já que ao se tornar gerador de energia informações de proteção e controle precisam ser enviadas a partir deste IED para outros que estejam envolvidos na proteção.

As aplicações de energia verificam se o fluxo GOOSE necessário está ou não provisionado. Se estiver, ele apenas ativa esse fluxo e altera a parametrização do IED através do serviço *write*. Se não estiver provisionado, ele coleta as informações contidas nesse *control block* (origem, destino e prioridade) e solicita provisionamento para a API ARES. Após o enlace ter sido provisionado, a GD pode ser liberada para funcionar. É enviado um comando para ativar o fluxo GOOSE e um outro para alterar o grupo de ajustes do IED, caso esse cenário demande mudança na parametrização do IED.

Com isso, o IED está liberado para comunicar e como consequência está liberado para gerar energia na rede. Ressalta-se que, como os ajustes do IED são realizados de acordo com a entrada das GDs no sistema, problemas com a atuação indevida do sistema de proteção podem ser amenizados com o auxílio do *framework* ARES.

O mesmo fluxo de informações se aplica aos outros dispositivos do plano de energia, mesmo que estes não façam parte da geração distribuída. Nesse caso, o fluxo é mais simples já que os fluxos necessários já são conhecidos e configurados no início da conexão. Um exemplo é a rede local da subestação. Os IEDs que possuírem mensagens GOOSE ou SV ativas já terão seus fluxos instalados na conexão com o SCADA-NG, de acordo com a prioridade definida em cada um de seus *datasets*. Já que os IEDs dentro da subestação não fazem parte do sistema de geração, todas as configurações e fluxos já estão ativos e configurados. No entanto, caso alguma proteção possa ser adaptada em resposta ao sistema, o mesmo processo pode ser utilizado fazendo com que o sistema de proteção que utilize comunicação possa responder em tempo real a mudanças no sistema de energia, obedecendo uma comunicação eficiente, onde o tráfego é configurado exatamente para aquele fluxo. Essa característica faz com a carga de tráfego na rede diminua consideravelmente, como será visto no Capítulo 6.

Capítulo 6

Implementação do Framework ARES

A implementação do *framework* ARES foi realizada com objetivo de avaliar a viabilidade da solução, verificando se os resultados são satisfatórios com os requisitos levantados. Para tanto, três ambientes de teste foram criados:

- Validação da API:
  A API foi implementada com a arquitetura *Representational State Transfer* (REST), conforme será detalhado na Seção 6.1, para validação da sua viabilidade de implementação. A rede de comunicação da implementação foi emulada.

- Teleproteção para subestações digitalizadas baseada no ARES:
  Este estudo de caso foi realizado com o objetivo de avaliar a viabilidade de implementação do *framework* ARES para uso na teleproteção de subestações. O cenário foi baseado em uma implementação real, detalhada em [144], e realizado com equipamentos. Neste estudo de caso, também foram realizados testes de desempenho da rede baseados no *framework* mesmo durante falhas na comunicação.

- Testes de desempenho em ambiente emulado:
  Para avaliação do componente de recuperação de falhas do *framework*, foram realizados os testes com o mecanismo *fast-failover* em ambiente emulado [122].

6.1 Validação da API

Neste cenário, são validadas as funcionalidades dos serviços *Discovery* e *Provisioning* do *framework* ARES. Os objetivos são:

1. Validar o serviço *Discovery* da API ARES;
   (a) Validar a coleta das informações dos *datapaths*.
2. Validar o serviço *Provisioning* da API ARES;
   (a) Validar se o caminho foi configurado com sucesso;
   (b) Verificar se apenas os *datasets* ativos têm fluxos configurados na rede.

6.1.1 Cenário de Testes

O ambiente de experimentos, resumido na Tabela 6.1, foi implementado em computadores com processador Intel Core i7, 16GB de memória RAM, executando o sistema operacional Ubuntu 18.04. A rede de comunicação foi emulada usando o Mininet [111] na Versão 2.2.1. O Mininet é uma plataforma flexível para emulação de redes OpenFlow executando *kernel* real, que permite a interação com o Wireshark e com o controlador SDN. Os componentes ARES foram desenvolvidos em python utilizando o controlador RYU [47] com o OpenFlow 1.3 [10]. Para emular o tráfego dos IEDs, foi utilizado o gerador GEESE [126, 140, 141], um gerador de tráfego IEC 61850 desenvolvido para reproduzir fielmente o tráfego GOOSE.

Tabela 6.1: Equipamentos e softwares utilizados nos experimentos.

Item	**Descrição**
Desktop	i7 |1TB HD |16GB RAM |8 portas Ethernet 1GB
Mininet [111]	Versão 2.2.1 - Emulador de redes OpenFlow
RYU [47]	Controlador SDN rodando OpenFlow 1.3
GEESE[126, 140, 141]	Gerador de tráfego GOOSE
Postman [19]	Cliente HTTP para Simular as aplicações de energia

A comunicação entre aplicações de energia e a API ARES foi implementada com a arquitetura REST, que tem sido bastante utilizada nos controladores SDN atuais. Para compor a aplicação de energia, foram utilizados um cliente/servidor MMS e um cliente *HyperText Transfer Protocol* (HTTP). O cliente/servidor MMS foi desenvolvido baseado na biblioteca "libIEC61850" [18]. Para o cliente HTTP, foi utilizada a ferramenta Postman [19], que permite testar serviços RESTfull de forma prática, efetuar o envio de requisições HTTP, realizar a análise do retorno das requisições, escrever e executar *scripts*.

A API ARES foi implementada como uma aplicação do controlador RYU, que abre um *socket* de servidor de rede e aguarda as requisições HTTP do cliente (Postman) para

executar estas requisições. Desta forma, o Postman (representando a aplicação de energia) pode acessar esta API e executar os serviços da API ARES. A topologia utilizada é a padrão do emulador Mininet , contendo um *switch* OpenFlow, dois *hosts*, que funcionam como IEDs (chamados de IED A e IED B), e um controlador OpenFlow. Essa topologia é suficiente para validar a API pois contém todos os componentes necessários para realizar o mapeamento e o provisionamento de enlaces. O IED A foi definido como publicador e, para tanto, iniciava uma ou mais instâncias do gerador GEESE. Tanto no IED B quanto no IED A, foi utilizado o tcpdump/Wireshark [24, 17] para capturar os pacotes, permitindo que os dados fossem armazenados para serem posteriormente tratados. A arquitetura de testes é ilustrada na Figura 6.1.

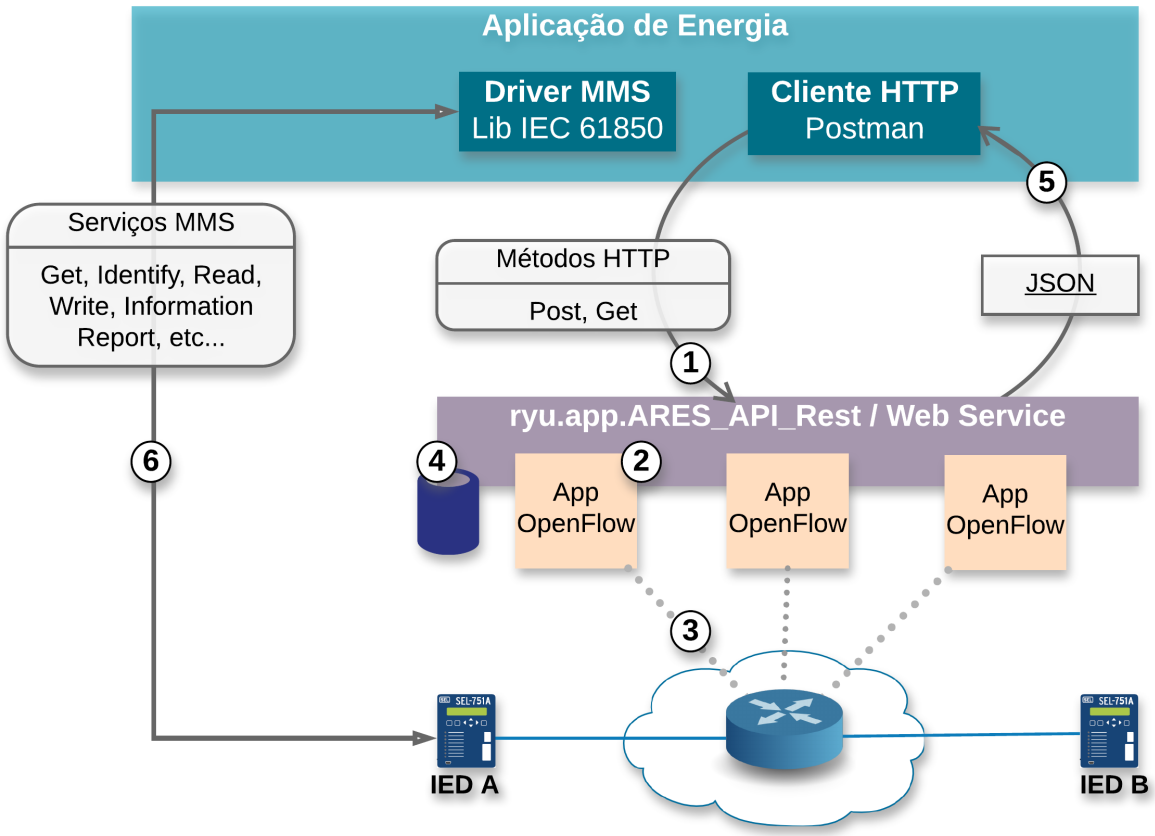


Figura 6.1: Arquitetura de testes para avaliação da API. Comunicação entre aplicação de energia e plano de energia onde o Passo 1 é a requisição e o passo 5 a resposta.

Conforme passo "1" da Figura 6.1, o Postman envia a requisição, baseada nos serviços da API ARES, utilizando a *Uniform Resource Identifier* (URI) do recurso de interesse e os métodos HTTP. Os métodos utilizados na implementação foram o GET para o serviço *Discovery* e o POST para o serviço *Provisioning*. A aplicação `ryu.app.ARES_API_rest` recebe essa requisição, processa o pedido e envia os parâmetros para os componentes ARES para executar as ações, conforme passo "2". Caso faça parte da requisição a interação em tempo real com a rede de comunicação, é executado o passo "3" através do OpenFlow. As informações já coletadas pelo ARES são salvas em um banco de dados, passo "4",

e enviadas em formato *JavaScript Object Notation* (JSON) para o Postman, conforme passo "5". O armazenamento destas informações é importante para que solicitações já realizadas não precisem ser feitas novamente. O passo "6", que ocorre em paralelo com todo o processo, representa a comunicação entre os equipamentos do plano de energia e as aplicações de energia do plano de gerenciamento, através do protocolo MMS.

6.1.2 Avaliação e Resultados

Para validação do serviço *Discovery*, a requisição foi enviada a partir do Postman utilizando o método GET do HTTP. Conforme o gráfico de fluxo gerado com a ferramenta Wireshark [24], representado na Figura 6.2, a primeira requisição, a URI "`/discovery`", solicita os `ids` de cada *datapath* da rede. Ressalta-se que a classe *datapath* do ARES compreende qualquer dispositivo que comunique na rede, seja ele SDN ou não, portanto, são retornados três *datapaths*, os IEDs e o *switch* OpenFlow.

Em seguida, o Postman realiza a requisição do *datapath* específico que quer coletar informações, utilizando a URI "`datapath/id`", individualmente. Em seguida, o *web server* retorna a requisição, em formato JSON, com os valores dos atributos do objeto *datapath* 1 solicitado (Figura B.1 no Apêndice).

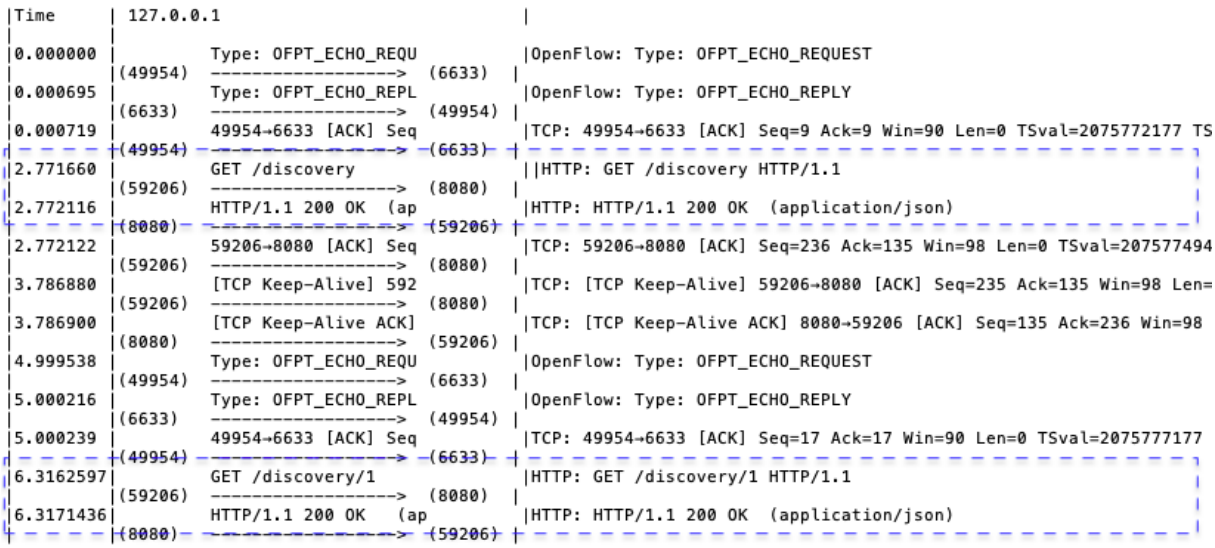


Figura 6.2: Wireshark *Flow Graph* do serviço *discovery*.

Para o serviço *Provisioning*, cujo fluxo está ilustrado na Figura 6.3, a requisição precisa conter os parâmetros da classe *path*. Neste caso, a requisição contém a origem, o destino, e a prioridade ou tipo do fluxo que precisa ser configurado (Figura B.3 no Apêndice). Todas essas informações são coletadas a partir dos serviços `get` e `read` do MMS, que solicitam os objetos/atributos do IED e seus valores. Com isso, tem-se a característica de cada fluxo de forma individual (detalhes da captura do pacote no Apêndice B). A requisição foi realizada com o método POST do HTTP na URI "`/provisioning/add`". Os parâmetros

da requisição (objeto da classe *path*) foram passados em formato JSON. Ressalta-se que, uma vez que o fluxo já foi criado, ao invés da URI ‘‘`/provisioning/add`’’ é usada a ‘‘`/provisioning/modify`’’ para modificar um fluxo já provisionado.

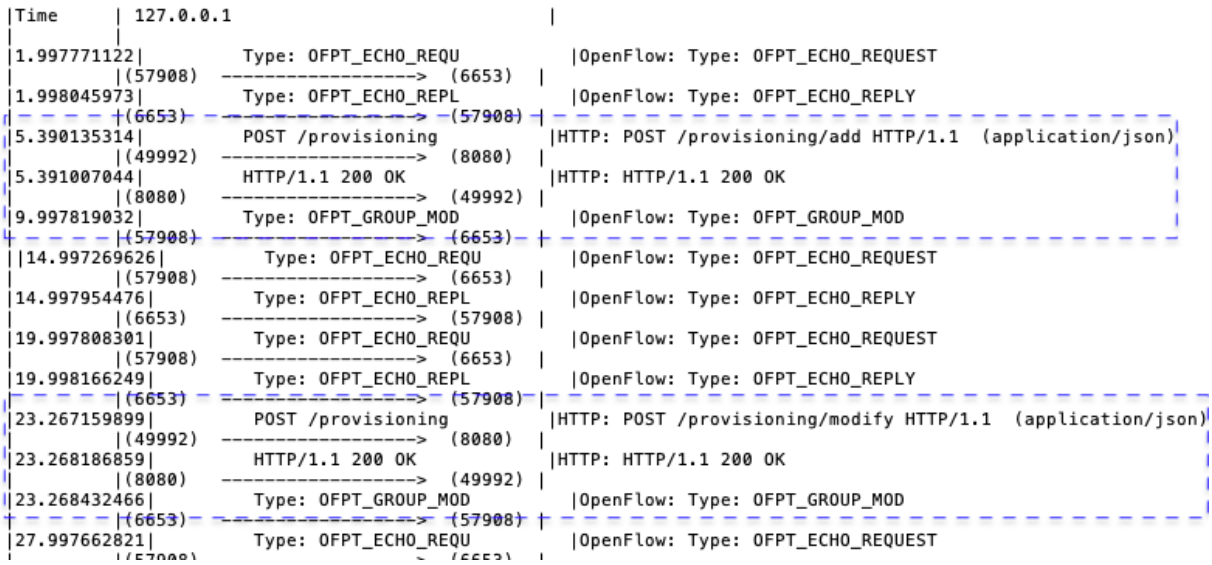


Figura 6.3: Wireshark *Flow Graph* para o serviço *Provisioning Request*.

Como ilustrado no gráfico de fluxos da Figura 6.3, assim que a solicitação de provisionamento é recebida, um pacote *group mode* (Figura B.2 no Apêndice) OpenFlow é enviado para o *switch*. Como os testes foram realizados com OpenFlow 1.3, com a opção de *fast-failover*, os fluxos foram provisionados com a tabela de grupo. Este serviço do OpenFlow configura os equipamentos de rede de acordo com a regra definida, que também é enviada no *payload* do pacote.

Para validar se os fluxos realmente foram configurados, permitindo que uma mensagem GOOSE, oriunda de A para o destino B possa chegar ao destino, foram efetuados os seguintes testes:

- Avaliação do fluxo GOOSE de A para B no destino.
- Avaliação do tráfego no IED de origem e no IED de destino.

Todas as mensagens GOOSE geradas nos testes seguiram o mecanismo de retransmissão padrão dos IEDs da SEL que foram utilizados no teste prático (Seção 6.2). Estes seguem uma Progressão Geométrica (PG) com valor inicial de intervalo entre quadros de 6ms e estabilizando em 1 seg a retransmissão. O mecanismo de retransmissão está ilustrado na Figura 3.16 e explicado na Seção 3.4.3.2. Os quadros gerados pelo GEESE tinham aproximadamente 288 bytes cada, baseado em um *dataset default*. Para validar a geração, foi feita uma transmissão com apenas um fluxo GOOSE do IED A para o IED B, conforme mostrado na Figura 6.4. O tráfego GOOSE no IED A é iniciado aproximadamente no tempo 7 segundos. Verifica-se que todos os pacotes oriundos do IED A chegaram ao IED

B, seguindo exatamente a PG esperada. Nota-se que, no início da transmissão, a PG gera uma rajada de mensagens, e logo estabiliza em 1 segundo. Portanto, funciona conforme o esperado.

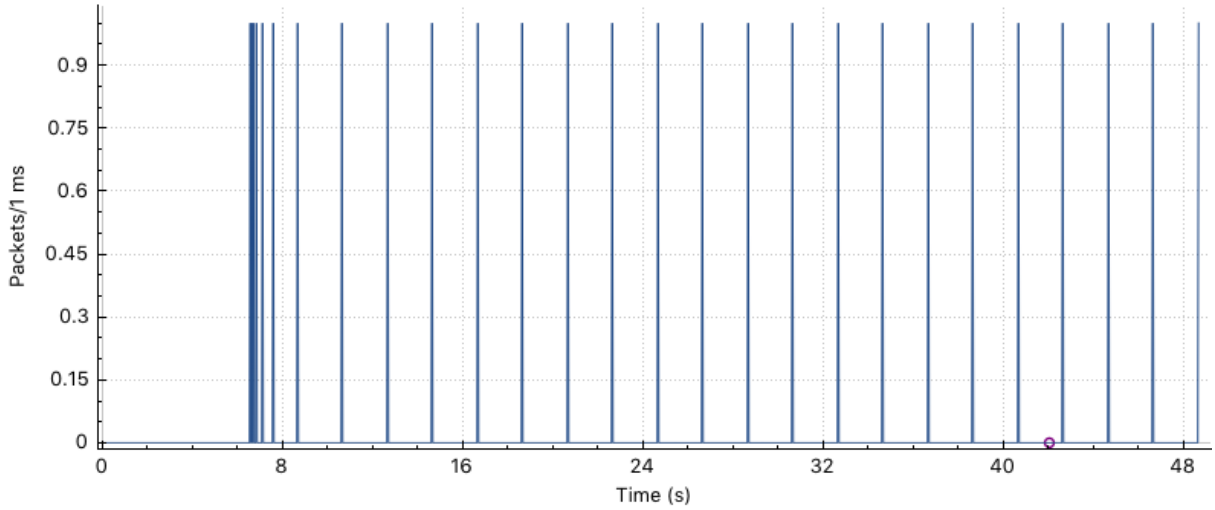


Figura 6.4: Fluxo GOOSE do IED A para o B já com o fluxo provisionado. Captura no IED B.

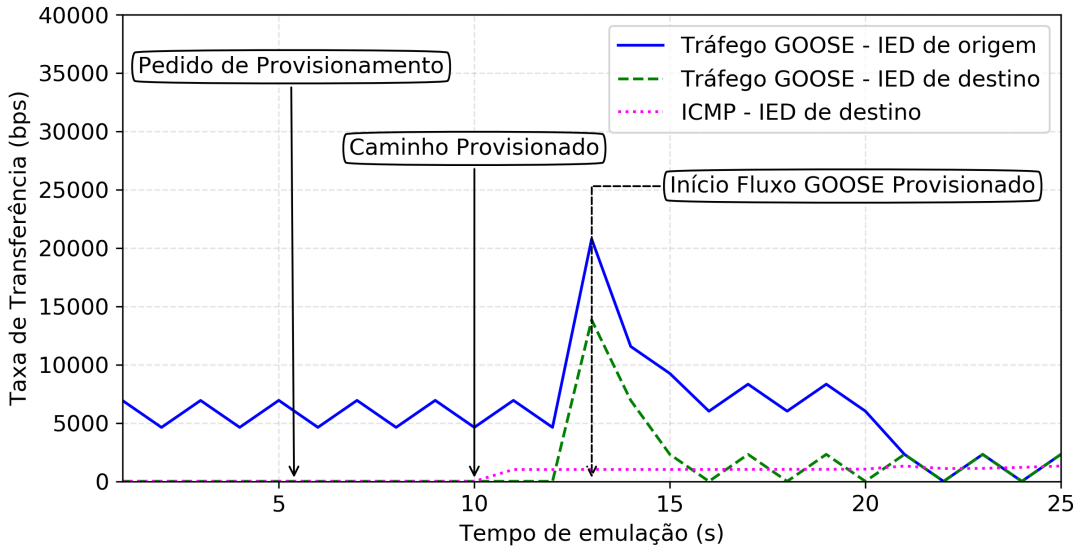


Figura 6.5: Tráfego GOOSE gerado no IED de origem e tráfego recebido no destino.

Em seguida, avaliou-se o uso da API com diversas instâncias de tráfego GOOSE. Foram iniciadas cinco instâncias do gerador GEESE no IED A, além do tráfego *Internet Control Message Protocol* (ICMP) de fundo. No momento inicial da captura, estes cinco fluxos já estavam estabilizados com retransmissão de um segundo. No tempo $5,4$ s do teste, o pedido de provisionamento do ARES foi realizado. Em seguida, aproximadamente no tempo 10 segundos, o caminho foi provisionado. Em seguida, no tempo 13 s, o fluxo GOOSE de interesse (GOOSE 6) foi iniciado.

A linha cheia na Figura 6.5 indica o tráfego GOOSE gerado no IED de origem. Verifica-se que o tráfego dos 5 fluxos GOOSE está em condição estável e que, logo após o tempo 13 segundos, se inicia o sexto fluxo com a rajada de início de transmissão. A linha verde tracejada indica o tráfego GOOSE recebido no IED de destino. Verifica-se que, no início da captura, mesmo com os 5 fluxos GOOSE sendo enviados da origem, os fluxos não são recebidos no destino. Esse comportamento já era esperado já que o ARES não provisionou o caminho para esses cinco fluxos. No tempo 10 segundos o ARES provisiona o fluxo ICMP, que passa a ser recebido após esse tempo, e também realizada a configuração para provisionamento do sexto fluxo GOOSE, que será iniciado logo em seguida. O tráfego ICMP de fundo, representado pela linha pontilhada, teve o fluxo provisionado para comparação no IED de destino. Portanto, até o provisionamento do enlace, mesmo que estivessem sendo gerados fluxos GOOSE e ICMP na origem, o destino não recebia esses dados. Assim que o provisionamento é realizado, o fluxo ICMP que já estava sendo gerado é recebido, e em seguida o novo fluxo GOOSE. No tempo 20 segundos, os 5 primeiros fluxos são encerrados, restando apenas o fluxo de interesse e o tráfego ICMP.

Para a avaliação do ARES relacionada aos pedidos de provisionamento realizados dinamicamente pela aplicação de energia, de forma a modificar a rede de acordo com o perfil exigido pelo fluxo, foram criados três fluxos diferentes, e seus provisionamentos foram realizados exatamente de acordo com cada perfil. Os três fluxos possuíam o mesmo `EtherType`, 0x88B8, no entanto endereços MAC *Multicast* diferentes e prioridades diferentes caracterizando cada fluxo.

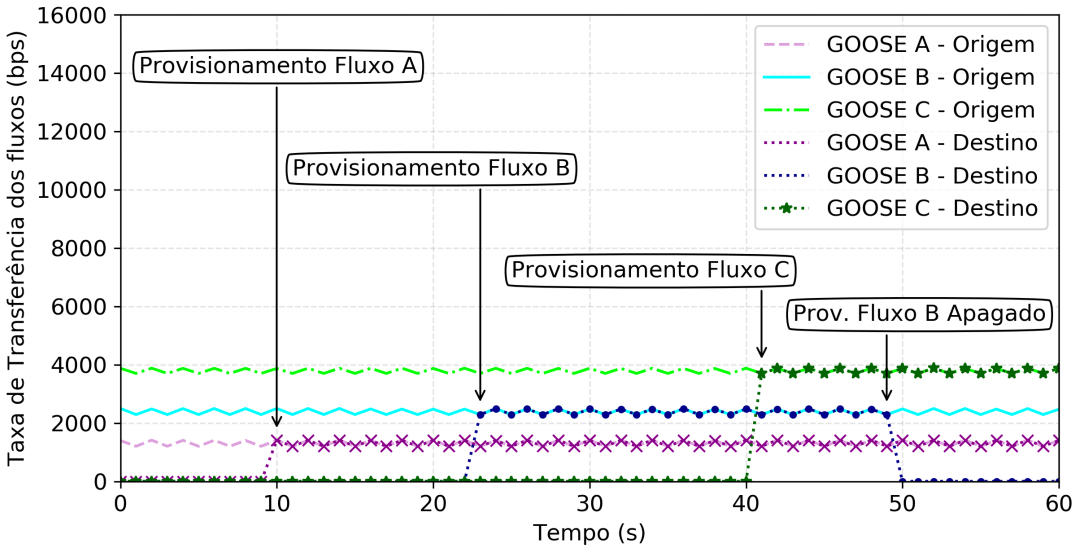


Figura 6.6: Tráfego GOOSE gerado no IED de origem e tráfego recebido no destino.

Para que o tráfego dos fluxos pudesse ser diferenciado, três tamanhos de *dataset* diferentes foram gerados. O fluxo A é o menor e tem o pedido de provisionamento realizado primeiro, em seguida o fluxo B e por último o fluxo C. O *switch*, além do

provisionamento, também recebe uma solicitação para apagar o fluxo B após pouco mais de 25 segundos. Conforme ilustra o gráfico da Figura 6.6, os fluxos só chegam ao destino exatamente na medida que são provisionados. Ressalta-se que numa rede tradicional, todos os fluxos GOOSE estariam sendo recebidos independente do seu perfil, inundando a rede. O ARES, além de diminuir a carga desta inundação, permite que apenas os fluxos configurados em cada IED e reportados ao plano de controle ARES tenham acesso à rede.

Os testes mostraram que a implementação da API ARES e a integração com o *framework* funcionaram como o esperado, permitindo que um sistema supervisório possa interagir em tempo real com a rede de comunicação, mapeando os dispositivos de forma automática e provisionando os enlaces de forma dinâmica, de acordo com a configuração dos IEDs envolvidos na comunicação. A configuração feita pelo ARES é realizada por fluxo, e não por dispositivo ou por protocolo (apenas), tornando o sistema mais flexível e mais inteligente. Tráfegos que não sejam conhecidos não são configurados, tornando o sistema mais confiável. Ressalta-se que, apesar de não avaliado por estar fora do escopo do trabalho, qualquer dispositivo só deveria ter permissão de participar da rede após autenticado [174]. Assim, a importância do tratamento da segurança do sistema por meio da implementação de mecanismos de segurança apropriados para o contexto é reforçada.

6.2 Estudo de Caso: Teleproteção de Subestações Digitalizadas

Este estudo de caso aborda a validação do *framework* ARES para um sistema de teleproteção. Os valores de atraso de comunicação exigidos para atuação correta das funções de teleproteção são rígidos e exigem avanços consideráveis também na área de comunicação. Portanto, além da validação de funcionalidades do *framework* foram avaliadas também as métricas de latência, perda de pacote e carga na rede com e sem o *framework*, em condição normal e em condições de falha na rede de comunicação. A análise da resiliência do sistema baseado no *framework* foi feita em comparação com os métodos tradicionais.

Os principais objetivos deste estudo de caso são:

1. Validar a coleta de informações dos IEDs através dos serviços MMS;
2. Avaliar se apenas o fluxo ativo está, de fato, configurado;
3. Avaliar a carga da rede de comunicação configurada de forma tradicional e com o *framework*;
4. Avaliar a latência da rede de comunicação configurada de forma tradicional e com o *framework*;
5. Avaliar a resiliência da rede de comunicação configurada de forma tradicional e com o *framework*.
   (a) Comparação com RSTP, PRP e HSR;
   (b) Avaliação com os IEDs em PRP e a rede configurada com o *framework*.

6.2.1 Teleproteção

As Linhas de Transmissão (LT), por percorrerem uma extensa área geográfica, estão sujeitas à maior probabilidade de ocorrência de eventos prejudiciais ao sistema elétrico de potência [183]. O tempo de permanência de uma falta em uma LT é crucial para o desempenho do sistema elétrico [183, 83]. Nesse sentido, a proteção de distância é considerada como uma boa solução para atender a exigência temporal para atuação da proteção, especialmente em LTs que apresentam grandes comprimentos [82]. Porém, a temporização utilizada que pode variar de 20 a 30 ciclos* [183] para o trecho de segunda zona, dentro da linha protegida, pode causar instabilidade no sistema, dependendo das condições operativas do mesmo, bem como do tipo de perturbação.

*O ciclo pode ser de 16,6ms para 60Hz e 20ms para 50Hz

Por este motivo, desde 2010, o grupo de trabalho 34/35.11 do Cigré [28] considera o uso de comunicação nos esquemas de proteção de linhas uma opção eficiente. A justificativa para o emprego de telecomunicações nos esquemas de proteção de linhas é respaldada na aceleração do tempo para enviar o comando de disparo, que pode ser executado em um tempo tipicamente menor, 2 a 3 ciclos após a ocorrência da falta em qualquer ponto da linha [183]. Os esquemas que utilizam comunicação para acelerar a atuação da proteção são conhecidos como esquemas de teleproteção e têm a estrutura geral definida na norma IEC 60834 [1].

Os esquemas de teleproteção conseguem melhorar a seletividade e o tempo de resposta dos esquemas *stand-alone* de proteção de LTs, pois permitem que os IEDs de proteção possam trocar informações lógicas entre os terminais de uma LT para comparar suas respostas e determinar o sentido correto da falta. Isto permite que a tomada de decisão do IED seja acelerada, tanto no bloqueio contra faltas externas, quanto na eliminação de faltas internas, em todo o comprimento da linha. Esses esquemas são baseados em sinalização, e são conhecidos como esquemas de comparação de estados baseados em telecomunicações.

O uso de comunicação resulta na necessidade do uso de protocolos de comunicação para a automação do sistema elétricos [124], o que gerou um esforço na padronização da comunicação entre subestações. A norma IEC 61850 [177] veio no sentido de melhorar o desempenho dos esquemas de proteção e controle em subestações, permitindo maior eficácia das atuações e maior sensibilidade no sistema [125]. A parte 90-1 [83] da norma IEC 61850, que trata o uso da IEC 61850 para esquemas de teleproteção, foi publicada em 2010 e considera quais as funções de proteção que podem ser utilizadas, as informações que devem ser trocadas, os requisitos de comunicação, as informações sobre os serviços e as arquiteturas de comunicação que podem ser usados além do uso da linguagem SCL [79].

No entanto, a implementação desses sistemas não depende somente do uso da norma e seus protocolos, como o GOOSE [86] e o SV [87], mas também dos sistemas de comunicação implementados. Uma falha na rede de comunicação impede que as informações possam ser trocadas, inviabilizando a comparação de estados pelos IEDs participantes dos esquemas de proteção. Por este motivo, a recuperação de falhas do sistema de comunicação deve ter tempos mínimos, não afetando as funções de teleproteção e atuação dos equipamentos. Outro ponto importante é a necessidade do isolamento de tráfego entre a subestações. O envio somente do tráfego necessário para os enlaces entre subestações permite que menos banda seja utilizada tornando os projetos menos caros e possibilitando melhora no desempenho.

O uso do *framework* ARES para comunicação entre subestações permite a implementação de uma recuperação de falhas eficiente além de uma comunicação mais leve e que onere menos o canal de comunicação em comparação com as redes tradicionais utilizadas atualmente. A configuração da rede de comunicação é autonômica e mais inteligente, já que a configuração é feita por fluxo, de acordo com cada *dataset* IEC 61850

existente para tráfego na rede, e não para o equipamento como um todo. A aplicação de energia baseada no *framework* para supervisão e controle do sistema de teleproteção é mais eficiente pois pode interagir em tempo real com a infraestrutura alocando recursos de forma dinâmica, pode mapear dispositivos e suas configurações ativas automaticamente e receber informativos de gerenciamento da rede de comunicação.

6.2.2 Cenários de Testes

O estudo de caso descrito neste capítulo foi realizado com base na arquitetura de um projeto de teleproteção implementado na empresa Braskem[†], descrito por Oliveira e Lopes [144]. A empresa possui um anel óptico interligando cinco subestações com uma rede *Synchronous Optical Network* (SONET), conforme Figura 6.7, com um multiplexador em cada subestação. O projeto contemplou a substituição de 266 relés eletromecânicos por IEDs com os protocolos da norma IEC 61850. O estudo de seletividade previu a aplicação de diversas funções de proteção com o uso de mensagens GOOSE no interior das subestações e entre subestações [144]. O enlace *Wide Area Network* (WAN) da empresa é composto por canais que totalizam 155Mbps.

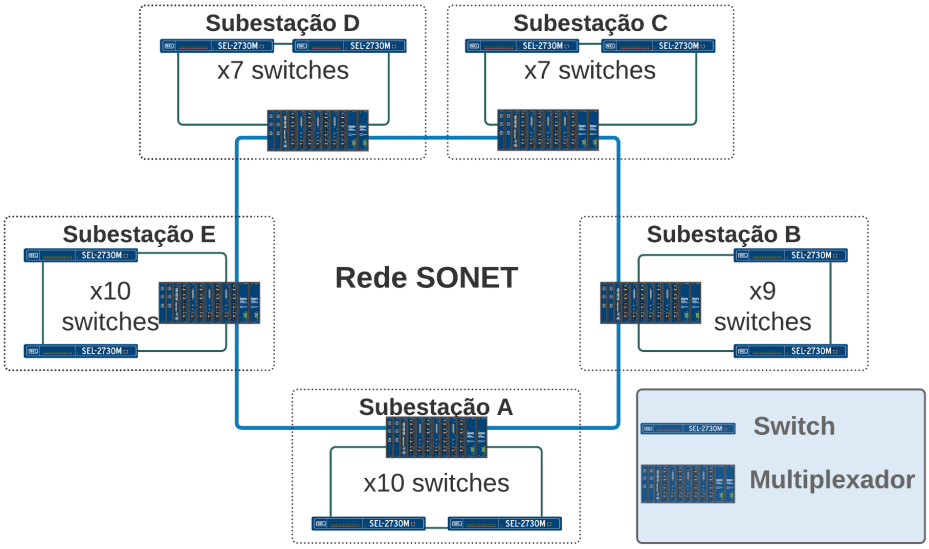


Figura 6.7: Topologia de comunicação entre subestações da Braskem. Adaptada de [144].

Para reproduzir o cenário, porém puramente em rede Ethernet, a rede foi reproduzida com *switches* tradicionais ou SDN, conforme ilustrado na Figura 6.8, com os equipamentos descritos na Tabela 6.2. Para cada subestação tem-se um *switch* de saída. Portanto, a WAN está representada por um anel com 5 *switches*. Para cada subestação, foram colocados quatro IEDs 751A pra representar a *Local Area Network* (LAN) da subestação. A comunicação avaliada será entre as subestações A e B, e, portanto, cada uma possui um

[†]https://www.braskem.com.br/perfil

Tabela 6.2: Equipamentos utilizados nos experimentos.

Modelo	**Descrição**	**Qtd.**
SEL 2740S [103]	*Switch* SDN	5
SEL 2730M [102]	*Switch* Ethernet Gerenciável, 24 Portas	5
SEL 9524 [109]	Antena GPS	1
SEL 2488 [101]	Relógio de Rede Sincronizado por Satélite	1
SEL 421 [104]	IED: Sistema de Proteção, Automação e Controle	2
SEL 751A [108]	IED: Proteção de Alimentador	20
Ultrabook DELL	i7 |500GB HD |8GB RAM	2

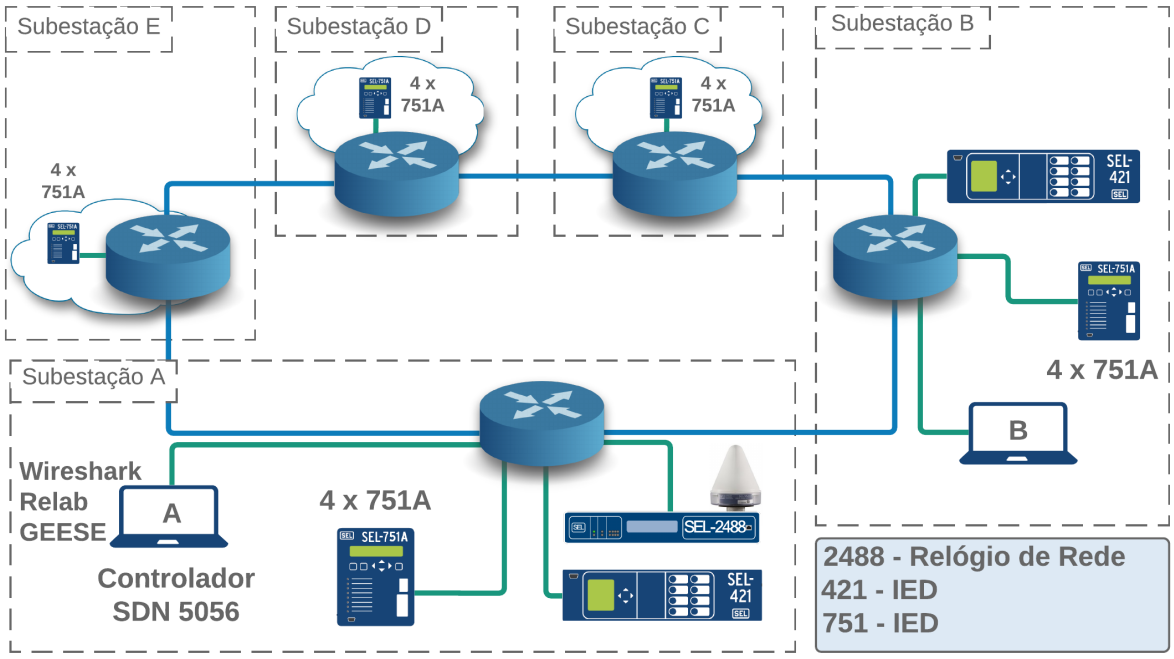


Figura 6.8: Topologia de testes com *switches* SDN, IEDs, supervisório e relógio para sincronismo temporal.

IED 421. Os equipamentos foram sincronizados com *Precision Time Protocol* (PTP) [4], através da antena GPS e do relógio de rede SEL 2488. As portas utilizadas entre os *switches* foram de 100Mbps, par metálico.

Para a configuração baseada no *framework*, foram utilizados *switches* SDN, com suporte ao OpenFlow, modelo 2740S. Para os testes com o RSTP, foram utilizados *switches* tradicionais com suporte ao protocolo RSTP, modelo 2730M. Os IEDs utilizados para realizar a teleproteção da linha de transmissão entre as subestações, modelo SEL-421, dão suporte também ao PRP, além da norma IEC 61850.

Além destes, dois *laptops* foram utilizados nos testes, um conectado no *switch* A e o outro no B. Os *softwares*, descritos na Tabela 6.3 foram instalados nos dois *laptops*, com exceção do controlador SDN, que estava instalado apenas no computador A. Para confi-

guração dos IEDs foram utilizados os *softwares* acSELerator QuickSet [105] e acSELerator Architect [106]. O controlador SDN utilizado foi o SEL-5056 [107], comercializado pela mesma empresa (SEL) dos *switches* SDN. Como cliente MMS, para leitura dos valores dos IEDs e envio de comandos, foi utilizado o *software* Relab. Para análise do tráfego da rede foram utilizados o Wireshark e o tcpdump.

Tabela 6.3: Softwares utilizados nos experimentos.

Software	**Descrição**
SEL 5056 [103]	Controlador SDN
SEL 5032: acSELerator Architect [106]	*Software* para configuração IEC 61850
SEL 5030: acSELerator QuickSet [105]	*Software* para parametrização do IED
Wireshark	*Sniffer* de Rede
Relab	Cliente MMS

Foram considerados 10 *datasets* GOOSE entre todas as subestações da planta industrial, compondo o tráfego da WAN. Desta forma, tem-se cada uma das cinco subestações enviando duas mensagens GOOSE, uma para cada subestação adjacente. Por exemplo, como ilustrado na Figura 6.8, um fluxo de mensagens GOOSE é enviado da subestação A para a B e vice-versa. Como estão representadas cinco subestações no anel, tem-se 10 fluxos que participam do anel da WAN. As mensagens entre as subestações A e B foram configuradas nos IEDs 421. As demais foram configuradas no IEDs 751A.

Para o tráfego da LAN foram configurados 8 *datasets* por IED, que era a maior quantidade que poderia ser gerada. Foram configurados quatro *datasets* cheios, com aproximadamente 1200 bytes cada, e quatro *datasets* com apenas um atributo, com aproximadamente 150 bytes cada. Esses *datasets* foram usados como tráfego de fundo, quando oriundos dos IED 751A, da LAN, e como tráfego de interesse quando oriundos dos IEDs 421, de teleproteção. Todos os IEDs 751A descritos na arquitetura foram configurados para publicar os oito *datasets* GOOSE, mais um ou dois para a WAN conforme o teste realizado e descrito na Seção 6.2.3 . Os IED 421 tiveram o envio alterado conforme o objetivo do teste, como cálculo de latência ou carga (conforme detalhado em cada teste).

Para apuração dos resultados, foram utilizados:

- Registro de sequencial de eventos (*Sequential Events Recorder* (SER)) dos IEDs: esse registro armazena a mudança de estado da variável interna do IED com a sua estampa de tempo. A precisão é de 4 milissegundos e os equipamentos são sincronizados através de GPS. Ressalta-se que, a precisão é de 4 ms, pois esse é valor do ciclo de processamento do IED. Desta forma, mesmo que o *frame* seja recebido no tempo "x", a estampa será marcada apenas no próximo ciclo, que ocorre de 4ms em 4ms. Esse tempo não tem como ser expurgado dos cálculos.

- Wireshark e tcpdump: para os casos que foram usadas essas ferramentas, o tráfego

das portas que estavam diretamente conectadas ao IED foram espelhadas para um computador.

6.2.3 Avaliação e Resultados

O diagrama da Figura 6.9 ilustra o passo a passo realizado nos primeiros testes. Nele estão representados os IEDs 421, A e B, o computador contendo o cliente MMS Relab e o controlador SDN 5056 e os *switches* SDN da rede, 2740M.

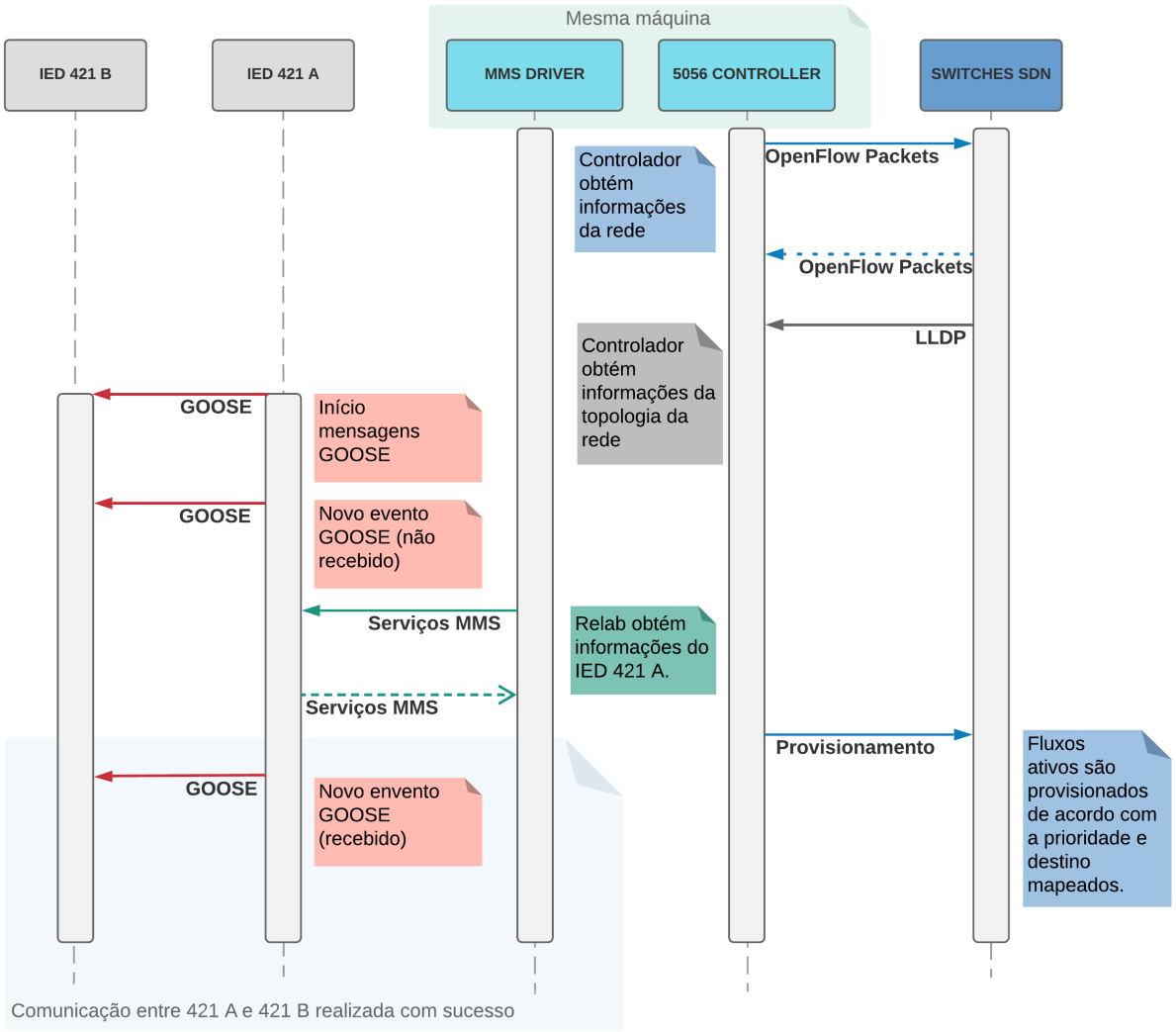
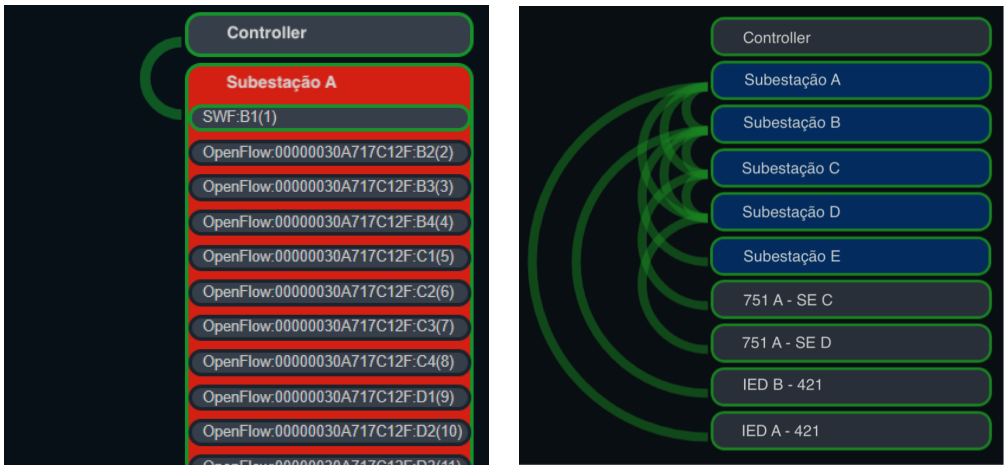


Figura 6.9: Diagrama de Testes.

Antes do Relab estabelecer a conexão com os IEDs, o caminho entre o supervisório e os IEDs precisa ser estabelecido. Logo, as primeiras mensagens que trafegam na rede são as mensagens LLDP para mapeamento da rede (Figura B.4 no Apêndice) e as mensagens OpenFlow entre os *switches* e o controlador. Conforme as mensagens LLDP chegam ao controlador, o ARES é capaz de inferir a topologia da rede (Figura B.5 no Apêndice), como ilustra a Figura 6.10.



(a) Primeiro *switch* mapeado. (b) Topologia mapeada.

Figura 6.10: Mapeamento do controlador SEL 5056 da topologia da rede de comunicação.

Após esta fase inicial, o controlador baseado no ARES configura o caminho entre o IED e o supervisório, e, desta forma, o Relab estabelece conexão com o IED e inicia o *driver* MMS. Com isso, os serviços *Initiate, Identify, Get* e *Read* começam a ser executados. Após a execução dos serviços MMS, o ARES coleta todas as informações relacionadas ao IED. Para este teste, foi realizado todo o processo de *self-description*, de forma que todo o conteúdo do IED fosse enviado para o supervisório.

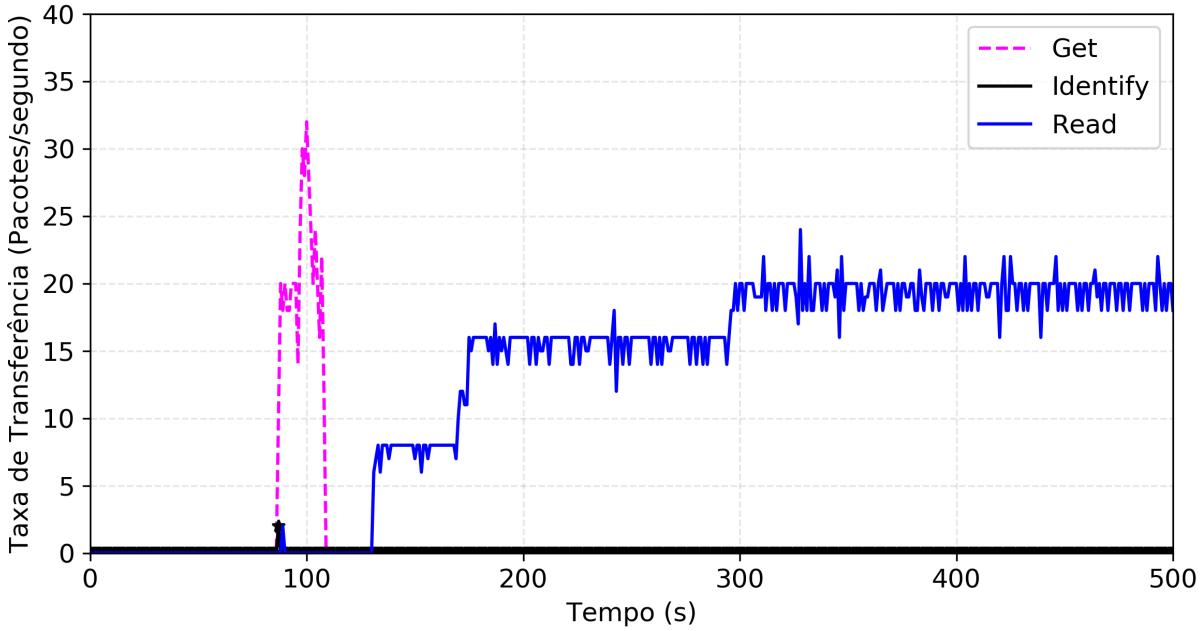


Figura 6.11: Comunicação entre 421 e cliente MMS. Coleta de informações para os serviços da API ARES.

Conforme ilustra o gráfico da Figura 6.11, a conexão foi iniciada próximo ao tempo

85 segundos. Em seguida, tem-se um pacote `Identify`, linha cheia preta, que permite mapear inclusive o modelo do IED e sua versão de *firmware*. O processo de *self-description* completo, serviço `Get` representado pela linha tracejada magenta, durou cerca de 20 segundos, e todos os atributos contidos no IED foram mapeados nesse tempo. A solicitação de leitura dos valores desses atributos através de *polling*, serviço `Read` representado pela linha azul, iniciou no tempo 130 segundos e permaneceu assim durante toda a conexão, atualizando os dados de 500 em 500 milissegundos. Esse processo permitiu o mapeamento automático no Relab de todo o IED.

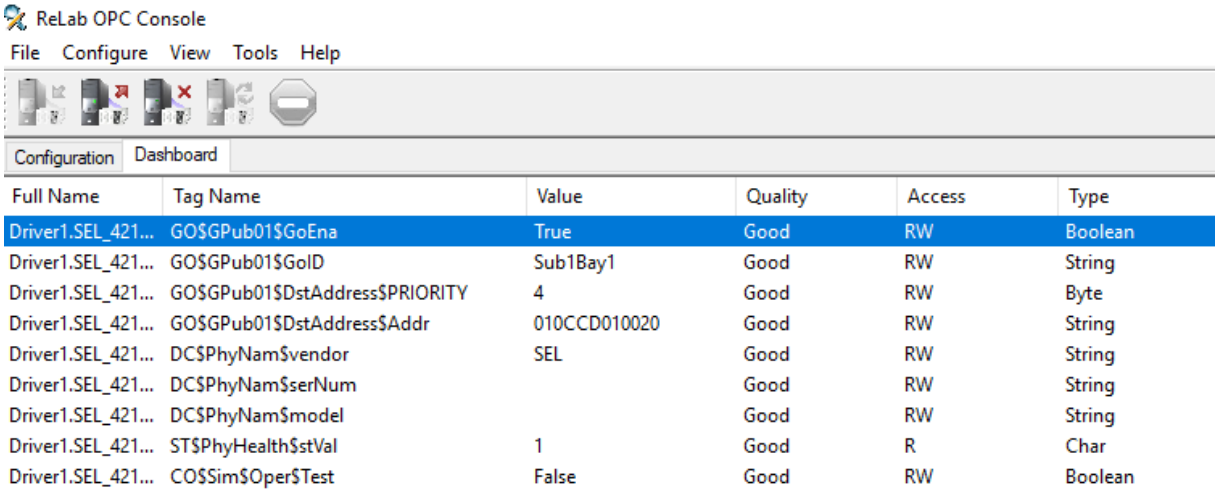


Figura 6.12: Comunicação entre 421 e cliente MMS, utilizando a visualização do *Dashboard* do Relab.

O *Dashboard* do Relab para esta conexão, com os atributos escolhidos para visualização, pode ser visto na Figura 6.12, onde as informações de interesse sobre o IED A são apresentadas. As informações mapeadas para este teste foram:

- Equipamento: fornecedor, número de série do IED, Modelo do IED, estado atual do IED (em funcionamento, em falha), estado operacional (em teste ou não);
- Tráfego GOOSE: se o *dataset* GOOSE está ativo ou não, identificação do fluxo GOOSE (Sub1Bay1), endereço de destino e prioridade do fluxo.

O fornecedor do equipamento é a empresa SEL, os valores de número de série e modelo vieram vazios (no entanto, já foram enviados pelo serviço `Identify`). A mensagem GOOSE, associada ao dataset `GPub01` está ativa, tem o identificador Sub1Bay1, prioridade 4 e destino *multicast* 01:0c:cd:01:00:20. O equipamento não apresenta problemas (health.stVal = 1) e não está em simulação (Sim.Oper.Test = False)[‡]. Com essas informações, o fluxo ativo no IED já está mapeado para a aplicação de energia.

[‡]A modelagem IEC 61850 permite que o fluxo seja colocado em modo simulação, de forma que a recepção e envio de mensagens são testadas, mas o conteúdo do *dataset* não é utilizado. Desta forma, não ocorrem atuações, mas a assinatura correta das mensagem pode ser testada

Assim que os IEDs são ligados, já começam a enviar mensagens GOOSE, conforme diagrama de fluxos da Figura 6.9. Os *datasets* GOOSE, por padrão, já ficam ativos nos equipamentos. Desta forma, assim que os dispositivos são ligados, as mensagens GOOSE já ficam disponíveis na rede. Isso ocorre antes mesmo da conexão com o supervisório. Ressalta-se que, conforme a proposta do *framework* ARES, o fluxo no IED de origem pode estar ativo ou não. Com isso, a aplicação de energia ARES pode decidir por liberar ou não um tráfego GOOSE na rede. Essa possibilidade é possível através do atributo `GoEna` (GOOSE Enable) da classe GoCB da norma. No entanto, os IEDs atuais não aceitam este comando, e, portanto, o mecanismo não foi avaliado nos equipamentos testados.

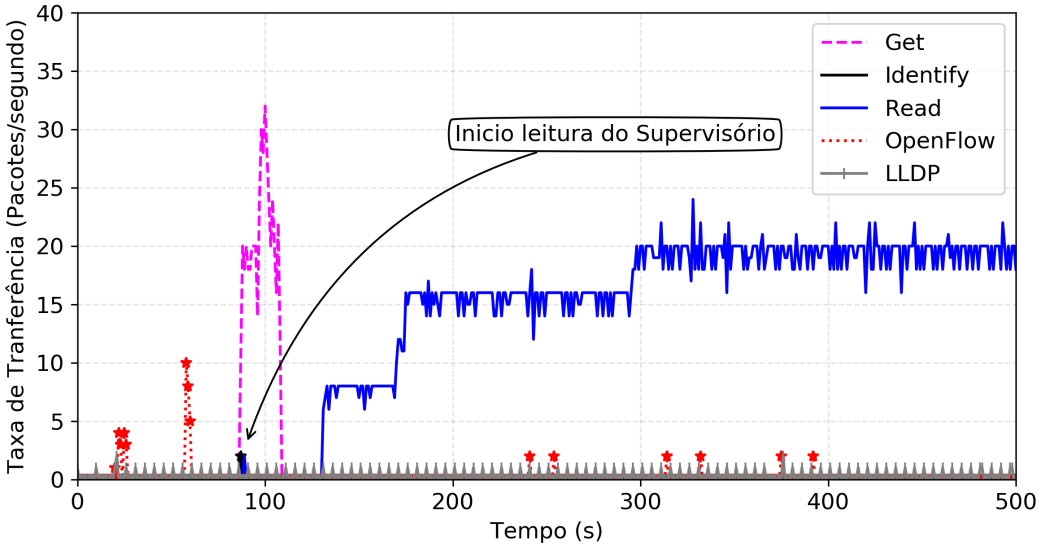


Figura 6.13: Tráfego da rede no momento do provisionamento do enlace capturado no Computador com Relab e 5056.

A Figura 6.13 mostra, além do tráfego MMS, o tráfego OpenFlow e LLDP na rede próximo ao período de mapeamento realizado pelo ARES. Ressalta-se que a troca LLDP na rede, a comunicação OpenFlow entre controlador e e *switches* e a comunicação MMS acontecem em paralelo. Como ilustrado na Figura 6.13, o tráfego de controle (OpenFlow e LLDP) é bem menor que um tráfego MMS de supervisão e controle MMS não afetando a qualidade da rede.

Com as informações coletadas pelo MMS e o mapeamento realizado pelo controlador o ARES já pode provisionar o fluxo. Com os serviços MMS realizados, a aplicação de energia ARES já sabe, além das informações do IED, que existe apenas um fluxo GOOSE ativo e suas informações.

O gráfico da Figura 6.14 mostra o tráfego do IED 421 B, assinante das mensagens e o tráfego gerado pelo publicador destas mensagens, o IED 421 A, com um *dataset* de aproximadamente 484 bytes. É mostrado também o tráfego WAN oriundo da subestação C, gerado pelo IED 751A, um *dataset* com 1200 bytes. Ressalta-se que o tráfego GOOSE,

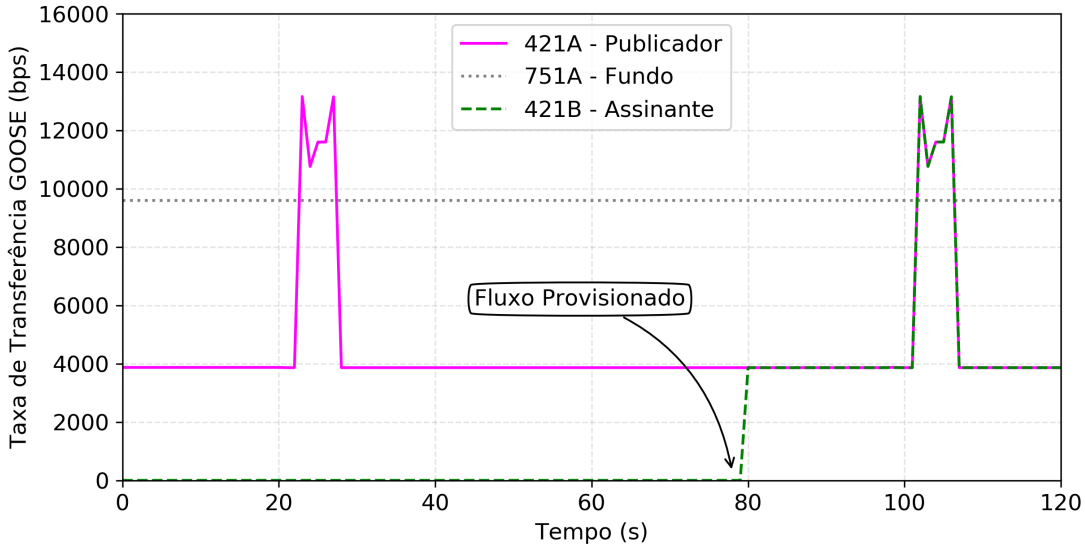


Figura 6.14: Tráfego da rede no momento do provisionamento do enlace.

apesar de não ser de interesse do assinante, por ser *multicast* em camada 2 é publicado para toda a rede.

Até o momento 80 segundos, nenhum fluxo está provisionado para alcançar o IED 421 B. Por este motivo, como mostra o gráfico da Figura 6.14, esse fluxo é gerado pelo publicador, mas não chega ao IED de destino. Da mesma forma, apesar de existir tráfego de fundo sendo gerado pelo IED 751A, este também não chega ao IED assinante. No momento 80 segundos, o ARES provisiona o fluxo e, com isso, apenas o fluxo de interesse, `Sub1Bay1`, chega ao destino. Ressalta-se que o pico da mensagem GOOSE, após o tempo 100 segundos, foi uma mudança de evento gerada, como a ocorrida após o tempo 20 segundos. Em 80 segundos, o tráfego recebido está em condições estáveis. Como já era esperado, o fluxo do IED 751A, que não possui fluxo configurado, continua sem chegar ao IED B.

O gráfico da Figura 6.15 ilustra os outros fluxos que o ARES provisionou. A linha cheia magenta representa o tráfego PTP para que os dispositivos fossem sincronizados no tempo. A linha pontilhada verde mostra o acesso Telnet do IED. Como um supervisório estava montado realizando aquisições com Telnet consecutivas, e um *script* para configuração da parametrização interna do IED fazia acessos ao dispositivo, pode-se verificar que o tráfego é maior do que os outros tráfegos ilustrados no gráfico. Para averiguação da configuração por conteúdo, o fluxo GOOSE teve o seu provisionamento desfeito, e, com, isso verificou-se a extinção desse tráfego no destino.

Os testes validaram que o mapeamento da rede em tempo real dos protocolos GOOSE e MMS pode ser realizado automaticamente por meio do ARES. Essa característica é especialmente importante, pois permite que a rede tenha os fluxos ativos configurados assim que os equipamentos sejam ligados. Por ser realizado de acordo com a configuração

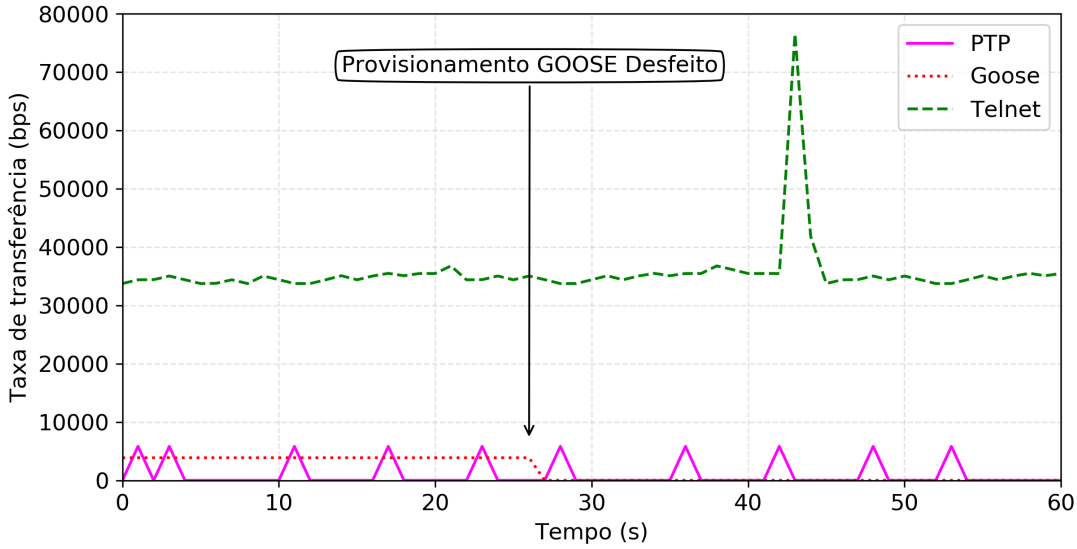


Figura 6.15: Tráfego no IED 421B.

dos IEDs, o provisionamento da rede retrata os fluxos ativos nos equipamentos finais. Essa característica onera menos a rede do que as soluções atuais, como será averiguado na Seção 6.2.4.

Da mesma forma, os fluxos são provisionados respeitando suas necessidades em tempo real. Caso seja de interesse que um *dataset* fique inativo durante um período determinado, o fluxo pertencente a este *dataset* também pode ser retirado da rede de comunicação, não onerando o canal sem necessidade. A liberação ou não do fluxo foi realizada apenas nos *switches* da rede de comunicação que tiveram seu fluxos provisionados ou alterados.

6.2.4 Testes de Desempenho

Nesta seção, o comportamento de uma rede controlada pelo ARES é comparado ao de uma rede controlada de forma tradicional. Os mecanismos das redes tradicionais utilizados em subestações para garantir resiliência são o RSTP, o PRP e o HSR. O PRP foi escolhido para representar as redes que são paralelas (HSR, PRP) e o RSTP para representar os mecanismos de recuperação.

Para tanto, a rede reproduzida com *switches* SDN, ilustrada na Figura 6.8, foi também reproduzida com *switches* ethernet tradicionais com suporte ao RSTP, modelo 2730M. Os outros IEDs, o relógio GPS e os computadores continuaram ligados aos mesmos equipamentos que já estavam nos testes anteriores.

Ressalta-se que o PRP é um método com arquitetura completamente diferente a empregada no estudo de caso, já que precisa de duas redes similares, completamente separadas, para funcionar. Com isso, o anel precisaria ser duplicado, além da conexão

com os IEDs. Desta forma, a comparação com os outros métodos é afetada. Para que a quantidade de dispositivos fosse mantida similar, os IEDs de prova foram ligados numa topologia linear com 3 e 2 *switches*. Como a rede é paralela, tem-se 5 *switches* no total, porém a rede A com 3 e a rede B com 2. Como o caminho escolhido pelo RSTP e pelo ARES tinha dois *switches*, a quantidade de saltos se manteve similar.

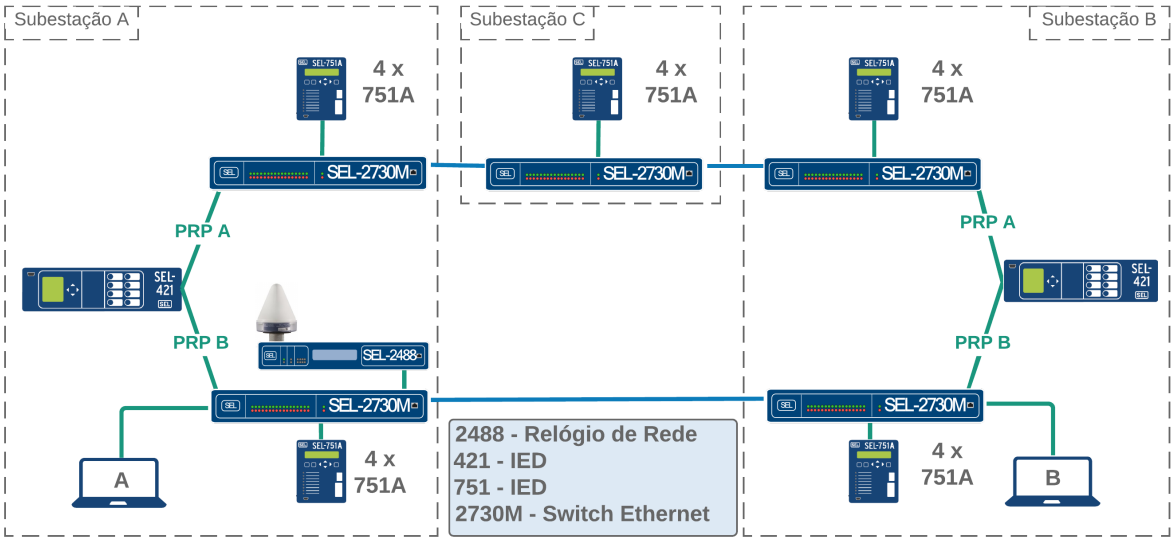


Figura 6.16: Topologia dos testes com IED 421 e PRP, no qual duas redes disjuntas, chamadas de Rede A e Rede B, são utilizadas simultaneamente para dar maior resiliência a falhas na rede.

O teste proposto promove uma sequência de eventos nos IEDs com uma alta frequência, fazendo com que todas as mensagens GOOSE enviadas tenham um conteúdo diferente da mensagem anterior, levando a uma reinicialização do processo de encaminhamento das mensagens GOOSE. Para tanto, foi desenvolvido um *script* de testes que, via Telnet, acessa os IED para alterar uma variável interna do IED. Essa variável [§], ao ser alterada, dispara uma sequência de eventos, que leva parte de todos os *datasets* GOOSE de fundo e do *dataset* de prova a mudar de estado a cada 4 ms (Figura B.6 do Apêndice). Como a primeira mensagem de retransmissão é gerada somente após esse tempo, não há espaço para a segunda mensagem da retransmissão ser gerada. Isso garante que a quantidade de mensagens GOOSE geradas seja igual a quantidade de eventos, permitindo que o SER do IED seja utilizado para os cálculos de latência. Essa metodologia para observação de perda de pacotes e latência é importante para evitar falsos positivos nestas medidas, já que o mecanismo de retransmissão da mensagem GOOSE envia a mesma mensagem várias vezes, e, caso a primeira não seja recebida, a próxima mensagem (de retransmissão) será recebida. Assim, em caso de perda, a mensagem de retransmissão é recebida e marcada no

[§]O IED de teste possui variáveis internas (que podem ser alteradas remotamente ou não) que são utilizadas em lógicas de controle. Com isso, pode-se escolher uma para servir de entrada para a lógica, sendo essa alterada remotamente, e utilizar uma de saída, resultado da lógica, para ser colocada dentro do *dataset* de interesse.

SER, não sendo possível expurgar se foi uma mensagem de retransmissão ou não.

6.2.4.1 Latência da GOOSE em Condições Normais

A latência foi obtida subtraindo-se a estampa de tempo em que a mensagem foi ativada no SER de destino do SER de origem, que estavam sincronizados por meio de GPS. Foram gerados 500 eventos espaçados de 4 ms e realizadas 20 rodadas para cada quantidade de fluxos GOOSE de fundo. Na primeira rodada, além do *dataset* de prova entre os IEDs 421, um IED 751A de cada subestação estava gerando tráfego de fundo, caracterizado por um *dataset* GOOSE, de 1200 bytes, por IED. Na segunda rodada, dois de cada subestação, e assim por diante até todos estarem gerando tráfego de fundo. Para o PRP, o tráfego de fundo que seria gerado pelos IEDs 751A adjacentes foi gerado pelo 421, já que os IED 751A não possuem PRP.

É importante notar que, como o valor foi coletado do sequencial de eventos, a latência total inclui os tempos de processamento dos dispositivos de origem e destino.

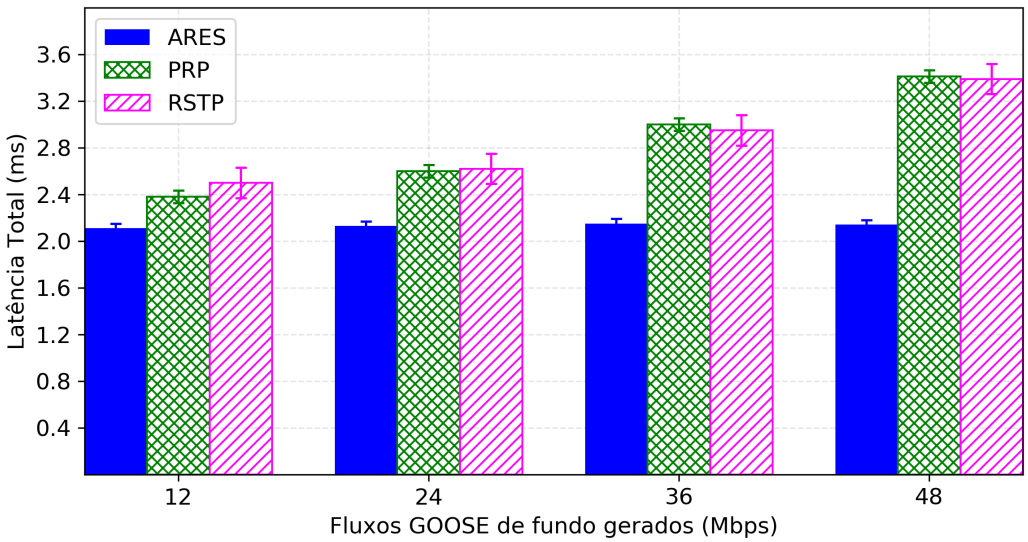


Figura 6.17: Latência total na rede, incluindo o processamento do *frame* nos IEDs.

O gráfico da Figura 6.17 mostra a latência para os três mecanismos testados, com intervalo de confiança de 95%. Verifica-se que a latência dos três é bastante parecida, ficando entre 2,11 e 3,41 ms. O lado do anel que estava desativado pelo RSTP não passava pelos IEDs de prova, o que deixou a quantidade de saltos iguais. Como o PRP recebe o primeiro *frame* pela topologia linear de dois saltos, o caminho é basicamente o mesmo. Verifica-se que, com o aumento do tráfego de fundo, a latência para o PRP e para o RSTP também aumenta. A diferença entre o ARES e as demais soluções pode estar relacionada aos *switches* utilizados no teste, que são de modelos e tecnologias diferentes (SDN e *switch* Ethernet tradicional), além do próprio tráfego reduzido, já que o ARES

possui uma carga de rede reduzida quando comparado ao RSTP e ao PRP. A avaliação desta carga é detalhada na Seção 6.2.4.2.

6.2.4.2 Carga na Rede em Condições Normais

Para a segunda parte dos testes, a carga total da rede foi medida com o Wireshark. Para tanto, todo o tráfego que chegava ao IEDs era direcionado para um computador. Foram avaliados três cenários:

1. Carga da rede do RSTP X ARES: Para este cenário, o *dataset* configurado permaneceu o mesmo, 1200 bytes, com 250 eventos por segundo. O PRP não foi avaliado neste cenário, pois não era possível reproduzir o estudo de caso utilizando o PRP com os equipamentos disponíveis;

2. Carga da rede com RSTP com VLAN X ARES: Para este cenário, o *dataset* configurado permaneceu o mesmo, 1200 bytes, com 250 eventos por segundo. O tráfego da WAN foi isolado do tráfego da LAN utilizando duas VLANs distintas. O PRP não foi avaliado neste cenário, pois não era possível reproduzir o estudo de caso utilizando o PRP com os equipamentos disponíveis;

3. Carga da rede com um fluxo. RSTP X ARES X PRP: Para este cenário, todos os IEDs 751A foram desligados. Apenas um *dataset* GOOSE, do IED 421 A para o IED 421 B permaneceu configurado.

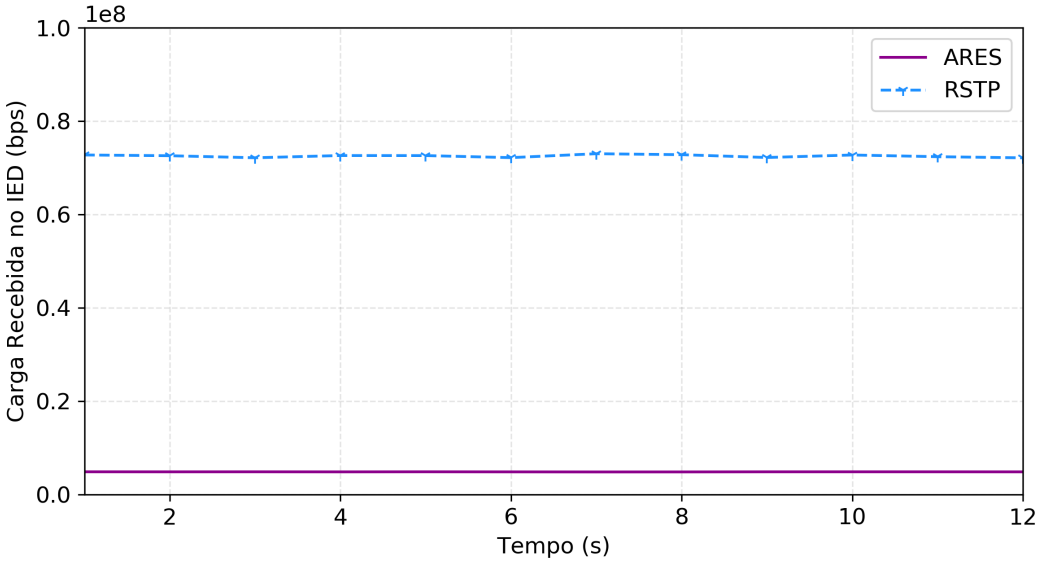


Figura 6.18: Carga recebida no IED assinante com RSTP e com a rede configurada baseada no ARES.

Conforme mostra o gráfico da Figura 6.18, o tráfego da rede com RSTP, quando comparado ao ARES, é muito mais alto, ultrapassando 70% da banda, o que equivale a

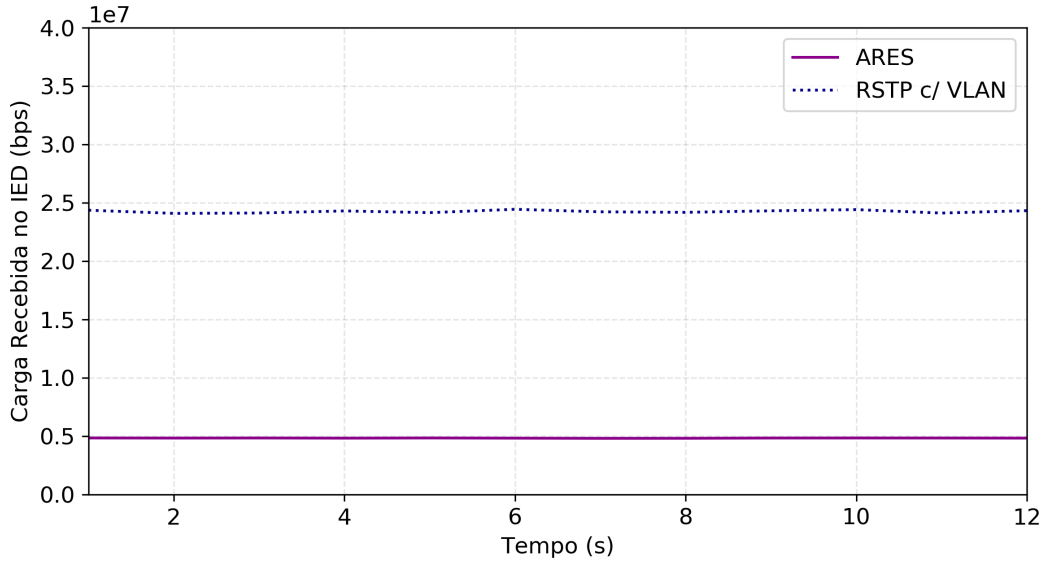
70Mbps. O anel em camada dois apresenta essa característica, pois o tráfego GOOSE acaba inundando todo o anel em uma rede tradicional. Mesmo sendo um tráfego relativamente mais baixo que o experimentado na prática (4 IEDs por subestação, enviando apenas uma mensagem GOOSE), nota-se que a carga recebida nos IEDs de prova é muito maior quando utilizado o RSTP, o que pode resultar, inclusive, no aumento do processamento dos mesmos. Este cenário mostra a importância de um método de configuração que permita que árvores *multicast* de camada dois sejam configuradas para não onerar a rede de comunicação com transmissões desnecessárias. Apesar do PRP não ter sido avaliado nesse cenário, percebe-se que a duplicação de tráfego gerada pelo PRP, neste cenário, seria um problema ainda maior.

Como o ARES, já conta com o isolamento de tráfego por padrão, a rede com RSTP foi reconfigurada para trabalhar com VLANs, de forma a garantir o isolamento do tráfego da WAN. Como as mensagens GOOSE saem marcadas do IED, as mensagens de teleproteção foram colocados em uma VLAN específica, diferente das demais. Desta forma, a rede RSTP configurada com VLANS estava liberando para a rede em anel somente o tráfego "WAN".

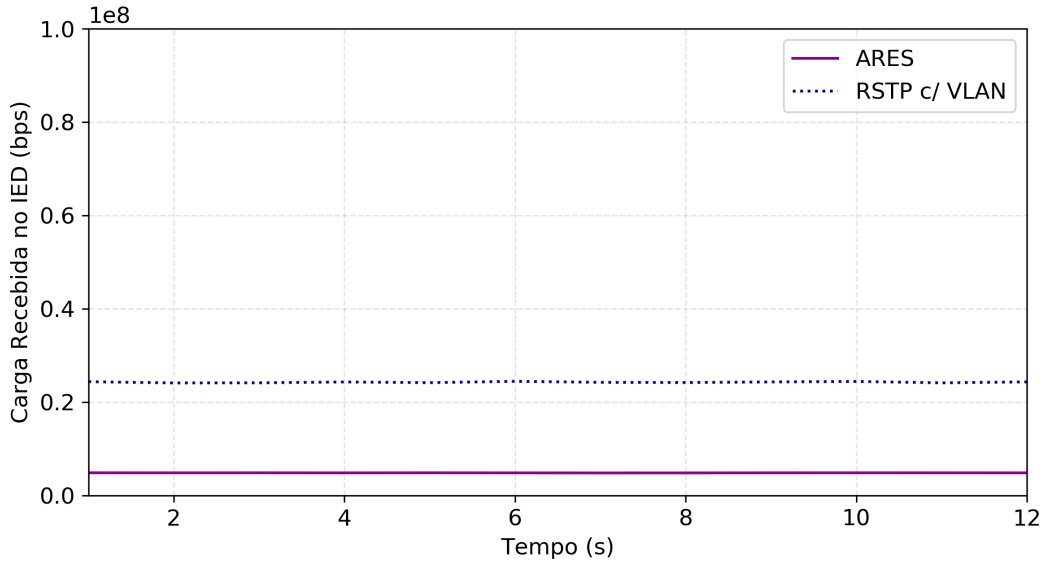
Conforme ilustram os gráficos da Figura 6.19, o tráfego do RSTP com VLAN ($\approx$ 24 *Mbps*), mesmo que muito menor que o cenário sem VLAN, ainda é maior do que o tráfego do ARES ($\approx 4,8$ *Mbps*). Isto ocorre, pois, mesmo tendo exatamente o mesmo tráfego sendo gerado, o RSTP com VLAN não impede que as mensagens GOOSE da WAN cheguem para o IED 421 B. Já o ARES, provisiona o fluxo por demanda, utilizando uma árvore *muticast*, de forma que apenas o tráfego de interesse seja recebido no IED 421 B. Com os fluxos provisionados com o ARES, mesmo sendo um fluxo *multicast* de camada dois, a mensagem é enviada apenas para o(s) IED(s) de destino, sem inundar a rede. Desta forma, com o ARES, o IED 421 B recebe apenas a mensagem de teleproteção direcionada para ele, a da subestação A e a da subestação B, enquanto que com o RSTP, o IED recebe todo o tráfego de teleproteção do anel.

Para que este isolamento seja possível também no RSTP, com esta granularidade, seria necessário que cada mensagem GOOSE fosse criada em uma VLAN diferente, de forma a criar uma espécie de "canal" para o tráfego seguir utilizando VLANs. Apesar de possível, é uma solução que torna o projeto da rede de comunicação muito complexo, tanto para implantação quanto para manutenção. Outra solução para o RSTP seria o uso de protocolos para montar a árvore *multicast* em camada dois, como o *GARP Multicast Registration Protocol* (GMRP). No entanto, estes protocolos precisam que os IEDs sejam capazes de enviar mensagens *join* e *leave*, além de recursos da camada três.

O terceiro cenário tem como objetivo avaliar a carga na rede destes mecanismos, incluindo o PRP. Para isso, apenas um fluxo foi deixado ativo de forma que este fosse o cenário mais neutro para os três mecanismos. Como apenas um fluxo é gerado, o problema relacionado a inundação de mensagens verificada no PRP e no RSTP, não influenciará nos



(a) RSTP com VLAN x ARES



(b) RSTP x RSTP com VLAN x ARES

Figura 6.19: Carga recebida no IED assinante.

testes. Novamente foram gerados 250 eventos por segundo com o mesmo *dataset*.

Neste cenário, conforme mostra a Figura 6.20, o tráfego no RSTP e no ARES é praticamente o mesmo, enquanto que com o PRP, é um pouco mais que o dobro. Ressalta-se que o tráfego parecido é devido a geração de apenas um fluxo, e da medida ser realizada no IED de destino. A rede com PRP e RSTP entregou esse fluxo para todos os outros IEDs na rede, enquanto que o ARES, apenas para o IED de interesse. A duplicação do tráfego já era esperada devido ao próprio funcionamento do PRP. No entanto, verificou-se também

que, além da duplicação do tráfego, existem pacotes de supervisão do PRP (Figura B.7(b) no Apêndice) e alguns *frames* que são duplicados mais de uma vez (Figura B.7(a) no Apêndice), tornando o tráfego maior do que apenas duas vezes o gerado pelo RSTP ou pelo ARES.

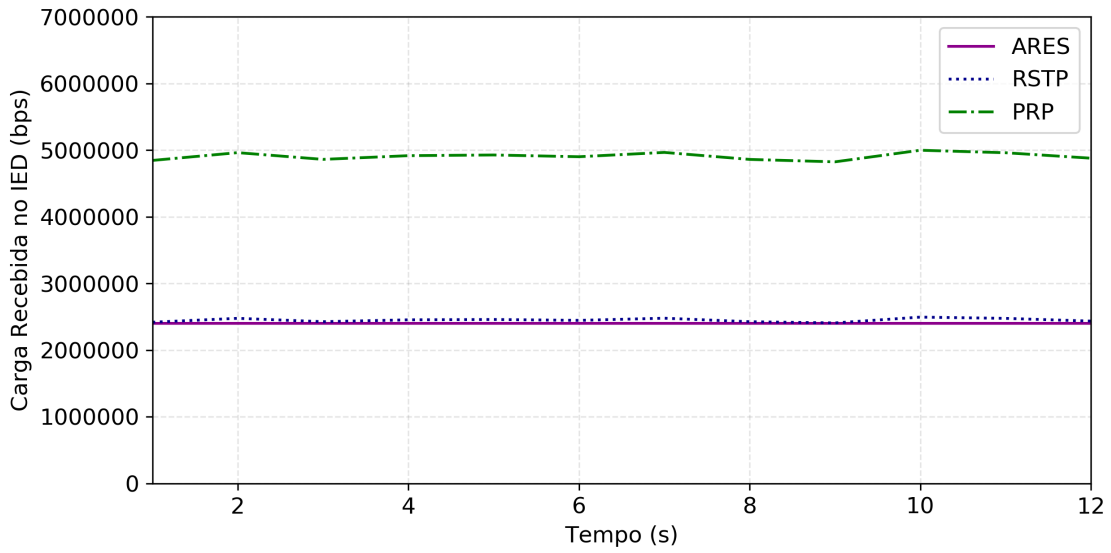


Figura 6.20: Carga recebida no IED assinante considerando apenas um *dataset* configurado.

A carga na rede de comunicação deve ser observada, já que, como verificado na Seção 6.2.4.1, o aumento de tráfego influencia na latência da rede.

6.2.4.3 Carga e latência na Rede durante Falhas de Comunicação

O terceiro teste teve como objetivo avaliar o comportamento dos mecanismos mesmo durante as falhas na rede de comunicação. Para os primeiros testem foram realizadas duas falhas de comunicação permanentes, em sequência, durante os 3 segundos de teste. A Figura 6.21 ilustra o resultado. Como os testes foram feitos em momentos diferentes, o tráfego foi ajustado na primeira falha para comparação.

A Figura 6.21 mostra que, durante a primeira falha, o PRP e o ARES continuam a entregar as mensagens no destino, sem perda da informação. Já na segunda falha, devido a topologia em anel só permitir um caminho *backup*, os dois mecanismos não entregam mais o tráfego ao destino. Com o RSTP, na primeira falha, o IED passa aproximadamente 300 ms sem receber o tráfego, o que é um tempo extremamente alto para uma infraestrutura crítica [179].

A configuração padrão das portas de comunicação dos *switches* é em auto-negociação. Para tentar reduzir o tempo de recuperação do RSTP, a rede foi reconfigurada para que as portas ficassem fixadas em 100Mbps. O gráfico da Figura 6.22 mostra os valores encontrados, onde a configuração da porta reduziu para quase 10% do valor o tempo de

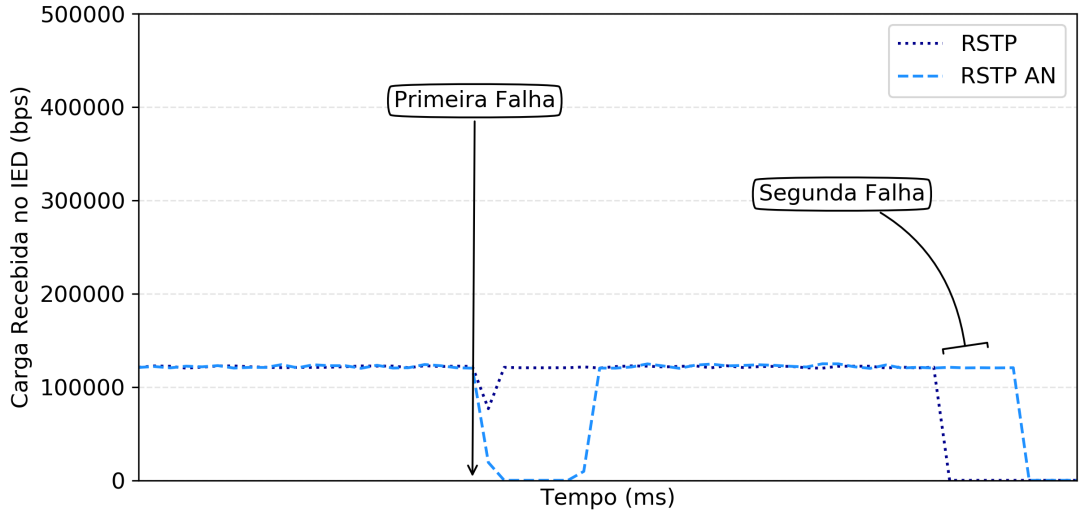


Figura 6.21: Carga na rede durante a execução de duas falhas em sequência. ARES x PRP x RSTP com a porta de comunicação em Auto Negociação (AN).

recuperação em caso de falha. Para os testes com o ARES, por ser um *switch* SDN, a velocidade das portas é fixada por padrão. O gráfico da Figura 6.22 resume os tempos de latência total, incluindo o processamento dos IEDs.

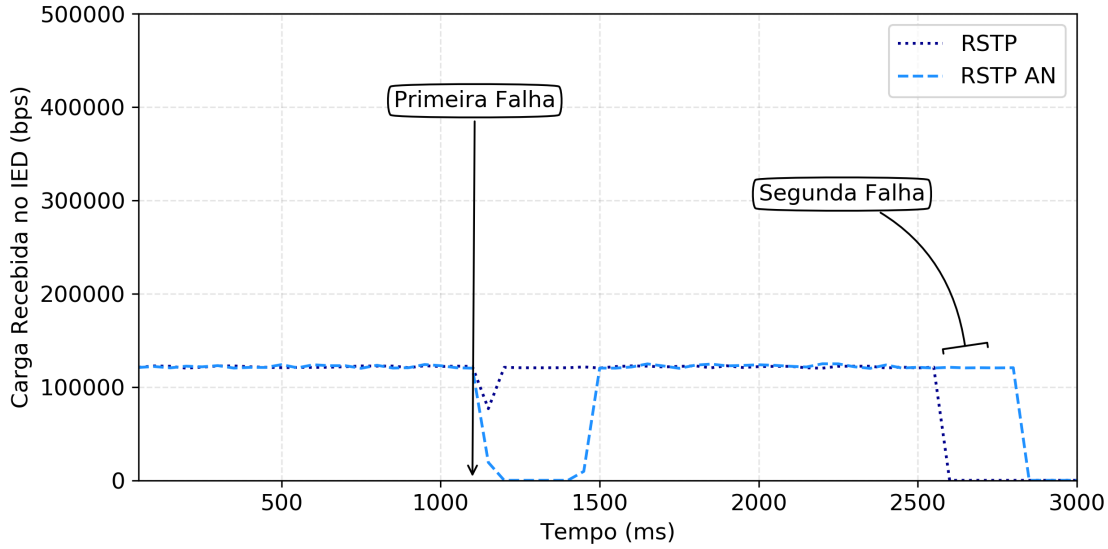


Figura 6.22: Carga na rede de comunicação configurada com RSTP durante a execução de duas falhas.

Como foi verificado, a configuração da porta em auto-negociação onera bastante o tempo de recuperação. Com as portas fixadas em 100Mbps, o tempo de recuperação caiu para $\approx 30ms$. Mesmo considerando que esse tempo inclui o processamento dos dispositivos finais, é um valor ainda bem alto para uma infraestrutura crítica.

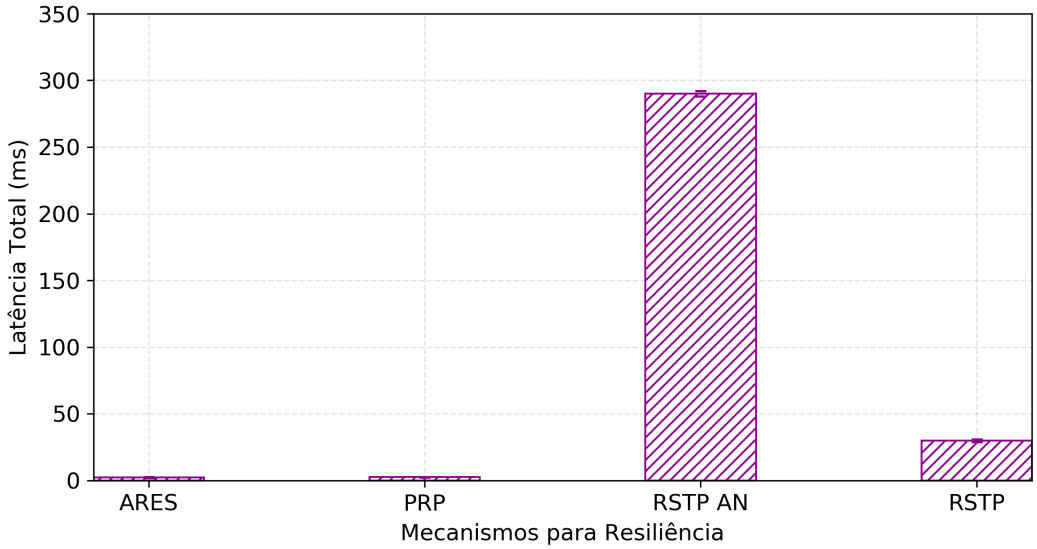


Figura 6.23: Latência total na ocorrência de uma falha de comunicação. Comparação entre os mecanismos.

Os testes de carga e de latência durante falhas na rede de comunicação mostraram que a carga do PRP é consideravelmente alta quando comparada ao RSTP ou ao ARES. No entanto, verificou-se também que a latência do RSTP durante uma falha é maior que nos demais mecanismos estudados, pois, na ocorrência de apenas uma falha na rede de comunicação, esta não é percebida pelos IEDs quando utilizam o PRP ou o ARES. Destaca-se que o ARES foi o único método que não onera a rede de comunicação com alto tráfego e mantém o tempo de recuperação transparente para os dispositivos finais.

Outro ponto importante, é que o ARES recupera para quantos caminhos secundários existirem. O PRP e o RSTP (versão mais rápida, em anel) só possuem um caminho secundário. Para os testes não serem tendenciosos, os resultados apresentados foram realizados para uma topologia com apenas um caminho secundário, a topologia em anel.

No entanto, com apenas um enlace a mais acrescentando na topologia, de forma a criar mais uma opção *backup* a ser usada pelo ARES, este seria resiliente a mais de uma falha, diferente dos outros mecanismos estudados. Por este motivo, optou por avaliar também este comportamento de forma a verificar a resiliência do *framework*. Para tanto, a topologia foi alterada conforme Figura 6.24, com acréscimo de apenas mais um enlace. O *switch* da subestação A foi conectado ao *switch* da C, de forma a criar mais uma opção *backup*. Foram avaliados o ARES e o RSTP com as portas fixadas em 100Mbps (melhor resultado encontrado). O PRP não pode ser testado já que os IEDs só possuem duas portas para duplicação do tráfego, não sendo possível realizar a triplicação do tráfego para uma terceira rede.

O gráfico da Figura 6.25 ilustra o comportamento da rede para a seguinte sequência de falhas:

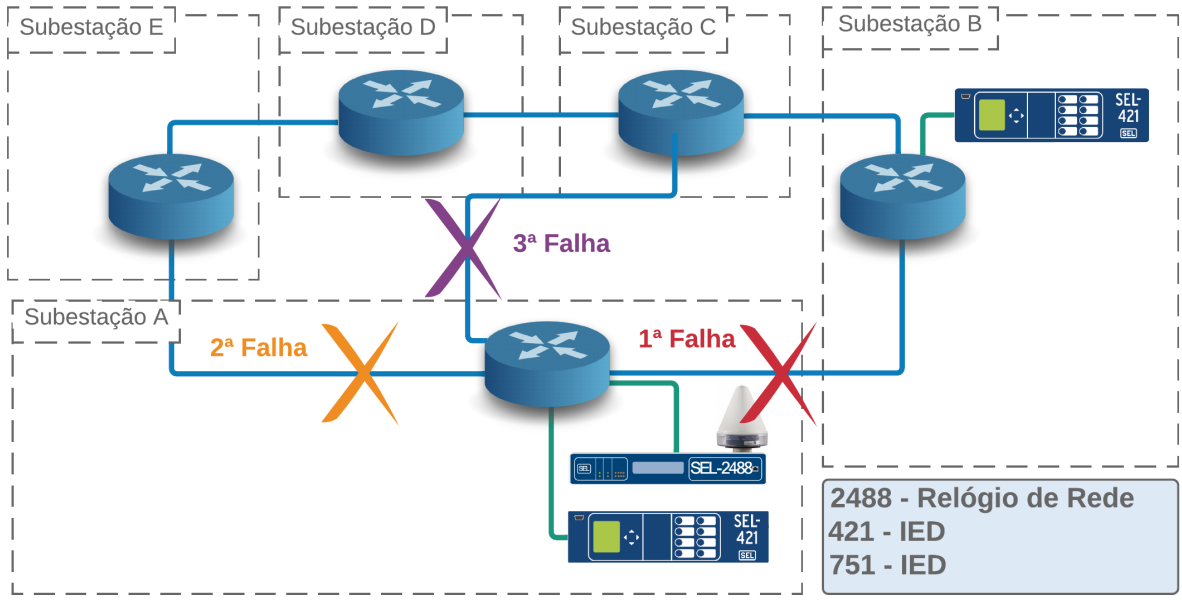


Figura 6.24: Topologia dos testes para realização de três falhas. Comunicação entre IEDs 421 com apenas um fluxo GOOSE. Três falhas sendo a primeira temporária.

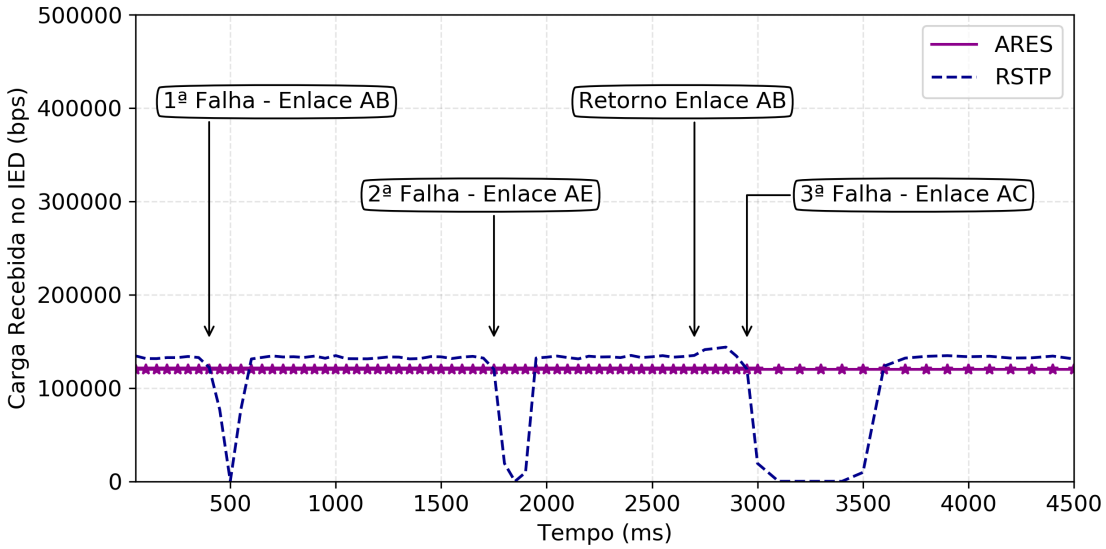


Figura 6.25: Carga na rede de comunicação configurada com RSTP e ARES durante a execução de três falhas.

- 1ª falha: falha temporária no enlace entre as subestações A e B aproximadamente no tempo 400 ms. Enlace reconectado após 2300 ms, aproximadamente no tempo 2700 ms;
- 2ª falha: falha no enlace entre as subestações A e E aproximadamente no tempo 1700 ms;
- 3ª falha: falha permanente no enlace entre as subestações A e C aproximadamente

no tempo 2800 ms;

Verifica-se no gráfico, que na ocorrência da primeira e da segunda falha, o RSTP demora mais tempo para recuperar do que nos testes anteriores. Este comportamento já era esperado já que topologia, apesar de pequena, possui mais de um ciclo, o que não ocorre na topologia em anel (apenas um ciclo). Com isso, o algoritmo de *spanning tree* precisa lidar com uma árvore mais complexa do que a árvore da topologia em anel, que é bastante simples. Assim, as informações de controle podem demorar mais a chegar. Nota-se também que na terceira falha o tempo é demasiadamente maior. O enlace AB retornou milissegundos antes desta falha onde verifica-se o pequeno aumento do tráfego de controle. Possivelmente, o processamento deste tráfego de controle pelos *switches* pode ter interferido no tempo de recomposição da queda do enlace AC em seguida, justificando o tempo consideravelmente maior. Esse comportamento também enfatiza o porquê do uso preferencial da topologia em anel nas subestações, quanto é utilizado o RSTP.

O ARES foi transparente durante todo o tempo, mantendo a rede em funcionamento durante as três falhas. Isso foi possível pois sempre existia uma opção secundária durante a falha, já que o enlace AB retornou antes da falha no enlace ED. Caso essa opção não existisse, como ocorria nos testes anteriores, não seria possível efetuar a recuperação.

Ressalta-se que o PRP, para ser implementado precisaria ter a topologia duplicada e só seria resiliente à falha em uma das duas redes.

6.3 Testes de Desempenho – Ambiente Emulado

Os tempos de latência medidos em um ambiente real, são calculados com base no SER dos IEDs. Esse cálculo inclui o tempo de processamento no dispositivo e o ciclo de processamento. Como esses valores não podem ser expurgados, esta seção apresenta testes emulados para a avaliação do ARES. O tempo que o componente de recuperação de falhas demorou para identificar a falha e restabelecer a comunicação foi medido. Tanto o algoritmo para *switches* OpenFlow 1.0, sem o mecanismo de *fast failover*, quanto do OpenFlow 1.3, com o *fast failover*, foram avaliados. Com o propósito de definir um limiar para os tempos encontrados com o ARES para recuperação de falhas, foi realizada uma comparação com os tempos do RSTP em uma versão melhorada, desenvolvida especialmente para subestações com requisitos temporais rígidos [155], que possui valores menores que os medidos nos testes anteriores. O PRP não foi avaliado pois o gerador de tráfego utilizado não possui o PRP implementado.

O ambiente de implementação, descrito a seguir, foi o mesmo para todos os testes. Os experimentos realizados e a análise de resultados estão descritos na Seção 6.3.2.

6.3.1 Cenário de Testes

O ambiente de implementação foi emulado por meio de virtualização em um notebook com processador Intel Core i5-3210M, e 4GB de memória RAM. Os testes foram realizados com três instâncias de máquinas virtuais simultâneas, cada uma delas com uma CPU virtual, 1024 MB de memória e executando o sistema operacional Ubuntu 11.10. O componente ARES foi desenvolvido em python utilizando o controlador RYU, o OpenFlow 1.3 e o OpenFlow 1.0.

Os experimentos foram emulados usando o Mininet na Versão 2.2.1 [111], criando assim uma rede virtual realista, executando kernel real, *switch* e código de aplicação em uma única máquina [111].

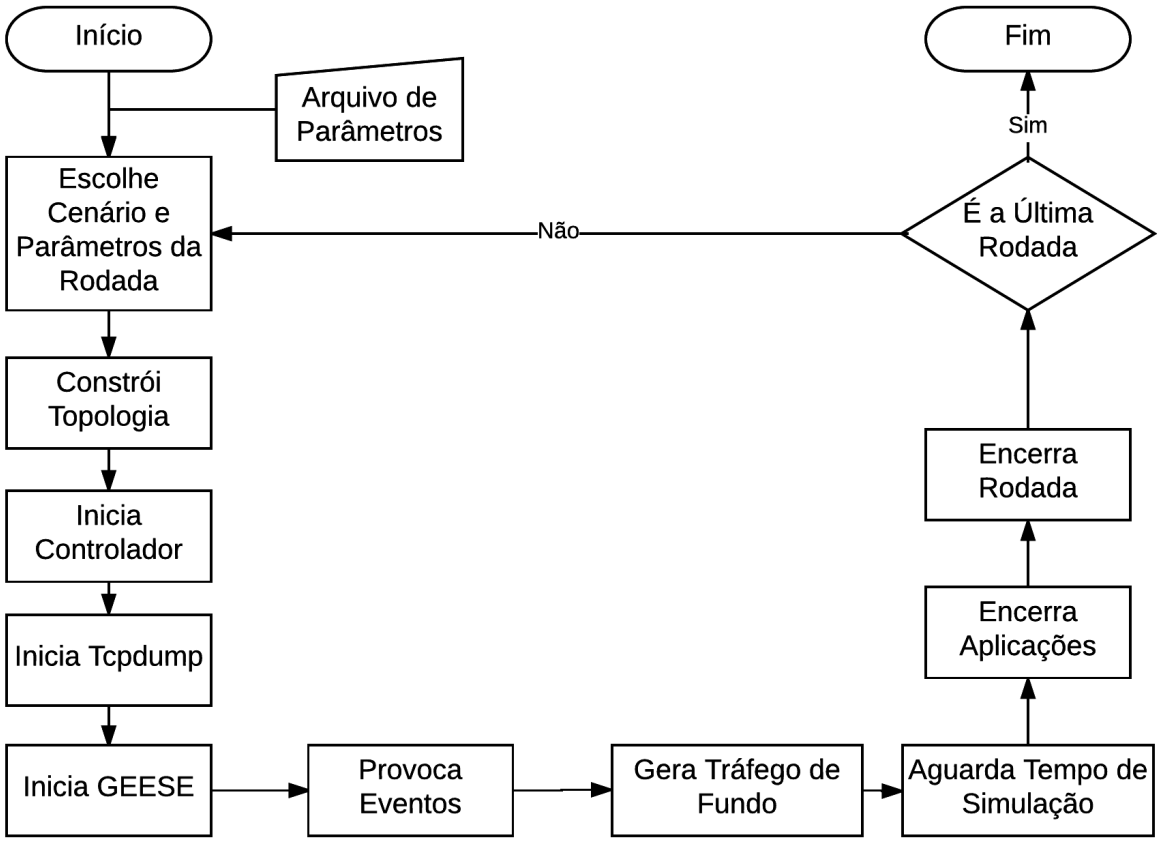


Figura 6.26: Fluxograma do *script* de testes do Mininet.

Foi criado um módulo no Mininet que constrói topologias, todas distribuindo os dispositivos do plano de energia uniformemente na rede. Este módulo também contém a classe que chama os componentes do ARES para controlar a rede. Como apresentado na Figura 6.26, foi desenvolvido um *script* de testes no Mininet que é responsável por gerar todos os nós e interconectá-los, assim como por inicializar o controlador e coletar os resultados. Para emular o tráfego de dispositivos finais, foi utilizado o gerador GEESE [126],

um gerador de tráfego IEC 61850 desenvolvido para reproduzir fielmente o tráfego GOOSE.

Nos testes, o publicador do grupo *multicast* e os receptores são escolhidos de forma aleatória seguindo uma distribuição uniforme para, desta forma, obter resultados não tendenciosos. As medidas extraídas envolvem atraso e tempo para restabelecimento em caso de falhas. O tcpdump foi usado para capturar os pacotes, permitindo que os dados fossem armazenados para serem posteriormente tratados.

6.3.2 Avaliação e Resultados

Foram considerados, para todos os testes realizados, enlaces de 100 Mbps, padronizados na norma IEC 61850, quadros GOOSE reais gerados pelo GEESE [126] com aproximadamente 160 bytes e um intervalo de confiança de 95% nos resultados. A duração dos experimentos foi de 100 segundos para cada rodada, incluindo, neste tempo, a estabilidade da rede, a configuração dos fluxos, a troca de mensagens e o tempo da simulação. Foi variada a quantidade de *switches* na rede, que continha no mínimo dois dispositivos.

As topologias escolhidas foram a topologia em malha e anel. A topologia em anel é bastante comum em sistemas elétricos por permitir que o RSTP recupere o anel em um tempo menor do que o padrão. A topologia em malha também foi testada por possuir diversos caminhos entre origem e destino. Esses valores são resumidos na Tabela 6.4.

Tabela 6.4: Parâmetros usados no experimento.

Enlaces	100 Mbps
Quadros GOOSE	160 bytes
Intervalo de confiança	95 %
Topologias	Anel e Malha
Duração do experimento	100 segundos

Com o propósito de definir um limiar para os tempos encontrados com o ARES para recuperação de falhas, a Figura 6.27 também ilustra os melhores tempos encontrados por Pustylnik et al. [155] com o RSTP melhorado. Essa versão do RSTP é uma versão aperfeiçoada, que funciona apenas para rede em anel, com enfoque de diminuir ao máximo os tempos encontrados. Ressalta-se que os valores descritos no gráfico foram os melhores tempos encontrados pelos autores. Por esse motivo, os valores foram plotados apenas no gráfico da Figura 6.27, já que se trata da mesma topologia usada pelos autores.

Ressalta-se que o tempo de recuperação medido engloba o tempo total para o *switch* detectar a falha e agir. Os tempos não foram separados, já que o tempo para detectar a falha depende do mecanismo em uso nos *switches*, como protocolos para detecção dessas falhas ou ausência de sinal na porta. No entanto, os tempos que estão sendo comparados no gráfico também são tempos totais medidos pelos autores.

A Figura 6.28 apresenta os tempos de recuperação encontrados para uma topologia em malha, logo, não é possível realizar a comparação com o RSTP melhorado, já que este foi desenvolvido para topologias em anel.

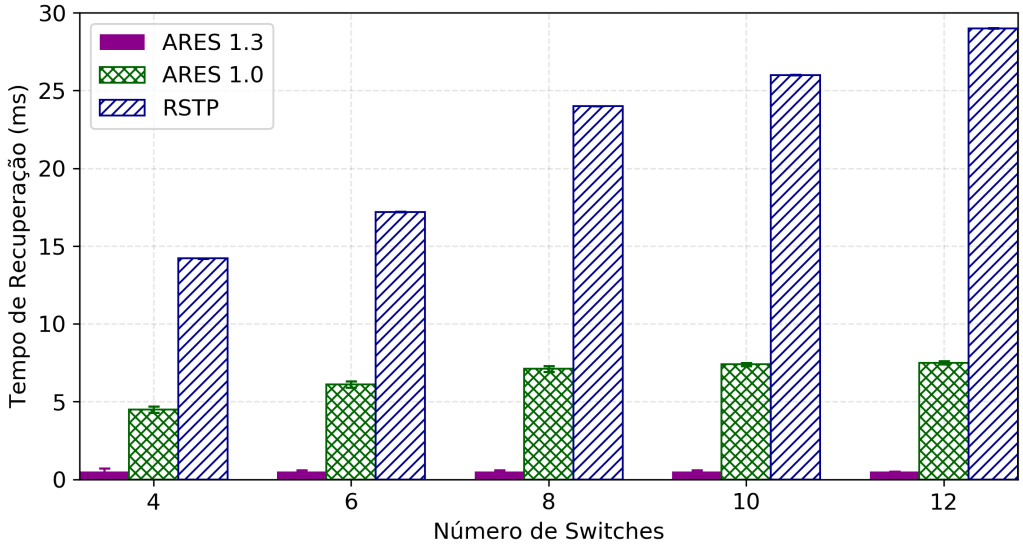


Figura 6.27: Tempo de recomposição em uma topologia em anel para o componente ARES `Recuperação de Falhas`.

Observa-se nas Figuras 6.27 e 6.28 que o tempo de recuperação em caso de falhas não excedeu 8 ms na rede controlada pelo ARES com o OpenFlow 1.0, indicado como ARES 1.0 nos gráficos. Isso mostra que o ARES, mesmo com uma versão mais antiga do OpenFlow, satisfaz as exigências temporais rígidas para recuperação da rede de comunicação das redes elétricas inteligentes, mostrando tempos melhores do que o RSTP, que apresenta cerca de 15 ms como seu tempo mais rápido na versão melhorada.

O atraso do RSTP é explicado devido à característica das redes tradicionais e seu plano de controle distribuído, onde uma falha na rede resulta em uma troca de mensagens de controle na rede antes de estabelecer um novo caminho. E todo este processo requer tempo. O valor de 8 ms para o ARES com OpenFlow 1.0 é devido ao comportamento reativo do *switch* OpenFlow 1.0 para tratamento de falhas. Após uma falha na rede, os *switches* enviam mensagens de aviso para o controlador para calcular um novo caminho. Assim, depois que o controlador recebe o evento de falha, ele calcula o novo caminho e configura todos os *switches*. Como o caminho de backup não é pré-configurado no *switch*, o tempo de recuperação é menor que a rede tradicional, no entanto ainda maior que o encontrado com o componente desenvolvido com o auxílio do recurso de *fast failover* (ARES com OpenFlow 1.3, indicado como ARES 1.3).

Observa-se na Figura 6.28 que o ARES na versão 1.3 do OpenFlow apresentou um tempo de recuperação excelente que não excedeu 0.6 ms. Um comportamento importante, observado no gráfico da Figura 6.28, é que mesmo com o aumento dos switches na rede,

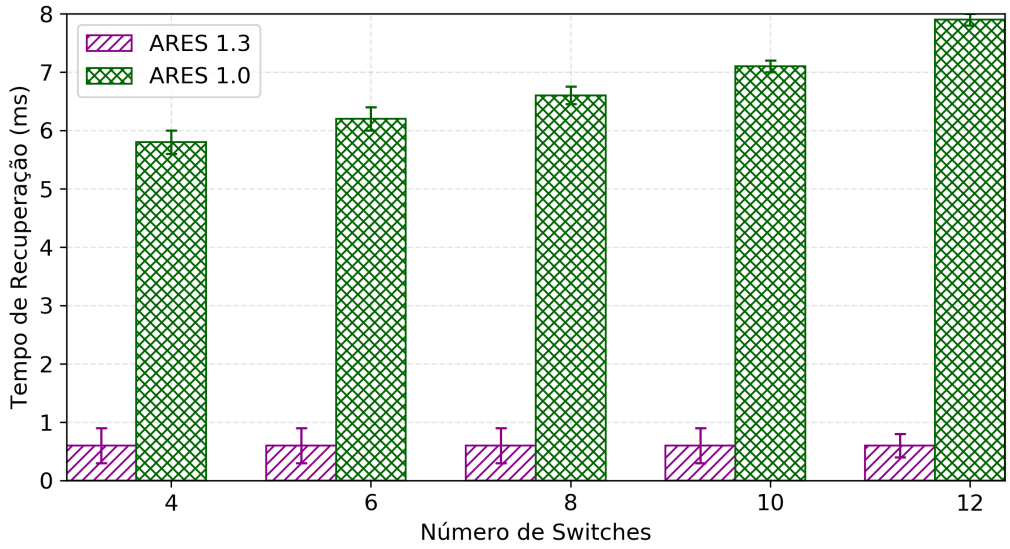


Figura 6.28: Tempo de recomposição em uma topologia malha para o componente ARES. `Recuperação de Falhas`.

o tempo não aumenta. Como a escala das redes elétricas é muito maior do que em subestações, uma solução que não dependa da quantidade de switches na rede se torna bastante interessante. Isso se deve à natureza proativa das tabelas de grupo do OpenFlow e dos algoritmos de recuperação de falhas do ARES. Assim, os tempos de recuperação dependem apenas do tempo para que o *switch* perceba que a opção principal está inativa mais o tempo de processamento do *switch* para comutar para a próxima opção ativa. Ressalta-se que esse resultado é muito importante no cenário das redes elétricas inteligentes, pois mostra que o ARES baseado no OpenFlow 1.3 não depende do número de *switches* da rede, sugerindo uma solução possivelmente escalável. Soluções como o RSTP têm o tempo elevado com o aumento do número de *switches*.

Outra análise importante é mostrada na Figura 6.29. A Figura 6.29 mostra o atraso médio para a entrega de uma mensagem GOOSE a todos os destinos do grupo *multicast* numa topologia em anel com 12 *switches*, cenário com maior atraso que o anterior, durante uma falha na rede de comunicação.

Cerca de 60 segundos após o início da emulação, um enlace é aleatoriamente desconectado usando o comando *ifdown* do Linux. Observa-se que o atraso médio para entregar a mensagem da origem para todos os destinatários não ultrapassou 2 ms na rede controlada pela ARES. Isso mostra que ARES atende à rígida restrição de tempo especificada por [80, 179] (3ms para mensagens GOOSE), mesmo quando ocorre uma falha de rede de comunicação.

Assim, o ARES apresenta algumas vantagens significativas, pois é independente da topologia, não duplica pacotes na rede, evitando sobrecarga, não tem a necessidade de ser implementado nos dispositivos do plano de energia e não necessita de duplicação dos

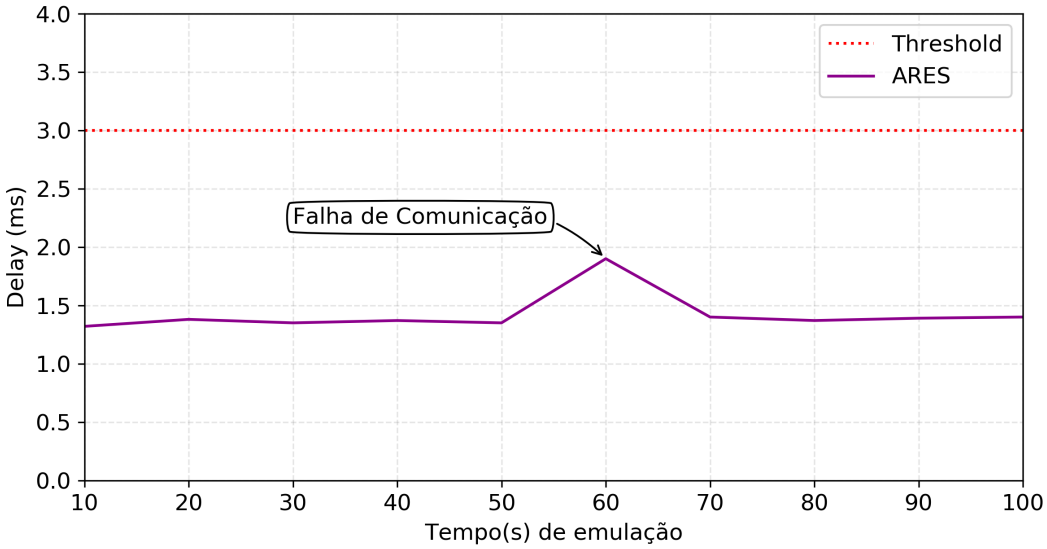


Figura 6.29: Atraso na rede durante uma falha, assumindo uma topologia em anel com 12 *switches*.

componentes da rede. Porém, ressalta-se o HSR, o PRP e o RSTP são mais usados e testados em redes de comunicação de subestações já em produção do que soluções com SDN, o que é uma vantagem se comparados ao ARES.

6.4 Considerações sobre os Resultados

Os testes mostraram que o mapeamento da rede de comunicação, dos dispositivos finais e de suas características é possível com a tecnologia existente, quando de acordo com o *framework* ARES. Desta forma, novas aplicações de energia com mapeamento dinâmico podem ser criadas, podendo, além de gerenciamento, realizar o controle dos dispositivos. A ausência da necessidade do mapeamento dos dispositivos de forma manual no SCADA, além da simplicidade, reduz a possibilidade de erro humano, característica essencial para o setor elétrico.

O provisionamento dos fluxos granular, de acordo com cada *dataset*, também se mostrou eficiente, de forma que a rede de comunicação é alocada dinamicamente de acordo com a configuração dos IEDs de interesse. Os dados coletados a partir de dispositivos baseados na norma IEC 61850, com os serviços MMS, são suficientes para a realização do provisionamento e do mapeamento dos dispositivos. Com isso, mostrou-se que, se a rede é baseada em OpenFlow e os dispositivos baseados em IEC 61850, o provisionamento dinâmico pode ser realizado.

Os testes mostraram que o provisionamento dos fluxos de acordo com cada *dataset* traz, além da flexibilidade, uma melhora no desempenho. Verificou-se que a alocação dos

recursos de acordo com *datasets* ativos permite um redução grande no tráfego, que resulta, inclusive, em uma latência menor do que com outros métodos.

Os testes realizados em ambiente real mostraram que a rede de comunicação baseada no *framework* é capaz de recuperar-se de uma falha de forma transparente para os dispositivos finais e sem aumentar a carga da rede de comunicação. De forma geral, os métodos usados para recuperação de falha podem ser separados em duas abordagens distintas, redundância com *backup* e redundância paralela.

Quando a redundância com *backup* é utilizada, existe uma opção secundária para o fluxo seguir em caso de falha. Os pacotes são enviados sem duplicatas de forma que, em caso de falha, o dispositivo precisa reconhecer que está em falha. Essa abordagem resulta em, mesmo que mínimo, um tempo de inatividade, pois depende diretamente do tempo que o dispositivo precisa para reconhecer a falha. Após reconhecida a falha, tem-se o tempo para reestabelecimento da mesma. Os testes com o RSTP mostraram que esse tempo de reconhecimento é crucial para o desempenho da rede. A necessidade de redução deste tempo ficou evidente, onde a simples configuração fixa da porta de comunicação fez com que esse tempo reduza para quase 10% do valor total, $\approx 300ms$ para $\approx 30ms$.

Além disso, os mecanismos de redundância com *backup* podem ser proativos ou reativos. O ARES funciona com base no mecanismo proativo, onde os caminhos *backup* são calculados/configurados antes de ocorrer a falha. O tempo de restabelecimento, neste caso, depende apenas do tempo de comutação do dispositivo para o caminho alternativo quando utilizando o *fast-failover*. Quando é necessário que um evento de falha seja gerado, esse tempo depende apenas do recebimento do evento e do provisionamento do enlace. Com o uso do grupo *fast failover*, o ARES atingiu menos de 0,61 milisegundos de tempo de recuperação no cenário emulado avaliado. Além disso, mesmo com o uso de versões antigas do OpenFlow, sem o *fast-failover*, de forma que, mesmo com o caminho pré-calculado o controlador precisa receber um evento e provisionar o enlace *backup*, o ARES mostrou melhores resultados que o RSTP. Com o ARES utilizando o *fast failover*, os tempos de recuperação dependem apenas do processamento do *switch*, mantendo os tempo lineares mesmo com o aumento dos *switches* na rede. Isto ocorre pois, os *switches* não precisam trocar informações com o controlador, nem com outros *switches*, para descobrir e aplicar um caminho *backup*.

Além da forma proativa, tem-se o mecanismo reativo, onde os caminhos *backup* são calculados/configurados após um evento de falha. O tempo de restabelecimento depende do tempo de comutação dos dispositivos envolvidos mais o tempo de cálculo do novo caminho, e o tempo de configuração destes. O RSTP funcionada de forma reativa, assim como muitas propostas SDN da literatura. Porém, como discutido em [119], para as redes elétricas inteligentes, uma proposta reativa, mesmo que SDN, aumenta consideravelmente os tempos de resposta, não sendo interessante para o setor elétrico.

Por fim, tem-se o método de redundância paralela, onde os dados são transmitidos em

cópia simultaneamente por múltiplos caminhos. Com isso o receptor espera receber uma cópia desse pacote por um desses caminhos. Essa abordagem elimina qualquer tempo de inatividade desde que a quantidade de caminhos afetados seja menor que a quantidade de caminhos disponibilizados. Os exemplos de uso destes mecanismos são o PRP e o HSR. Como o PRP funciona com duas redes distintas e similares, poderia, com melhora no desempenho, ser utilizado em conjunto com SDN. Além disso, o ARES, por ser baseado em SDN, poderia utilizar mecanismos de redundância paralela sem a necessidade de uso do PRP.

Para todos os casos, os caminhos podem ser disjuntos em nós e/ou enlaces. De forma geral, dois caminhos distintos podem ser totalmente disjuntos ou de enlace ou/e de nós intermediários. Soluções que são completamente disjuntas atingem maior resiliência.

Conclui-se que, de uma perspectiva geral, a resiliência e a redundância estão intimamente relacionadas por meio de técnicas de detecção e isolamento de falhas. Dependendo da natureza da falha, o período que a rede fica em recuperação pode ser reduzido e, portanto, a disponibilidade da rede aumenta. O módulo de configuração de caminhos do ARES garante o caminho *backup* (quando esse existir) e o módulo de evento notifica as falhas para que os novos caminhos continuem sendo criados de forma proativa.

Outro ponto importante da avaliação, é que os mecanismos, como o RSTP, não necessariamente escolhem o caminho mais curto (ou mais rápido) para comunicar. E, portanto, não tendem a aproveitar melhor a topologia da rede para atingir o atraso ideal, o que é considerado essencial para serviços sensíveis ao tempo. O RSTP, por exemplo, depende dos parâmetros de configuração e da localização da falha.

O PRP, por ser um método de redundância paralela, apresenta como maior vantagem ser transparente a falhas, desde que não atinja as duas redes. No entanto, aumenta mais que o dobro a carga nos dispositivos de origem e destino além de alterar os *frames* gerados. Outro ponto importante, é que o PRP não é transparente para os dispositivos finais, logo, não mantém compatibilidade com os equipamentos "não PRP". O RSTP, apesar de ter um tempo de recuperação muito alto, não precisa estar disponível nos equipamentos finais.

De forma geral, o *framework* ARES pode ser implementado de forma transparente para os elementos finais. Possui opções para implementação com a modelagem IEC 61850 atual, mantendo compatibilidade com os equipamentos existentes. Aloca recursos da rede de forma dinâmica e granular, de acordo com os *datasets* configurados. Permite que as novas aplicações de energia sejam criadas de forma modular, podendo interagir, umas com as outras. Com relação ao módulo de configuração de caminhos, não aumenta o processamento dos dispositivos nem a quantidade de *switches* na rede ou o tráfego como acontece com o PRP ou o HSR. Mesmo com o aumento da quantidade de *switches* na rede, o tempo de recuperação não se eleva, indicando boa escalabilidade. Assim, acredita-se que o *framework* ARES avança o estado da arte, viabilizando a construção de ambientes de comunicação confiáveis e escaláveis para as redes elétricas inteligentes, além de aplicações

de energia mais inteligentes e dinâmicas.

Capítulo 7

Conclusão

A digitalização de subestações de energia iniciou com a possibilidade de supervisão e controle através de um sistema de aquisição de dados (SCADA) e de protocolos de supervisão, como o MODBUS, da década de 70 [146]. Com o decorrer do tempo, novos protocolos de supervisão e controle surgiram, como o DNP3 e o MMS (ISO 9506), e com eles mais recursos para controle e supervisão dos equipamentos da rede elétrica. Em seguida, protocolos como o GOOSE e o SV foram propostos para trafegar dados de proteção e de amostragem de tensão e corrente utilizando a modelagem e os serviços descritos na norma IEC 61850. Essa possibilidade é vista como um marco na digitalização de subestações, pois permite que novas filosofias de proteção e controle sejam implementadas. No entanto, todas são dependentes de uma infraestrutura de comunicação robusta e eficiente.

Nesse sentido, a automação do sistema elétrico tem ficado cada vez mais inteligente inserindo a possibilidade de comunicação aonde não existia, ou aonde só eram utilizados cabos de controle. Como já era esperado, essas possibilidades se expandiram além das subestações e atualmente a norma IEC 61850 tem sido considerada uma das bases para a implementação das redes elétricas inteligentes. Diversos autores têm proposto soluções promissoras, que trazem um alto grau de automação e comunicação para todo o sistema elétrico, utilizando os protocolos da norma IEC 61850 (GOOSE, MMS e SV) e o seu modelo de informação, para *microgrids* [65, 180, 164, 170], para automação da distribuição [8], para a comunicação de veículos elétricos [181], entre outros.

Com a evolução dos sistemas e a inserção de fontes de energia renováveis, tem-se um cenário com dispositivos multifuncionais com comunicação bidirecional e em tempo real. Surge uma quantidade significativa de propostas que exploram o novo paradigma das redes elétricas inteligentes e dependem de sistemas de comunicação mais flexíveis e dinâmicos, com interação em tempo real, sendo este, um dos principais desafios da área. Apesar disso, os sistemas de comunicação utilizados nestes cenários não acompanharam a evolução das novas propostas, restringindo a implementação destas.

Dentre as novas soluções, tem-se a necessidade de aperfeiçoamento dos sistemas

supervisórios. Alguns autores [56, 137] já apontaram a necessidade de modernização do SCADA tradicional, que não atende mais aos requisitos das redes elétricas inteligentes. A configuração manual, que é realizada atualmente no SCADA de subestações, não é mais exequível quando a rede a ser supervisionada aumenta de escala. A necessidade de mapeamento de pontos manualmente* no SCADA praticamente inviabiliza a sua implementação. Com isso, a escala das redes elétricas inteligentes não pode ser gerenciada pelos sistemas supervisórios atuais [113]. Como detalhado em [113], o alto custo e baixa interoperabilidade tornam as soluções baseadas no SCADA tradicional impraticáveis, limitando efetivamente sua adoção da forma com que é implementado hoje. Portanto, os sistemas supervisórios precisam ser aperfeiçoados para atender a nova escala e novas funcionalidades das redes elétricas inteligentes.

Nesta tese, estes problemas foram identificados e discutidos. A solução intitulada ARES foi proposta e sua implementação validada. A exploração da capacidade multifuncional dos dispositivos, com alocações dinâmicas, que respeitem a característica configurada para o fluxo é um dos pilares do *framework*, que viabiliza a implementação destas novas propostas em redes elétricas inteligentes. Para que novas aplicações de energia possam ser implementadas, elas precisam contar com uma rede de comunicação mais dinâmica e que atenda às restrições temporais rígida impostas pelo novos sistemas de proteção [179, 177]. A comunicação precisa ser confiável evitando que falhas na rede de comunicação interfiram nos mecanismos de proteção e controle da rede elétrica [169]. O sistema supervisório precisa ser capaz de permitir maior dinamismo e flexibilidade para que possa acompanhar a escala das redes elétricas inteligentes.

A proposta ARES introduz uma nova API que permite que os serviços de supervisão e controle configurem dinamicamente a rede permitindo o desenvolvimento de uma nova geração de aplicações de energia, que possam agir sobre a rede de comunicação em tempo real, além de permitir a implementação das aplicações de energia já propostas para as redes elétricas inteligentes. Dessa forma, tem-se um sistema de supervisão modular, baseado no *framework*, de forma que a escala das redes elétricas inteligentes não seja uma barreira para as novas soluções. A extensão da modelagem IEC 61850 foi proposta, permitindo que novas implementações baseadas na prioridade do dispositivo físico para o sistema elétrico, ou na sua função (e mudança de função) sejam realizadas. Com a implementação do *framework* ARES, é possível que um novo SCADA, intitulado nesta tese como SCADA-NG, possa ser construído com aplicações de energia mais inteligentes e mais capazes. Da mesma forma, a resiliência de uma rede baseada no *framework* foi avaliada validando que a solução atende aos requisitos impostos pelo setor de energia elétrica para o estudo de caso apresentado.

*Cada variável interna do dispositivo gera um ponto a ser mapeado, desde a magnitude de uma tensão até uma variável que seja usada para receber um comando do *display*, ou painel frontal de um dispositivo.

7.1 Contribuições da Tese

A contribuição principal desta tese é o *framework* ARES, que permite:

- que aplicações de energia utilizem os atributos de cada *dataset* IEC 61850 do plano de energia para alocar seus recursos de forma dinâmica, provisionando seu caminho de forma automática;
- que os equipamentos e suas características sejam mapeados no supervisório de forma automática, desde que autenticados;
- que cada fluxo na rede e sua situação (ativo/inativo) seja mapeado automaticamente;
- que eventos sejam reportados para as aplicações. Isto é essencial para que a rede tenha um melhor aproveitamento, permitindo, inclusive, que caminhos *backup* sejam utilizados para enlaces com sobrecarga e não só para enlaces em falha;
- que as abordagens de recuperação de falha sejam combinadas para um melhor resultado latência x tempo de indisponibilidade.
- a extensão da modelagem IEC 61850 para trabalhar com prioridade de dispositivos físicos e multifuncionalidade de dispositivos, entre outros. Essa característica é muito importante para programas de resposta à demanda e carga e recarga de veículos elétricos.
- que caminhos *backup* sejam utilizados para enlaces com sobrecarga e não só para enlaces em falha, com base nas notificações do serviço *Event* da API.
- que enlaces reprovisionados ou em falha/sobrecarga, sejam monitorados e utilizados pelas aplicações de energia.

O *framework* ARES oferece uma API com novas classes e serviços para mapeamento e provisionamento automáticos, e, um serviço de notificações que contém, inclusive, informações de sobrecarga, ou alterações em tempo real.

Além da definição completa do *framework*, suas classes, serviços, componentes e módulos, uma contribuição importante desta tese é a extensão da norma IEC 61850. Com essa extensão, novas possibilidade relacionadas às redes de comunicação podem ser exploradas. Mapeamentos de fluxos de acordo com o tipo de mensagem, ativação e desativação de fluxos de comunicação em tempo real, priorização de dispositivos críticos como postos de recarga de hospitais, entre outros, podem ser realizados. Desta forma, com a implementação do *framework* ARES e sua API, as aplicações de energia poderão implementar novos serviços que até então não eram possíveis. Exemplos são:

1. a entrada automática de dispositivos do plano de energia no SCADA-NG;

2. a possibilidade de mudança de perfil dos dispositivos (carga para gerador, por exemplo) serem reportadas e tratadas de acordo, aumentando consideravelmente o dinamismo e flexibilidade dos sistemas supervisórios;

3. a definição da prioridade para cargas e geradores, que podem, inclusive ter a prioridade definida pela aplicação de energia com base na situação atual do restante da rede elétrica;

4. a liberação da entrada de geradores distribuídos de acordo com situação da rede elétrica e a estabilidade prevista;

5. o gerenciamento dinâmico de ativos do sistema de distribuição, etc.

Ademais, com o provisionamento dinâmico por *dataset*, a rede de comunicação não sofre com a carga desnecessária das mensagens *multicast* de camada 2, o que influencia diretamente na latência da rede e no seu desempenho. O *framework* permite que novas soluções de resiliência sejam testadas, inclusive baseadas em redundância paralela, a fim de aumentar o desempenho da rede de comunicação do sistema de infraestrutura crítica.

A Tabela 7.1, relacionada as características levantadas anteriormente no estado da arte com o *framework* ARES ressaltando os aspectos que são cobertos pelo *framework* e suas limitações atuais.

Tabela 7.1: Propostas para redes elétricas inteligentes baseadas em *smart grid*. "✓" indica que o tópico foi abordado mesmo que parcialmente e "–" que não foi abordado.

Aspectos	***Framework* ARES**	Goodney et al. [64]	Cahn et al. [40]	Lopes et al. [120]	Dorsch et al. [51]	Molina et al. [135]	Sydney et al. [176]	Byun et al. [39]	Qin et al. [156]	Kim et al. [93]	Dong et al. [50]	Pfeiffenberger et al. [152]	Reitblatt et al. [159]	Gyllstrom et al. [70]	Pigossi e Lopes [153]	Silva et al. [48]
Domínio	SG	PMU	SE	SE	SG	SG	SG	SG	SG	SG	SG	SG	SG	SG	SE	SG
Monitoramento da Rede/Sistema	✓	–	✓	✓	✓	✓	✓	✓	✓	–	✓	–	–	–	–	–
Descoberta de Dispositivos	✓	–	–	✓	✓	–	–	–	–	–	–	–	–	–	✓	–
Balanceamento de Carga	–	–	✓	–	–	✓	✓	✓	–	–	–	–	–	–	–	–
Qualidade de Serviço	✓	–	–	✓	✓	–	✓	✓	✓	–	–	–	–	–	–	–
Segurança	–	–	✓	–	–	✓	–	–	–	–	✓	–	–	–	✓	✓
Recuperação de Falhas	✓	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	–	–
Provisionamento e monitoramento a partir do SCADA	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Provisionamento dinâmico e autonômico de acordo com os *datasets* dos IEDs	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Modelagem própria	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

PMU. *Smart Grid* (SG). Subestações (SE)

7.2 Trabalhos Futuros

Como trabalho futuro, pretende-se estender o *framework* para incorporar segurança cibernética nativa, fornecendo módulos de autenticação e controle de acesso, entre outros, que possam minimizar a vulnerabilidade da rede. Da mesma forma, o balanceamento de carga, já tradicional de soluções SDN, pode ser incorporado ao ARES.

Muitas aplicações de energia personalizadas podem ser propostas e desenvolvidas baseadas no *framework*. Alguns exemplos são:

1. aplicação de energia para sistemas de Teleproteção de subestações: que configure automaticamente a rede de teleproteção com base na configuração dos IEDs, que informe alarmes em tempo real na aplicação que podem, por exemplo, gerar *tickets* informando o local da falha pra manutenção sem queda do serviço caso tenha caminho *backup*, entre muitas outras funções;

2. aplicação para controle de carga e recarga de veículos elétricos: que priorize dinamicamente os veículos que podem ser carregados primeiro com base na prioridade definida nos dispositivos físicos e tenham o controle da localização de cada VE em tempo real;

3. aplicação de energia para supervisão e gerenciamento de recursos de energia distribuídos: que gerencie dinamicamente a entrada e saída dos recursos de acordo com a situação atual da rede elétrica de forma a manter a rede elétrica estabilizada;

4. aplicação de energia para visualização de dados e controle dos IEDs do sistema de distribuição: os usuários podem selecionar os equipamentos para ter suas informações em tempo real, tanto da rede de comunicação quanto do conteúdo dos IEDs. Se forem IEC 61850 *servers*, podem ainda serem alocados em uma mapa com sua localização geográfica em tempo real;

5. Aplicação de energia para gerenciamento de ativos: provê o gerenciamento de ativos, inclusive da rede de distribuição de energia, de forma automática e em tempo real;

Outro trabalho interessante a ser realizado é o desenvolvimento de mais um componente para o módulo de configuração de caminhos para trabalhar com redundância paralela, para uma análise mais profunda da resiliência da rede. Uma solução em conjunto, pode trazer algumas vantagens, dentre elas, a redução do tempo total já que o tempo para detecção da falha, num primeiro momento, não existiria.

Como os *datapaths* do *framework* são qualquer dispositivo que comunique no plano de energia ou de dados, o desenvolvimento de *smart meters* definidos por softwares e IEDs definidos por *software* também são uma abordagem promissora.

Também com relação as redes definidas por *software*, duas extensões podem ser realizadas. Uma proposta de uso de controladores distribuídos para o *framework* ARES pode trazer ganhos, principalmente para a escalabilidade da solução. A extensão do *framework* para outras plataformas SDN, como o NETCONF [55][†], também podem ser realizada.

Ressalta-se que a implementação do *framework* ARES em um piloto da rede elétrica inteligente é uma das metas a serem realizadas como trabalhos futuros desta tese.

[†]O *Network Configuration* (NETCONF) foi definido pelo *Internet Engineering Task Force* (IETF), originalmente por meio da *Request for Comments* (RFC) 4741 [54], depois substituída pela RFC 6241 [55], sendo seu principal idealizador Rob Enns da empresa Juniper Networks.

Referências

[1] IEC 60834: Teleprotection Equipment of Power Systems - Performance and Testing. Relatório Técnico, IEC - Internacional Electrotechnical Comission, 1999.

[2] ISO 9506-2:2003:Industrial Automation Systems – Manufacturing Message Specification (MMS) – Part 2: Protocol Specification. Standard 2, International Organization for Standardization, 2003/07.

[3] ISO 9506-1:2003:Industrial Automation Systems – Manufacturing Message Specification (MMS):Part 1: Service Definition. Standard 2, International Organization for Standardization, 2003/08.

[4] IEEE 1588- IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. Relatório Técnico, IEEE, 2008.

[5] Multi-agent approach to emergency control of power system. *3rd International Conference on Deregulation and Restructuring and Power Technologies, DRPT 2008*, April (2008), 2157–2161.

[6] *OpenFlow Switch Specification, Version (Wire Protocol 0x01)*. The OpenFlow Consortium, 2009.

[7] IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3). Relatório Técnico, July 2010.

[8] Distributed power system automation with IEC 61850, IEC 61499, and intelligent control. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews 41*, 1 (2011), 81–92.

[9] *OpenFlow Switch Specification Version 1.1.0 (Wire Protocol 0x02)*. The OpenFlow Consortium, 2011.

[10] *OpenFlow Switch Specification Version 1.3.0 (Wire Protocol 0x04)*. The OpenFlow Consortium, 2012.

[11] *OpenFlow Switch Specification Version 1.4.0 (Wire Protocol 0x05)*. The OpenFlow Consortium, 2013.

[12] Adaptive protection scheme for smart grids. *Developments in Power System Protection (DPSP 2014), 12th IET International Conference on* (2014), 1–6.

[13] Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015* (2015), 165–173.

[14] Integration of IEC 61850 into a Vehicle-to-Grid system with networked electric vehicles. *2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2015* (2015), 1–5.

[15] Decentralized Cloud-SDN Architecture in Smart Grid: A Dynamic Pricing Model. *IEEE Transactions on Industrial Informatics 14*, 3 (2018), 1220–1231.

[16] IEEE 1609 WAVE and IEC 61850 Standard Communication Based Integrated EV Charging Management in Smart Grids. *IEEE Transactions on Vehicular Technology 9545*, c (2018), 1–9.

[17] *Documentation TCPDUMP*. http://www.tcpdump.org, Accessed in 2018 set.

[18] *libIEC61850 / lib60870-5*. https://libiec61850.com/libiec61850/about/, Accesso em agosto de 2018.

[19] *The Only Complete API Platform*. https://www.getpostman.com/products, Accesso em agosto de 2018.

[20] *What Is SDN All About, Then?* http://www.noxrepo.org/2012/03/sdn/, Accesso em janeiro de 2018.

[21] *Open Networking Foundation*. https://www.opennetworking.org/, Accesso em maio de 2018.

[22] *Open Networking Summit*. http://www.opennetsummit.org/why-sdn.html, Accesso em maio de 2018.

[23] *Clean slate research program*. http://cleanslate.stanford.edu/. Stanford Univesity, Accesso em outubro de 2018.

[24] *About Wireshark*. https://www.wireshark.org/, Accesso em setembro de 2018.

[25] Institute of Electrical and Electronics Engineers. 802.1Q - Standard for Local and metropolitan area networks: Virtual Bridged Local Area Networks. Relatório Técnico, IEEE, 2003.

[26] Institute of Electrical and Electronics Engineers. IEEE 802.1AB - Standard for Local and metropolitan area networks – Station and Media Access Control Connectivity Discovery. Relatório Técnico, IEEE, 2005/2016.

[27] Abi-Ramia, M. A., de Castro Fernandes, N., Fortes, M. Z., Lopes, Y. Power protection asset manager with iec 61850. In *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)* (May 2018), p. 1–6.

[28] Adamson, A. Protection Using Telecommunications. Relatório Técnico December, CIGRÉ Joint Working Group 34/35.11, 2000.

[29] Aftab, M. A., Hussain, S. M. S., Ali, I., Ustun, T. S. IEC 61850 and XMPP Communication Based Energy Management in Microgrids Considering Electric Vehicles. *IEEE Access 6* (2018), 35657–35668.

[30] Akkaya, K., Uluagac, A. S., Aydeger, A. Software defined networking for wireless local networks in Smart Grid. *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)* (2015), 826–831.

[31] Ali, I., s. hussain. Communication design for energy management automation in microgrid. *IEEE Transactions on Smart Grid PP*, 99 (2016).

[32] Araújo, P. Spanning tree protocols: Evoluções. Instituto Superior de Engenharia de Lisboa (ISEL).

[33] Ates, Y., Boynuegri, A., Uzunoglu, M., Nadar, A., Yumurtaci, R., Erdinc, O., Paterakis, N., Catalão, J. Adaptive Protection Scheme for a Distribution System Considering Grid-Connected and Islanded Modes of Operation. *Energies 9*, 5 (2016), 378.

[34] Bahmanyar, A., Jamali, S., Estebsari, A., Pons, E., Bompard, E., Patti, E., Acquaviva, A. Emerging smart meters in electrical distribution systems: Opportunities and challenges. In *2016 24th Iranian Conference on Electrical Engineering (ICEE)* (May 2016), p. 1082–1087.

[35] Bayod-Rujula, A. A. Future development of the electricity systems with distributed generation. *Energy 34*, 3 (2009), 377–383.

[36] Brunner, C., Lang, G., Leconte, F. Implementation guideline for digital interface to instrument transformers using IEC 61850-9-2. *Raleigh: UCA International Users Group 10604* (2004), 1–31.

[37] Bu, S., Yu, F., Liu, P. Dynamic pricing for demand-side management in the smart grid. In *2011 IEEE Online Conference on Green Communications (GreenCom)* (setembro de 2011), p. 47 – 51.

[38] Budka, K., Deshpande, J., Hobby, J., Kim, Y.-J., Kolesnikov, V., Lee, W., Reddington, T., Thottan, M., White, C., Choi, J.-I., Hong, J., Kim, J., Ko, W., Nam, Y.-W., Sohn, S.-Y. GERI - Bell Labs smart grid research focus: Economic modeling, networking, and security & privacy. In *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)* (outubro de 2010), p. 208–213.

[39] Byun, J., Hong, I., Kang, B., Park, S. A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting. *IEEE Transactions on Consumer Electronics 57*, 2 (2011), 436–444.

[40] Cahn, A., Hoyos, J., Hulse, M., Keller, E. Software-defined energy communication networks: From substation automation to future smart grids. In *IEEE SmartGridComm* (2013).

[41] Chaves, R. C. P., Leão, F. B. Sistema de proteção adaptativo para redes de distribuição com inserção de geradores distribuídos. *XX Congresso Brasileiro de Automática* (2014), 2338–2345.

[42] Chelluri, S., D. D. D. J. K. A. Design and validation practices for ethernet networks to support automation and control applications. NTPC Limited Schweitzer Engineering Laboratories.

[43] Cheng-gen, W., Bao-hui, Z., Jin, S., Lin-yan, C., Peng, L., Zhi-guo, H., Zhi-qian, B., Klimek, A. A novel fast searching algorithm for power system self-adaptive islanding. In *2009 Asia-Pacific Power and Energy Engineering Conference (APPEEC 2009)* (mar de 2009), p. 1 – 6.

[44] Cheng-gen, W., Bao-hui, Z., Zhi-guo, H., Zhi-qian, B., Yu, S. Study on power system self-adaptive islanding. In *2011 International Conference on Advanced Power System Automation and Protection (APAP)* (outubro de 2011), vol. 1, p. 270 – 274.

[45] Chun-Hao, L., Ansari, N. The progressive smart grid system from both power and communications aspects. *IEEE Communications Surveys Tutorials 14*, 3 (2012), 799–821.

[46] Commission, I. E. In *IEC 62351: Power systems management and associated information exchange - Data and communications security*. 2018.

[47] Community, R. S. F. RYU: Component-Based Software Defined Networking Framework: Build SDN Agilely, Acesso em dezembro de 2018.

[48] d. Silva, E. G., d. Silva, A. S., Wickboldt, J. A., Smith, P., Granville, L. Z., Schaeffer-Filho, A. A one-class nids for sdn-based scada systems. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)* (June 2016), vol. 1, p. 303–312.

[49] de Meneses, L. T. Automao da deteco de fraudes em sistemas de medio de energia eltrica utilizando lgica fuzzy em ambientes SCADA. Dissertação de Mestrado, Universidade Federal do Rio Grande do Norte, RN, Brasil, abril de 2011.

[50] Dong, X., Lin, H., Tan, R., Iyer, R. K., Kalbarczyk, Z. Software-defined networking for smart grid resilience: Opportunities and challenges. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security* (New York, NY, USA, 2015), CPSS '15, ACM, p. 61–68.

[51] Dorsch, N., Kurtz, F., Georg, H., Hagerling, C., Wietfeld, C. Software-defined networking for smart grid communications: Applications, challenges and advantages. *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 422–427.

[52] Driesen, J., Vermeyen, P., Belmans, R. Protection issues in microgrids with multiple distributed generation units. In *2007 Power Conversion Conference - Nagoya* (April 2007), p. 646–653.

[53] Electric Power Research Institute - EPRI. *EPRI Intelligrid [Online]*. http://intelligrid.epri.com.

[54] Enns, R. NETCONF Configuration Protocol. Relatório Técnico, Internet Eng. Task Force - RFC 4741, dezembro de 2006.

[55] Enns, R., Bjorklund, M., Schoenwaelder, J., Bierman, A. Network Configuration Protocol (NETCONF). Relatório Técnico, Internet Eng. Task Force - RFC 6241, junho de 2011.

[56] Etherden, N., Vyatkin, V., Bollen, M. H. J. Virtual power plant for grid services using iec 61850. *IEEE Transactions on Industrial Informatics 12*, 1 (Feb 2016), 437–447.

[57] Fang, X., Misra, S., Xue, G., Yang, D. Smart grid - the new and improved power grid : A survey. *Power PP, no. 99* (2011), 1–37.

[58] Fang, X., Misra, S., Xue, G., Yang, D. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials 14*, 4 (2012), 944–980.

[59] Farag, H. E., El-Saadany, E. F. Voltage regulation in distribution feeders with high dg penetration: From traditional to smart. In *2011 IEEE Power and Energy Society General Meeting* (July 2011), p. 1–8.

[60] Feamster, N., Rexford, J., Zegura, E. The road to SDN. *ACM SIGCOMM Computer Communication Review 44*, 2 (2014), 87–98.

[61] Fernandes, N. C., Magalhaes, L. C. S. *Network Innovation Through Openflow and Sdn: Principles and Design. Chapter 5:Control and Management Software for SDNs: Conceptual Models and Practical View (ISBN 9781466572096)*, 1 ed. Fei Hu. (Org.), 2013.

[62] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., Poolla, K. Smart grid data integrity attacks: Characterizations and countermeasures. *Cyber and Physical Security and Privacy* (novembro de 2011), 232–237.

[63] Gonçalves, L. F. Contribuições para o Estudo Teórico e Experimental de Sistemas de Geração Distribuída. Dissertação de Mestrado, Universidade Federal do Rio Grande do Sul, 2004.

[64] Goodney, A., Kumar, S., Ravi, A., Cho, Y. H. Efficient PMU networking with software defined networks. In *SmartGridComm* (2013).

[65] Gray, K., Kumm, J., Mraz, J. A High-Level Framework for Implementation and Test of IEC 61850-based Microgrid Power Management Systems. 4–7.

[66] Gu, J.-c., Yang, M.-t., Yan, C.-f., Chung, H.-y., Chang, Y.-r., Lee, Y.-d., Chan, C.-m., Hsu, C.-h. A Group Setting of IED in Microgrid Protection Management System. 760–765.

[67] Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., Shenker, S. Nox: Towards an operating system for networks. *SIGCOMM Comput. Commun. Rev. 38*, 3 (julho de 2008), 105–110.

[68] Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G. Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics 7*, 4 (novembro de 2011), 529–539.

[69] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G. P. A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics 9*, 1 (Feb 2013), 28–42.

[70] Gyllstrom, D. *Making Networks Robust to Component Failures*. Tese de Doutorado, 2014.

[71] Gyllstrom, D., Braga, N., Kurose, J. Recovery from link failures in a Smart Grid communication network using OpenFlow. In *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (nov 2014), IEEE, p. 254–259.

[72] Habib, H. F., Lashway, C. R., Mohammed, O. A. A Review of Communication Failure Impacts on Adaptive Microgrid Protection Schemes and the Use of Energy Storage as a Contingency. *IEEE Transactions on Industry Applications 54*, 2 (2018), 1194–1207.

[73] Heine, H., Bindrich, D. Designing reliable high-performance iec61850 substation communication networks based on prp and hsr topologies. 22nd International Conference and Exhibition on Electricity Distribution.

[74] Hopkinson, K., Wang, X., Giovanini, R., Thorp, J., Birman, K., Coury, D. Epochs: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Transactions on Power Systems 21*, 2 (May 2006), 548–558.

[75] Hub, S. POX Controller Tutorial, Acesso em dezembro de 2018.

[76] Ilic, M. D., Xie, L., Khan, U. A., Moura, J. M. F. Modeling of future cyber; physical energy systems for distributed sensing and control. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 40*, 4 (July 2010), 825–838.

[77] Ingram, D., Schaub, P., Campbell, D. Multicast traffic filtering for sampled value process bus networks. In *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society* (2011), p. 4710–4715.

[78] International Electrotechnical Commission. IEC 61850-5: Communication requirements for functions and device models. Relatório Técnico, IEC, 2003.

[79] International Electrotechnical Commission. IEC 61850-6: Configuration Description Language for Communication in Electrical Substations Related to IEDs. Relatório Técnico, IEC, 2009.

[80] International Electrotechnical Commission. IEC 61850-7-420: Basic communication structure - Distributed Energy Resources logical nodes. Relatório Técnico, IEC, 2009.

[81] International Electrotechnical Commission. IEC 61850-7-2: Communication Network and Systems for Power Utility Automation. Basic information and communication structure - Abstract communication service interface (ACSI). Relatório Técnico, IEC, 2010.

[82] International Electrotechnical Commission. IEC 61850-7-4: Communication Network and Systems for Power Utility Automation. Basic Communication Structure - Compatible Logical Node Classes and Data Object Classes. Relatório Técnico, IEC, 2010.

[83] International Electrotechnical Commission. IEC 61850-90-1: Use of IEC 61850 for the communication between substations. Relatório Técnico, IEC, 2010.

[84] International Electrotechnical Commission. IEC 62439-3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). Relatório Técnico 62439, IEC, 2010.

[85] International Electrotechnical Commission. IEC 61850-7-1: Communication Network and Systems for Power Utility Automation. Basic Communication Structure - Principles and Models. Relatório Técnico, IEC, 2011.

[86] International Electrotechnical Commission. IEC 61850-8-1: Specific communication service mapping - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. Relatório Técnico, IEC, 2011.

[87] International Electrotechnical Commission. IEC 618509-2: Specific communication service mapping (SCSM)-Sampled values over ISO/IEC 8802-3. Relatório Técnico, IEC, 2011.

[88] International Electrotechnical Commission. IEC 61850-90-8: IEC 61850 object models for electric mobility. Relatório Técnico, IEC, 2016.

[89] Jin, X., Gokaraju, R., Wierckx, R., Nayak, O. High Speed Digital Distance Relaying Scheme using FPGA and IEC 61850. *IEEE Transactions on Smart Grid 3053*, c (2017), 1–1.

[90] Kabalci, Y. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews 57* (2016), 302 – 318.

[91] Kabisch, S., Schmitt, a., Winter, M., Heuer, J. Interconnections and Communications of Electric Vehicles and Smart Grids. *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* (oct 2010), 161–166.

[92] Kezunovic, M. Smart fault location for smart grids. *IEEE Transactions on Smart Grid 2*, 1 (March 2011), 11–22.

[93] Kim, J., Filali, F., Ko, Y. B. A lightweight coap-based software defined networking for resource constrained ami devices. In *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (Nov 2015), p. 719–724.

[94] Kirrmann, H. Parallel redundancy protocol: an upcoming standard for hard-real time redundancy in industrial ethernet. IEC SC65C MT9HA, 2007, Switzerland Proceedings ... IEC MT9 session, p.1 -43.

[95] Kirrmann, H.; Weber, K. K. O. W. H. Seamless and low-cost redundancy for substation automation systems (high availability seamless redundancy, hsr). Power and Energy Society General Meeting, 2011 IEEE , vol., no., pp.1-7, 24-29.

[96] Kirrmann, H.; Hansson, M. M. P. Iec 62439 prp: Bumpless recovery for highly available, hard real-time industrial networks. Emerging Technologies and Factory Automation. IEEE Conference on , vol., no., pp.1396-1399.

[97] Kumar, D., Sood, M. Software Defined Networking: A Concept and Related Issues. *International Journal of Advanced Networking & Applications 6*, 2 (2014), 2233–2239.

[98] Kurose, J. F., Ross, K. W. *Computer Networking: A Top-Down Approach*, 5th ed. Addison-Wesley Publishing Company, USA, 2009.

[99] Laaksonen, H., Ishchenko, D., Oudalov, A. Adaptive Protection and Microgrid Control Design for Hailuoto Island. *IEEE Transactions on Smart Grid 5*, 3 (may 2014), 1486–1493.

[100] Laaksonen, H. J. Protection principles for future microgrids. *IEEE Transactions on Power Electronics 25*, 12 (Dec 2010), 2910–2918.

[101] Laboratories, S. E. SEL-2488: Relógio de Rede Sincronizado por Satélite, Acesso em janeiro de 2019.

[102] Laboratories, S. E. SEL-2730M: Switch Ethernet Gerenciável com 24 Portas, Acesso em janeiro de 2019.

[103] Laboratories, S. E. SEL-2740S: Switch de Rede Definida por Software, Acesso em janeiro de 2019.

[104] Laboratories, S. E. SEL-421: Sistema de Proteção, Automação e Controle, Acesso em janeiro de 2019.

[105] Laboratories, S. E. SEL-5030: acSELerator QuickSet Software, Acesso em janeiro de 2019.

[106] Laboratories, S. E. SEL-5032: acSELerator Architect Software, Acesso em janeiro de 2019.

[107] Laboratories, S. E. SEL-5056: Software-Defined Network Flow Controller, Acesso em janeiro de 2019.

[108] Laboratories, S. E. SEL-751A: Relé de Proteção do Alimentador, Acesso em janeiro de 2019.

[109] Laboratories, S. E. SEL 9524: GNSS Antenna: Reliable signal acquisition for critical infrastructure, Acesso em janeiro de 2019.

[110] LAN/MAN Standards Committee. 801.1D: IEEE Standard for Local and metropolitan area networks - MAC Bridges. Relatório Técnico, IEEE, 2004.

[111] Lantz, B., Heller, B., McKeown, N. A network in a laptop. In *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks - Hotnets '10* (2010), ACM Press, p. 1–6.

[112] Lara, A., Kolasani, A., Ramamurthy, B. Network innovation using openflow: A survey. *Communications Surveys Tutorials, IEEE*, 99 (2013), 1–20.

[113] Lazzarini, R., Stefanelli, C., Tortonesi, M. Large-scale e-maintenance: A new frontier for management? In *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)* (May 2013), p. 732–735.

[114] Lee, P. K., Lai, L. L. A practical approach for smart meter applied in demand side and distributed generation. In *8th International Conference on Advances in Power System Control, Operation and Management (APSCOM 2009)* (Nov 2009), p. 1–5.

[115] Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., Mili, L. Power system and communication network co-simulation for smart grid applications. In *ISGT 2011* (Jan 2011), p. 1–6.

[116] Lin, H., Veda, S. S., Shukla, S. S., Mili, L., Thorp, J. Geco: Global event-driven co-simulation framework for interconnected power system and communication network. *IEEE Transactions on Smart Grid 3*, 3 (Sept 2012), 1444–1456.

[117] Liserre, M., Sauter, T., Hung, J. Y. Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics. *IEEE Industrial Electronics Magazine 4*, 1 (March 2010), 18–37.

[118] Lopes, Y., Fernandes, N., de Castro, T., Farias, V., Noce, J., Marques, J., Muchaluat-Saade, D. *Security Solutions and Applied Cryptography in Smart Grid Communications*. IGI Global, Idea Group Inc, 2016, cap. Vulnerabilities and Threats in Smart Grid Communication Networks.

[119] Lopes, Y., Fernandes, N. C., Bastos, C. A. M. SMARTFlow: Uma Proposta para a Autoconfiguração de Redes de Subestação IEC 61850 Baseada em OpenFlow. In *Anais do XIX Workshop de Gerência e Operação de Redes e Serviços (WGRS 2014)* (Florianópolis, Brasil, 2014), WGRS 2014, SBRC, p. 31–44.

[120] Lopes, Y., Fernandes, N. C., Bastos, C. A. M., Muchaluat-Saade, D. C. SMARTFlow: A Solution for Autonomic Management and Control of Communication Networks for Smart Grids. 30th ACM SAC, p. 2212–2217.

[121] Lopes, Y., Fernandes, N. C., Castro, T. B., Muchaluat-Saade, V. S. F. D. C. Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids. In *Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (2015), SBC, p. 55–109.

[122] Lopes, Y., Fernandes, N. C., Muchaluat-Saade, D., Obraczka, K. ARES: An autonomic and resilient framework for smart grids. In *IM 2017* (Lisboa, Portugal, maio 2017).

[123] Lopes, Y., Fernandes, N. C., Muchaluat-Saade, D. C. Geração Distribuída de Energia: Desafios e Perspectivas em Redes de Comunicação. In *Minicursos do XXXIII SBRC* (2015), SBC, p. 55–109.

[124] Lopes, Y., Fernandes, N. C., Obraczka, K. Smart grid communication: Requirements and scada protocols analysis. In *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)* (May 2018), p. 1–6.

[125] Lopes, Y., Frazão, R. H., Molano, D. A., dos Santos, M. A., Calhau, F. G., Bastos, C. A. M., Martins, J. S. B., Fernandes, N. C. Smart Grid e IEC 61850: Novos Desafios em Redes e Telecomunicações para o Sistema Elétrico. In *Minicursos do XXX SBrT* (2012), SBrT, p. 1–44.

[126] Lopes, Y., Muchaluat-Saade, D. C., Fernandes, N. C., Fortes, M. Z. Geese: A traffic generator for performance and security evaluation of IEC 61850 networks. In *IEEE ISIE* (June 2015), p. 687–692.

[127] Lopes, Y., Saade, D. C. M., de Albuquerque, C. V. N., Fernandes, N. C., Fortes, M. Z. Quality of service for wireless network implementation in advanced metering infrastructure. *IEEE Latin America Transactions 15*, 10 (Oct 2017), 1875–1880.

[128] Lu, S., Repo, S., Giustina, D. D., Figuerola, F. A. C., Lof, A., Pikkarainen, M. Real-time low voltage network monitoring – ict architecture and field test experience. *IEEE Transactions on Smart Grid 6*, 4 (July 2015), 2002–2012.

[129] Ma, J., Mi, C., Wang, T., Wu, J., Wang, Z. An adaptive protection scheme for distributed systems with distributed generation. *2011 IEEE Power and Energy Society General Meeting* (2011), 1–6.

[130] Maharjan, S., Zhang, Y., Gjessing, S., Ulleberg, O., Eliassen, F. Providing microgrid resilience during emergencies using distributed energy resources. In *2015 IEEE Globecom Workshops (GC Wkshps)* (Dec 2015), p. 1–6.

[131] Manson, S. M., Upreti, A., Thompson, M. J. Case study: Smart automatic synchronization in islanded power systems. *IEEE Transactions on Industry Applications 52*, 2 (2016), 1241–1249.

[132] Marra, A. F. Redes definidas por software como solução confiável para comunicação do barramento de processo da iec 61850, 2016. Trabalho de Conclusão de Curso apresentado, INATEL, especialização em Automação de Subestações.

[133] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J. Openflow: enabling innovation in campus networks. *ACM SIGCOMM 38*, 2 (2008), 69–74.

[134] Miranda, J. C. IEC-61850: interoperabilidade e intercambialidade entre equipamentos de supervisão, controle e proteção através das redes de comunicação de dados. Dissertação de Mestrado, Escola de Engenharia de São Carlos - USP, SP, Brasil, junho de 2009.

[135] Molina, E., Jacob, E., Matias, J., Moreira, N., Astarloa, A. Using software defined networking to manage and control iec 61850-based systems. *Comput. Electr. Eng. 43*, C (abril de 2015), 142–154.

[136] Moore, R., Midence, R., Goraj, M. Practical experience with IEEE 1588 high Precision Time Synchronization in electrical substation based on IEC 61850 Process Bus. In *Power and Energy Society General Meeting, 2010 IEEE* (2010), p. 1–4.

[137] Moradi-Pari, E., Nasiriani, N., Fallah, Y. P., Famouri, P., Bossart, S., Dodrill, K. Design, modeling, and simulation of on-demand communication mechanisms for cyber-physical energy systems. *IEEE Transactions on Industrial Informatics 10*, 4 (2014), 2330–2339.

[138] National Institute of Standards and Technology. NIST Framework and Roadmap for Smart Grid Interoperability Standards. Relatório Técnico, National Institute of Standards and Technology, 2010.

[139] Nikkhajoei, H., Lasseter, R. H. Microgrid protection. In *2007 IEEE Power Engineering Society General Meeting* (June 2007), p. 1–6.

[140] Noce, J., Lopes, Y., Fernandes, N. C., Albuquerque, C. V. N., Muchaluat-Saade, D. C. Identifying vulnerabilities in smart gric communication networks of electrical substations using geese 2.0. In *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)* (June 2017), p. 111–116.

[141] Noce, J. D., Lopes, Y., Fernandes, N. C., Saade, D. C. M. Identificando Falhas de Segurança na Rede de Comunicação de Subestações Digitalizadas em Redes Elétricas Inteligentes Utilizando GEESE 2.0. In *XXI Congresso Brasileiro de Automática (CBA)* (2016).

[142] Nthontho, M., Chowdhury, S. P., Winberg, S. Smart communication networks standards for smart energy management. In *2011 IEEE 33rd International Telecommunications Energy Conference (INTELEC)* (Oct 2011), p. 1–9.

[143] Nutaro, J., Teja Kuruganti, P., Shankar, M., Miller, L., Mullen, S. Integrated modeling of the electric grid, communications, and control. *International Journal of Energy Sector Management 2*, 3 (2008), 420–438.

[144] Oliveira, W., Lopes, Y. Teleprotection over sonet based on iec 61850. In *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)* (May 2018), p. 1–6.

[145] ONS. Submodulo 2.6: Requisitos mínimos para os sistemas de proteção e de telecomunicações. Relatório Técnico, Operador Nacional do Sistema Elétrico (ONS), Data da Vigência 01/01/2017.

[146] Organization, M. *MODBUS Specifications*, fevereiro de 2017.

[147] Pan, J., JAIN, R., Paul, S. A survey of energy efficiency in buildings and microgrids using networking technologies. *IEEE Communications Surveys Tutorials*, 3 (Third 2014), 1709–1731.

[148] Patel, A., Aparicio, J., Tas, N., Loiacono, M., Rosca, J. Assessing communications technology options for smart grid applications. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)* (outubro de 2011), p. 126–131.

[149] Paulino, M. E. C., Siqueira, I. P., Chesf, U. A. C. Requisitos para interoperabilidade de IED's e sistemas baseados na norma IEC 61850. In 10º *Seminário Técnico de Proteção e Controle - X STPC* (outubro de 2010), p. 1–10.

[150] Pereira, A. C., Abboud, R., Pellizzoni, R., Zanirato, E., Caceres, D. Sistemas de proteção e automação de subestações de distribuição usando a norma IEC 61850. In *Cigre 2009* (2009), no. B5-22, p. 1–8.

[151] Pérez, R., Vásquez, C. Fault location in distribution systems with distributed generation using support vector machines and smart meters. In *2016 IEEE Ecuador Technical Chapters Meeting (ETCM)* (Oct 2016), vol. 01, p. 1–6.

[152] Pfeiffenberger, T., Du, J. L., Arruda, P. B., Anzaloni, A. Reliable and flexible communications for power systems: Fault-tolerant multicast with sdn/openflow. In *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)* (July 2015), p. 1–6.

[153] Pigossi, A. C., Lopes, Y. Substation security mechanism based on sdn and mms. In *2018 Simpósio Brasileiro de Sistemas Elétricos (SBSE)* (May 2018), p. 1–6.

[154] Pinotti, I. K. Desenvolvimento do protocolo rstp – rapid spanning tree protocols. Trabalho de Conclusão de Curso, Porto Alegre, 2009, pp 12-17.

[155] Pustylnik, M., Zafirovic-Vukotic, M., Moore, R. Performance of the Rapid Spanning Tree Protocol in Ring Network Topology. White Paper, Siemens, 2007.

[156] Qin, Z., Denker, G., Giannelli, C., Bellavista, P., Venkatasubramanian, N. A software defined networking architecture for the internet-of-things. In *2014 IEEE Network Operations and Management Symposium (NOMS)* (2014), p. 1–9.

[157] Rahnamay-Naeini, M., Wang, Z., Mammoli, A., Hayat, M. M. Impacts of control and communication system vulnerabilities on power systems under contingencies. In *2012 IEEE Power and Energy Society General Meeting* (July 2012), p. 1–7.

[158] Rehmani, M. H., Davy, A., Jennings, B., Assi, C. M. Software defined networks based smart grid communication: A comprehensive survey. *CoRR abs/1801.04613* (2018).

[159] Reitblatt, M., Canini, M., Guha, A., Foster, N. FatTire: Declarative Fault Tolerance for Software-Defined Networks. *HotSDN* (2013).

[160] Ren, F., Zhang, M., Soetanto, D., Su, X. Conceptual design of a multi-agent system for interconnected power systems restoration. *IEEE Transactions on Power Systems 27*, 2 (May 2012), 732–740.

[161] Repo, S., Lu, S., Poho, T., Giustina, D. D., Ravera, G., Selga, J. M., Figuerola, F. A. C. Active distribution network concept for distributed management of low voltage network. In *IEEE PES ISGT Europe 2013* (Oct 2013), p. 1–5.

[162] Rocha, G. L. N., Lopes, Y. Analysis of sympathetic tripping problem in photovoltaic distributed generation with iec 61850. In *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)* (May 2018), p. 1–6.

[163] Rothenberg, C. E., Nascimento, M. R., Salvador, M. R. OpenFlow e redes definidas por software : um novo paradigma de controle e inovação em redes de pacotes. *Control 7* (2011), 65–75.

[164] Ruiz-Alvarez, A., Colet-Subirachs, A., Figuerola, F. A.-C., Gomis-Bellmunt, O., Sudria-Andreu, A. Operation of a utility connected microgrid using an IEC 61850-based multi-level management system. *IEEE Transactions on Smart Grid 3*, 2 (2012), 858–865.

[165] Salomonsson, D., Soder, L., Sannino, A. Protection of low-voltage dc microgrids. *IEEE Transactions on Power Delivery 24*, 3 (July 2009), 1045–1053.

[166] Sauter, T., Lobashov, M. End-to-End Communication Architecture for Smart Grids. *IEEE Transactions on Industrial Electronics 58*, 4 (April 2011), 1218–1228.

[167] Sechilariu, M., Wang, B., Locment, F. Building integrated photovoltaic system with energy storage and smart grid communication. *IEEE Transactions on Industrial Electronics 60*, 4 (2013), 1607–1618.

[168] Seetharaman, S. OpenFlow and SDN tutorial. In *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2012 and the National Fiber Optic Engineers Conference* (2012), p. 1–52.

[169] Selga, J. M., Zaballos, A., Navarro, J. Solutions to the computer networking challenges of the distribution smart grid. *IEEE Communications Letters 17*, 3 (2013), 588–591.

[170] Shi, W., Xie, X., Chu, C.-C., Gadh, R. Distributed Optimal Energy Management in Microgrids. *IEEE Transactions on Smart Grid 6*, 3 (2015), 1137–1146.

[171] Siano, P. Demand response and smart gridsa survey. *Renewable and Sustainable Energy Reviews 30* (2014), 461 – 478.

[172] Silva, F. d. O., Goncalves, M. A., de Souza Pereira, J. H., Pasquini, R., Rosa, P. F., Kofuji, S. T. On the analysis of multicast traffic over the entity title architecture. In *Networks (ICON), 2012 18th IEEE International Conference on* (2012), p. 30–35.

[173] Sivanthi, T., Goerlitz, O. Systematic real-time traffic segmentation in substation automation systems. In *Emerging Technologies Factory Automation (ETFA), 2013 IEEE 18th Conference on* (2013), p. 1–4.

[174] Soares, A. A. Z., Mattos, D. M. F., Lopes, Y., Medeiros, D. S. V., Fernandes, N. C., Muchaluat-Saade, D. C. An Efficient Authentication Mechanism based on Software-Defined Networks for Electric Vehicles.

[175] Sortomme, E., Venkata, S. S., Mitra, J. Microgrid protection using communication-assisted digital relays. *IEEE Transactions on Power Delivery 25*, 4 (Oct 2010), 2789–2796.

[176] Sydney, A., Ochs, D. S., Scoglio, C., Gruenbacher, D., Miller, R. Using GENI for experimental evaluation of Software Defined Networking in smart grids. In *Computer Networks* (2014).

[177] Technical Committee on Power systems management and associated information exchange. IEC 61850 - communication networks and systems in substations. Relatório Técnico, International Electrotechnical Commission (IEC), 2002- 2013.

[178] Teimourzadeh, S., Aminifar, F., Davarpanah, M., Shahidehpour, M. Adaptive Protection for Preserving Microgrid Security. *IEEE Transactions on Smart Grid 3053*, c (2017), 1–9.

[179] U.S. Department of Energy. Communication requirements of smart grid technologies. Relatório Técnico, International Electrotechnical Commission, outubro de 2010.

[180] Ustun, T. S., Khan, R. H., Hadbah, A., Kalam, A. An adaptive microgrid protection scheme based on a wide-area smart grid communications network. In *2013 IEEE Latin-America Conference on Communications* (2013), p. 1–5.

[181] Ustun, T. S., Ozansoy, C. R., Zayegh, A. Implementing vehicle-to-grid (V2G) technology with IEC 61850-7-420. *IEEE Transactions on Smart Grid 4*, 2 (2013), 1180–1187.

[182] Vieira, J. C. M., Usp, S. E. L. E., Carlos, S., Paulo, S., Unicamp, D. F. Um Método Prático Para a Definição Dos Ajustes De Relés. 199–213.

[183] Villegas Guerrero, C. A. Uso do RTDS em testes de esquemas de teleproteção aplicando o Padrão IEC 61850. Mestrado, Universidade Federal de Itajubá, MG, Brasil, 2017.

[184] Wang, W., Xu, Y., Khanna, M. A survey on the communication architectures in smart grid. *Computer Networks 55*, 15 (oct 2011), 3604–3629.

[185] Wei, M., Chen, Z. Communication Systems and Study Method for Active. *Proc. NORADAC Conference* (2010), 1–11.

[186] XiCai, Z., ShuChao, W., Lei, X., YaDong, F. Practice and trend of DSAS in China. In *Advanced Power System Automation and Protection (APAP), 2011 International Conference on* (2011), vol. 3, p. 1762–1766.

[187] Yan, Y., Qian, Y., Sharif, H., Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys and Tutorials 15* (2013), 5–20.

[188] Zhenbo, W. E. I., Jing, G. O. U. An Overview on Application of Complex Network Theory in Power System Analysis. 1–5.

[189] Ziviani, N. *Projeto de Algoritmos: Com Implementações em Pascal e C.*, 2 ed. Thomson Learning, 2004.

Glossário

datasets Um *dataset* é um conjunto de objetos IEC 61850 agrupados de uma forma conveniente pelo cliente. São organizados como uma única coleção de objetos para a conveniência do cliente. Esta capacidade permite, assim, uma utilização mais eficiente da largura de banda das comunicações. Logo, um *dataset* GOOSE, por exemplo, pode conter vários objetos GOOSE e o que é enviado como *payload* da mensagem é o dataset [81] . 40, 94, 97, 112, 121, 131, 142

pipeline É o conjunto de tabelas de fluxo interconectadas entre si para prover o encaminhamento e modificações de pacotes em um *switch* OpenFlow [10]. 70, 72

aplicação de energia Neste documento, o termo refere-se as aplicações existentes no SCADA responsáveis por supervisionar e controlar as áreas das redes elétricas inteligentes. Aplicações de energia englobam aplicações de resposta à demanda, de tarifação, de supervisão de subestações, dentre outras. O termo aplicação puramente também é utilizado no texto. 17, 18

campos coringas Conhecidos como *wildcards*, não são especificados podendo conter qualquer valor. Dessa forma, o *switch* não se preocupa com o valor especificado no campo, apenas sabe se casou ou não [6]. 70

falta Uma falta elétrica é o contato ou arco acidental entre partes vivas sob potenciais diferentes, entre parte viva e a terra ou entre parte viva e massa. 12–14

fluxo Um fluxo (de comunicação) é a representação de determinado grupo de mensagens em função de suas características. Essas características variam de acordo com o cabeçalho das mensagens. 3

metadados Um valor de registro que é utilizado para enviar uma informação de uma tabela para a próxima [10]. 69

provisionamento Neste documento, o termo refere-se à configuração de um serviço de redes de comunicação para um cliente em particular. O provisionamento engloba a ideia de configurar a conexão entre os equipamentos, seja com a configuração de circuitos ou dos recursos de rede, da origem até o destino, para determinada comunicação. 17

sistema de proteção O sistema de proteção é o conjunto de equipamentos composto por relés de proteção, relés auxiliares, equipamentos de teleproteção e acessórios destinados a realizar a proteção em caso de falhas elétricas, tais como um curto-circuito, e de outras condições anormais de operação dos componentes de um sistema elétrico (Linha de Transmissão, barramentos e equipamentos [145]. 20

APÊNDICE A – Diagrama de Componentes de Implementação ARES

O diagrama de componentes, ilustrado na Figura A.1, mostra um exemplo de implementação, onde uma aplicação de energia utiliza os serviços prestados pela API ARES, localizada no ARES *Control Plane*. Os componentes dos módulos ARES, por sua vez, utilizam os serviços prestados pelo núcleo SDN para efetuar suas funções. O núcleo exemplificado pode sofrer variações de acordo com o controlador em uso. Da mesma forma, a aplicação de energia pode utilizar um ou mais serviços da API de acordo com o seu objetivo.

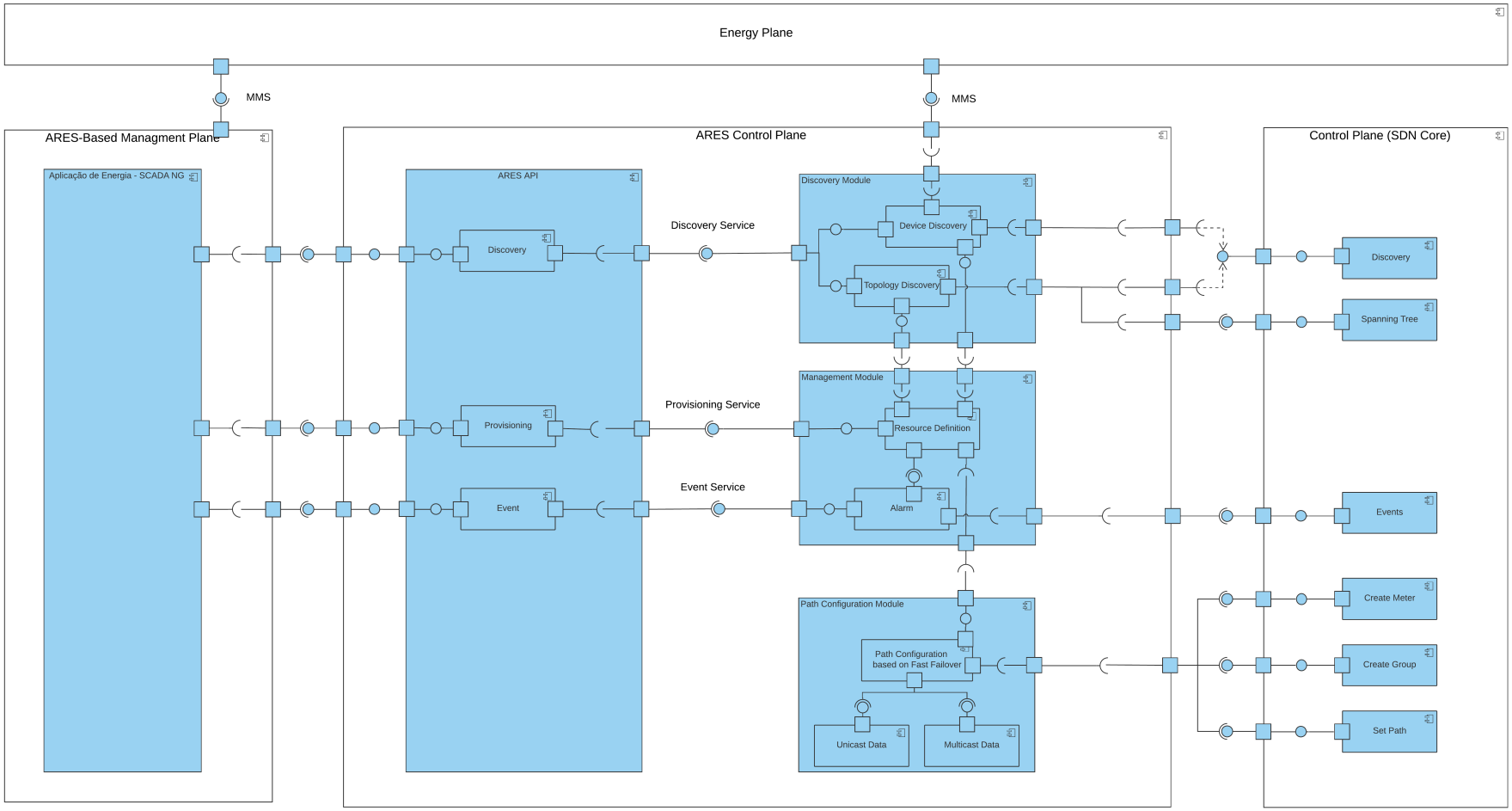


Figura A.1: Exemplo de diagrama de componentes de Implementação baseado no ARES

APÊNDICE B – Testes

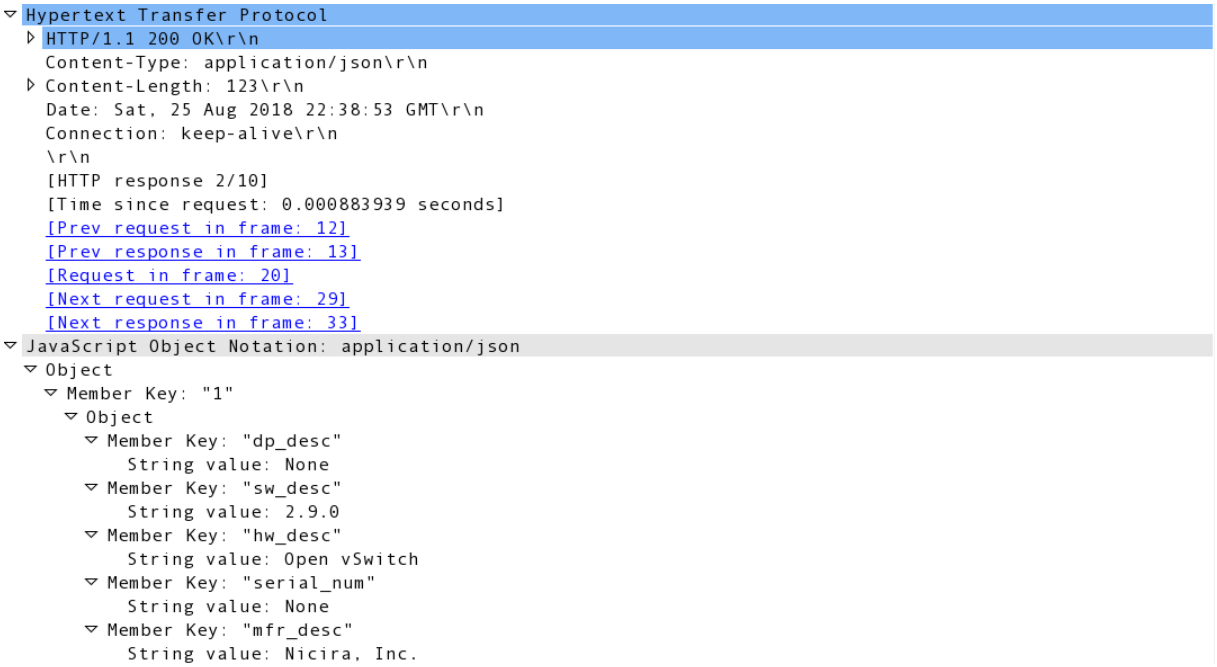


Figura B.1: Captura da resposta da segunda requisição do serviço *Discovery*.

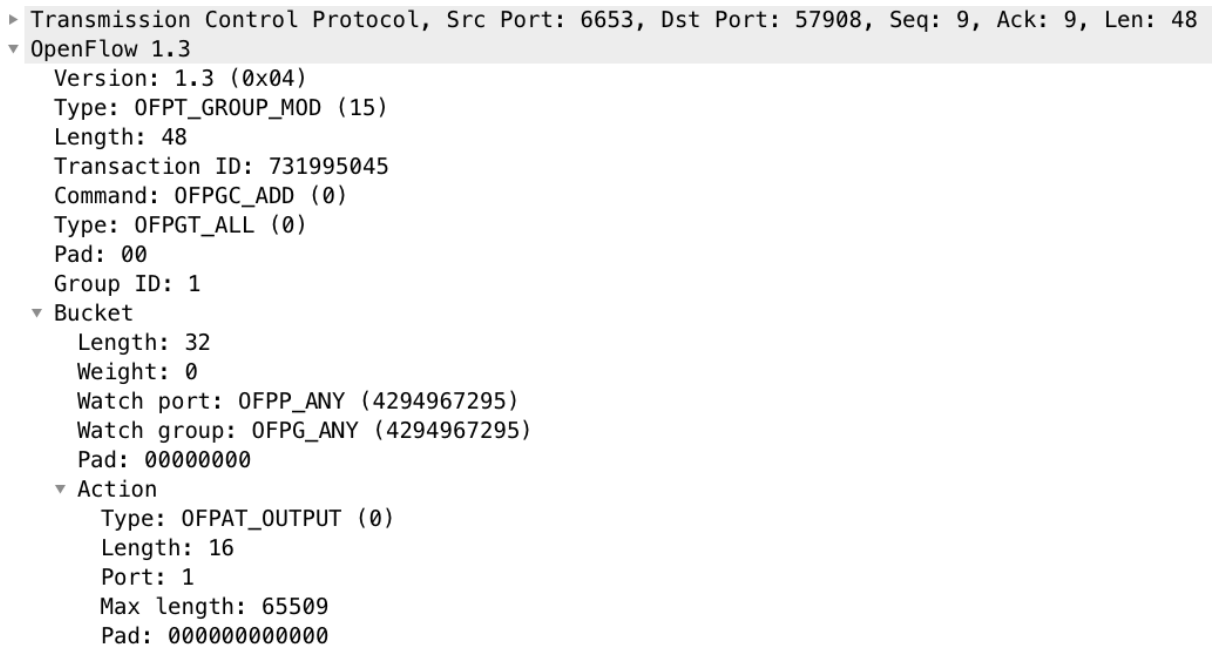


Figura B.2: Captura da configuração de Fluxo a partir do serviço OpenFlow Group Mode

POST Provisioning Request

http://localhost:8080/ARESAPI/provisioning

Serviço Provisioning Request da API ARES. Passa como parâmetros os atributos da classe Path. Retorna o status do provisionamento e os atributos da classe datapath.

Headers

Content-Type	application/json

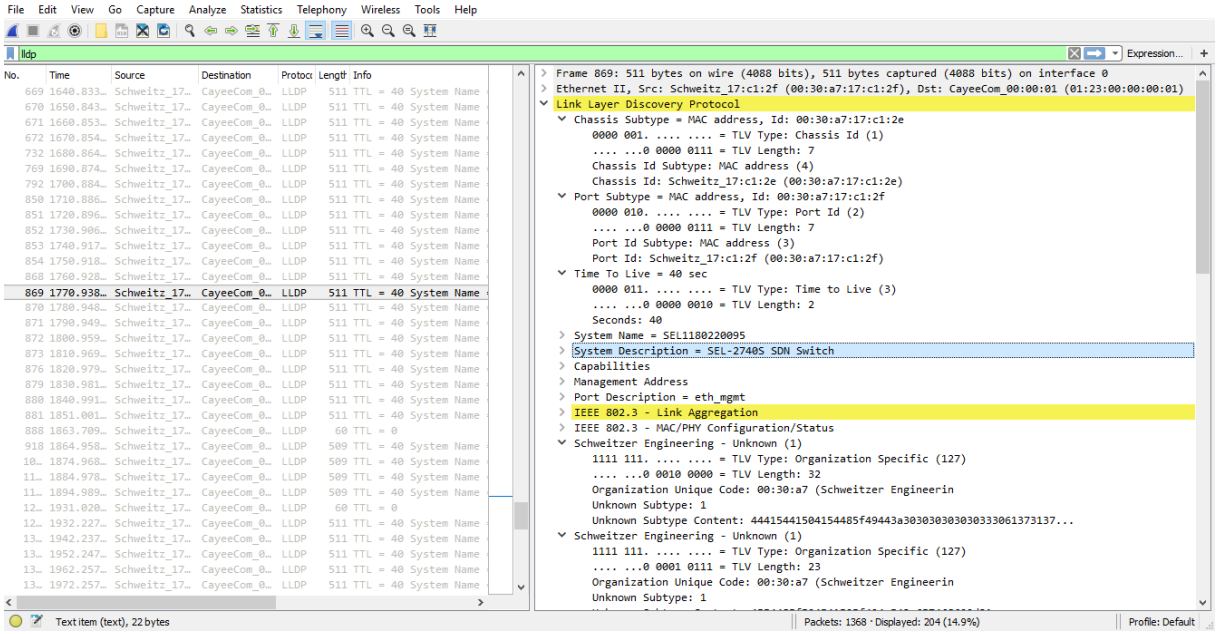
Body raw (application/json)

```
{
  "source": "00:00:00:00:00:01",
  "destination": {
    "dst1": "00:00:00:00:00:02",
    "dst2": "00:00:00:00:00:03"
  },
  "type": "tipo1A"
}
```

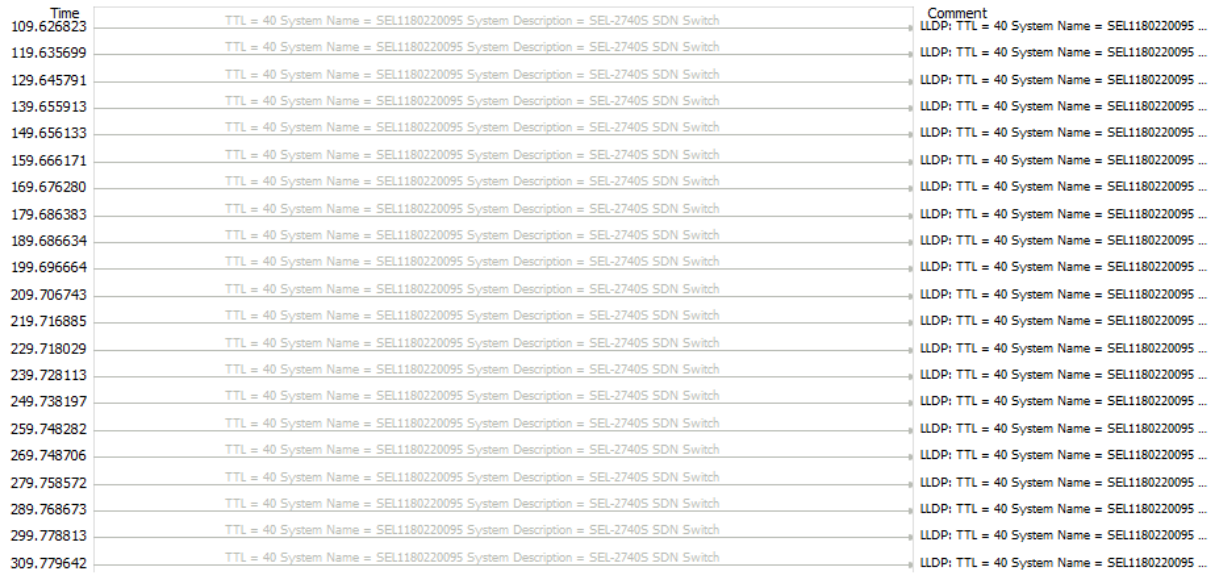
Example Request — Provisioning Request

```
curl --request POST \
  --url http://localhost:8080/ARESAPI/provisioning \
  --header 'Content-Type: application/json' \
  --data '{
  "source": "00:00:00:00:00:01",
  "destination": {
    "dst1": "00:00:00:00:00:02",
    "dst2": "00:00:00:00:00:03"
  },
  "type": "tipo1A"
}
```

Figura B.3: Implementação do Serviço *Provisioning* de Requisição

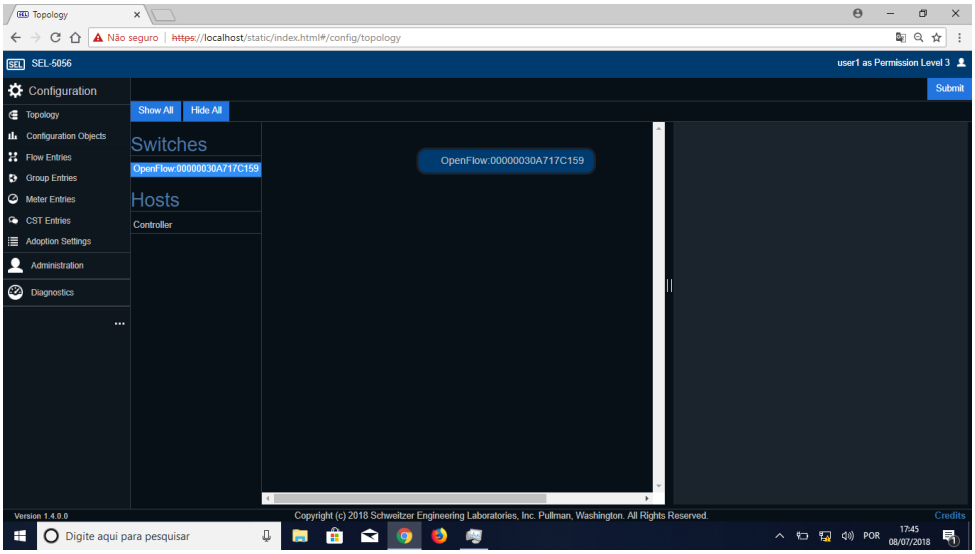


(a) Captura Pacotes LLDP.

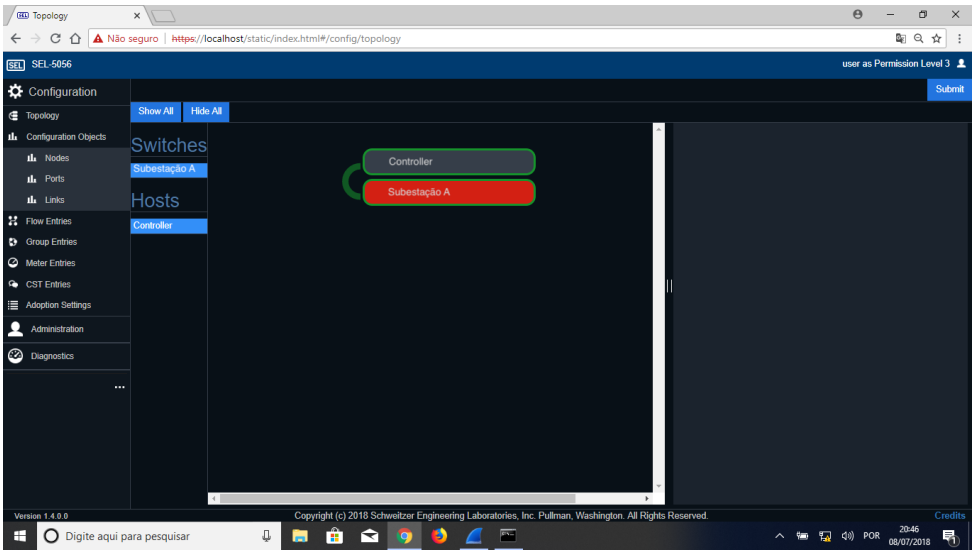


(b) *Wireshark Flow Graph.*

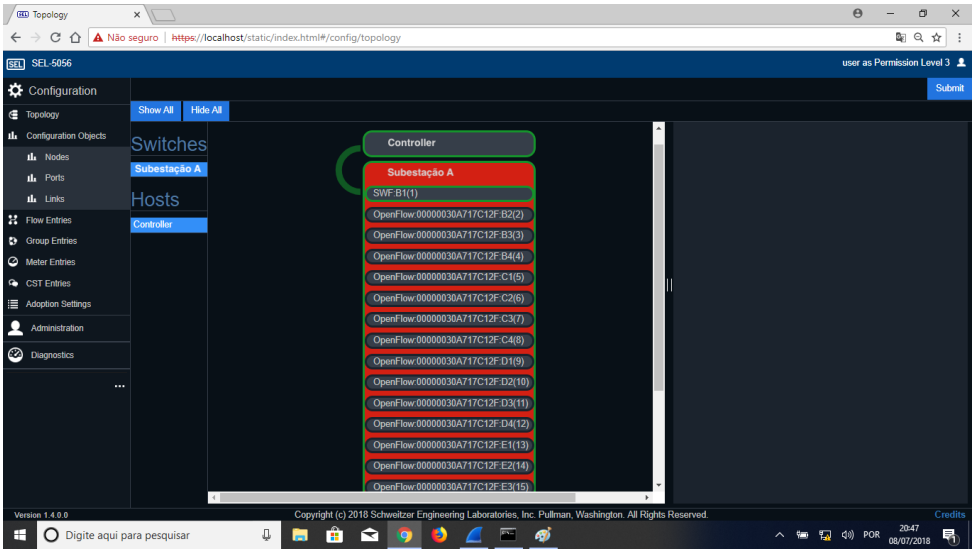
Figura B.4: Controlador SEL 5056 - Captura Pacotes LLDP.



(a) *Switch* da Subestação A.



(b) *Switch* da Subestação A.

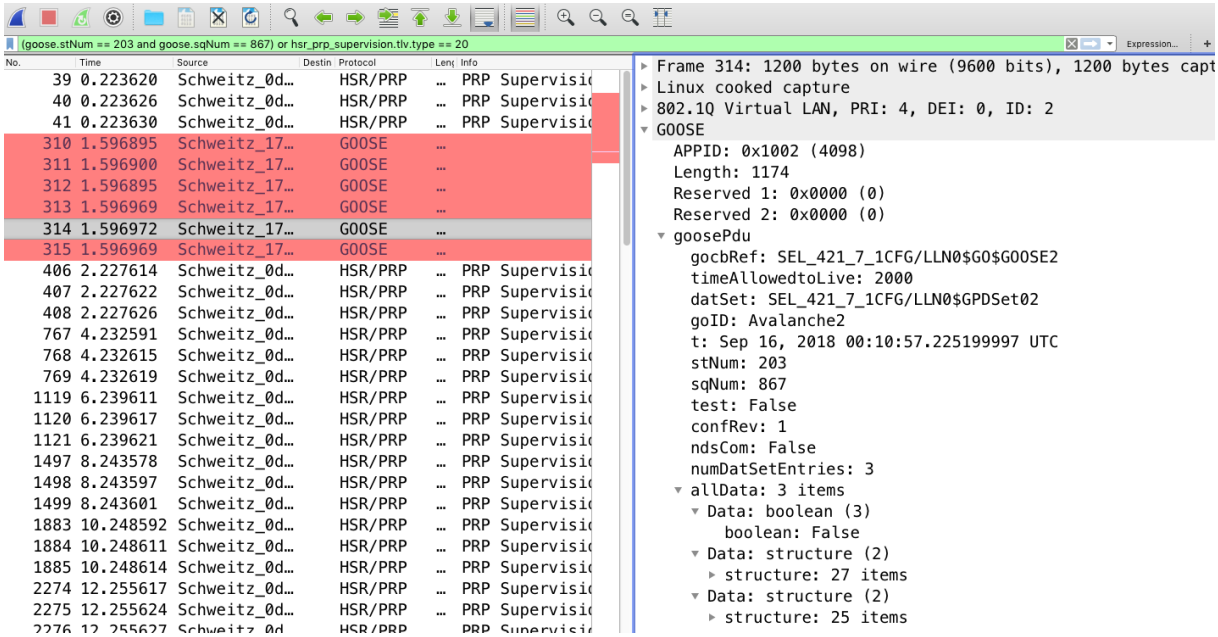


(c) Nomeação e portas.

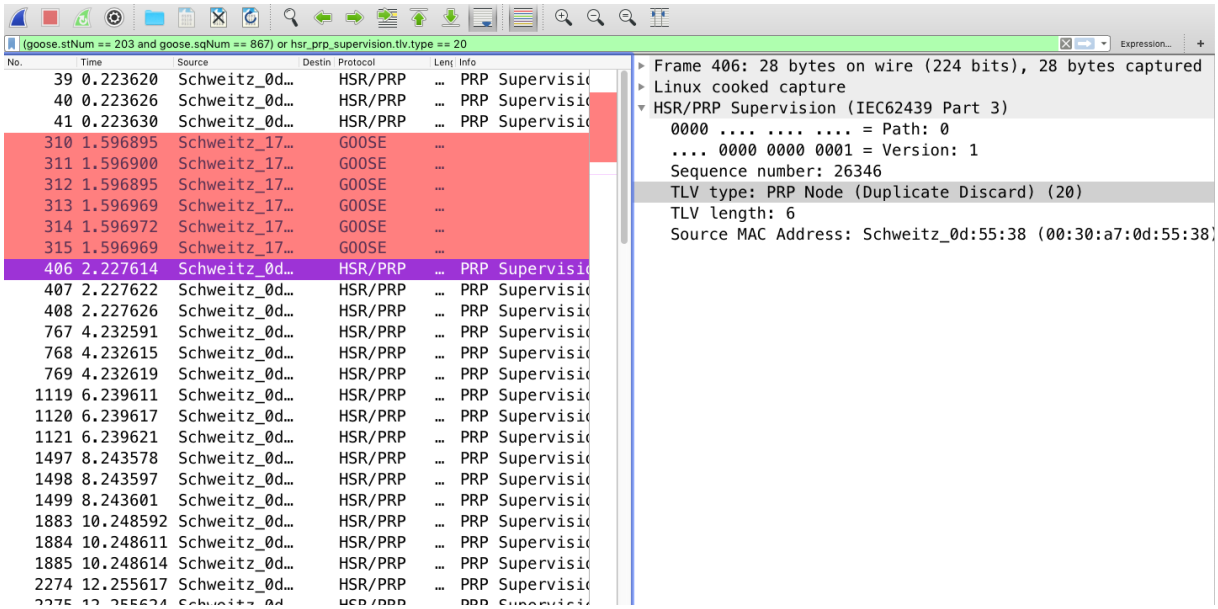
Figura B.5: Controlador SEL 5056 - Topologia - Processo de descoberta.

```
=>>ser

SEL_751A                                  Date: 08/18/2018   Time: 16:35:24
R1                                        Time Source: Internal

Serial No = 2008052312      FID = SEL-751A-R310-V0-Z007003-D20150206
CID = A306

#      DATE         TIME                ELEMENT              STATE
14   08/18/2018   16:35:21.382   SV01T                      Asserted
13   08/18/2018   16:35:21.386   SV01T                      Deasserted
12   08/18/2018   16:35:21.391   SV01T                      Asserted
11   08/18/2018   16:35:21.395   SV01T                      Deasserted
10   08/18/2018   16:35:21.399   SV01T                      Asserted
9    08/18/2018   16:35:21.403   SV01T                      Deasserted
8    08/18/2018   16:35:21.407   SV01T                      Asserted
7    08/18/2018   16:35:21.411   SV01T                      Deasserted
6    08/18/2018   16:35:21.416   SV01T                      Asserted
5    08/18/2018   16:35:21.420   SV01T                      Deasserted
4    08/18/2018   16:35:21.424   SV01T                      Asserted
3    08/18/2018   16:35:21.428   SV01T                      Deasserted
2    08/18/2018   16:35:21.432   SV01T                      Asserted
1    08/18/2018   16:35:21.436   SV01T                      Deasserted

=>>
```

Figura B.6: Exemplo da captura no SER da variável `SV01T`. Ela é ativada e desativada a cada 4ms.



(a) *Frame* GOOSE repetido.



(b) *Frame* de supervisão PRP/HSR

Figura B.7: Capturas *frames* em rede configurada com o PRP.

APÊNDICE C – Métodos para Reestabelecimentos da Rede de Comunicação em Caso de Falhas

Este apêndice descreve os métodos para restabelecimento da rede de comunicação em caso de falhas mais utilizados em subestações. São eles o RSTP, o PRP e o HSR. Além do funcionamento, as vantagens e desvantagens de cada um são descritos.

C.1 RSTP

O protocolo RSTP baseia-se na criação de melhores rotas para o tráfego dos dados em uma rede. A melhor rota é definida como sendo a que possui menor custo. Um exemplo de custo utilizado é o menor número de saltos (*hops*) entre o dispositivo fonte e o destino. Para isso, esse protocolo insere identificadores em *switches* e em suas portas para classificação. Com isso, torna-se possível o estabelecimento de uma rota ótima e rotas alternativas para situações onde ocorra uma interrupção na rede. O princípio de funcionamento do RSTP consiste na troca de informações, *Bridge Protocol Data Units*s (BPDUs), entre os *switches* da rede com o objetivo de encontrar um *switch* raiz e habilitar ou desabilitar portas para eliminar os *loops* na rede. Após a eleição do *switch* raiz, as melhores rotas da rede podem ser definidas [32]. Os *switches* utilizam os BPDUs para trocar informações entre eles e estabelecer as melhores rotas até o *switch* raiz. Uma porta que recebe um BPDU que contém o melhor caminho para o *switch* raiz torna-se a porta raiz desse *switch*. Todas as outras portas restantes transmitem os BPDUs contendo informações sobre a porta raiz.

Os estados das portas no RSTP podem ser [154]:

- *Discarding*, significando que a porta está devolvendo pacotes de dados diferentes de BPDUs
- *Learning*, significando que a porta está aprendendo informações de pacotes de configuração

- *Forwarding*, significando que a porta está repassando pacotes de dados diferentes de BPDUs.

Além disso, as portas podem assumir diferentes funções, através das quais será estabelecida a melhor rota para o tráfego de dados e a rota alternativa, em caso de falha na rede. As funções que uma porta pode assumir são [32]:

- Porta raiz: possui o melhor caminho para o *switch* raiz que é geralmente o caminho de menor custo. Ressalta-se que o *switch* raiz não possui porta raiz;
- Porta designada: encaminha BPDUs dentro de um segmento. Existente em *switches* raiz e não-raiz;
- Porta alternativa: porta que leva a outro caminho (redundante) para o *switch* raiz e, por isso, tal porta assume o estado de descarte (bloqueio) durante uma topologia estável em uso. No caso da porta raiz falhar, a porta alternativa se torna imediatamente a porta raiz, sem esperar a rede convergir;
- Porta de backup: porta adicional, redundante, no estado de descarte (bloqueio) durante uma topologia estável em uso. No caso da porta designada falhar, a porta de backup se torna imediatamente a porta designada (para o respectivo segmento), sem esperar a rede convergir.

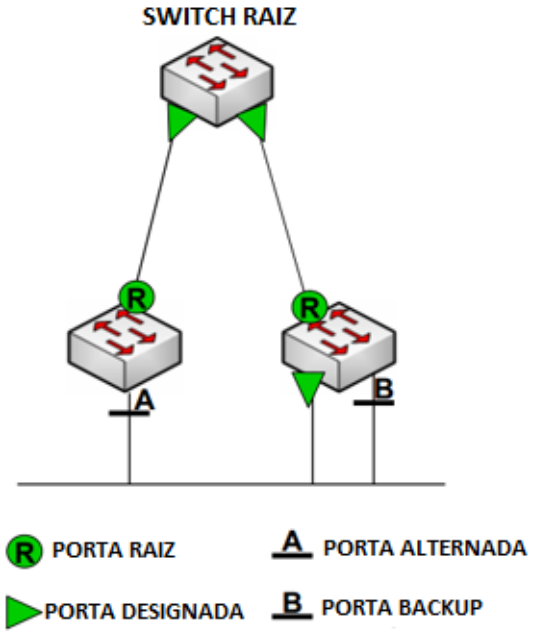


Figura C.1: Exemplo de topologia indicando o estado das portas [32].

De acordo com o estado de cada porta, será estabelecida a melhor rota e definidas rotas alternativas para o reestabelecimento da rede, em caso de uma falha na mesma.

Contudo, para que uma falha seja caracterizada, os BPDUs utilizam três vezes o hello-time (*default* de 2 segundos) para considerar um enlace em falha . Ou seja, se em 6 segundos não houver resposta, o *switch* já considera a conexão perdida e seta seus BPDUs para informar os demais switches [154].

C.1.1 Vantagens e Desvantagens

Uma das vantagens do RSTP é que esse protocolo não precisa estar implementado nos dispositivos finais da rede, tais como os IEDs de uma rede de automação de uma subestação de energia. Basta que os *switches* dessa rede possuam suporte a esse protocolo, para que seja possível restabelecer a rede em caso de uma interrupção.

Uma desvantagem do RSTP reside no tempo de recomposição da rede, que fica em torno de 2 segundos [94] para redes muito extensas, ou até mais. Em uma rede de automação de uma subestação um tempo de recomposição dessa magnitude pode causar perdas de mensagens importantes, como por exemplo, um sinal de disparo para abertura de um disjuntor, que eliminará um curto-circuito no sistema elétrico.

Contudo, o tempo para recomposição do RSTP dependente muito do tamanho e da topologia de rede. Além disso, o *Spanning Tree Algorithm* (STA) implementado e os ajustes de custo e prioridade de portas dos *switches* também causam uma grande variação nesse tempo. No estudo comparativo realizado por Chelluri et al. [42], por exemplo, os autores testaram diversas topologias e configurações e encontraram no máximo 15ms de recomposição com uma topologia específica da empresa em que trabalham chamada de *Ladder*.

C.2 PRP

O PRP [84] implementa o princípio de redundância nos dispositivos através da conexão destes em duas redes locais (LANs) de comunicação independentes A e B e que operam em paralelo. Para isso, esses dispositivos precisam ter duas interfaces de rede compatíveis com o protocolo PRP. Esses dispositivos são conhecidos como *Double attached node implementing PRP*s (DANPs). Um DANP de origem envia a mensagem através das duas redes LAN's a ele conectadas, e um DANP de destino recebe essa mensagem através das duas redes dentro de uma janela de tempo, usando então a primeira mensagem e descartando a mensagem duplicada [94].

Os dispositivos que não possuem suporte ao PRP são chamados de *Single Attached Node*s (SANs). Quando SANs precisam ser conectados às redes redundantes, são utilizados dispositivos denominados de RedBox (*Redundancy Box*). O SAN conecta-se ao RedBox através de sua única interface de rede e o RedBox duplica essa interface, conectando-se às

duas redes independentes, fornecendo assim a redundância ao dispositivo SAN [84, 73]

A Figura C.2 mostra uma rede redundante, com a utilização de duas redes independentes, as quais podem ter topologias diferentes, e.g., anel, estrela, malha, etc.

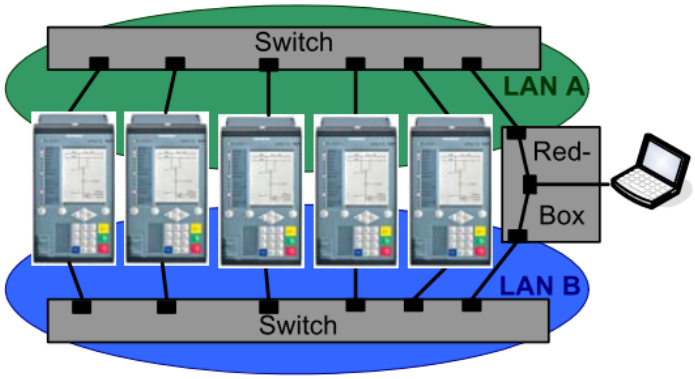


Figura C.2: Arquitetura simplificada de uma rede com aplicação do PRP [73].

Diversas topologias podem ser aplicadas em redes redundantes que utilizam o PRP. Abaixo são exemplificadas as topologias descritas na Norma IEC 62439-3 [84].

A Figura C.3 ilustra a topologia linear. A Figura C.4, ilustra a rede PRP composta por duas redes independentes com a topologia em anel.

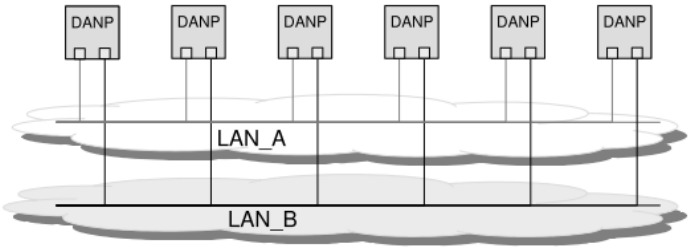


Figura C.3: Rede PRP com topologia em barramento [84].

Os DANPs possuem duas portas físicas que operam em paralelo e que estão ligadas as camadas de comunicação superiores através da camada de enlace, nesse caso denominada *Link Redundant Entity* (LRE), como mostra a Figura C.5 [84].

O LRE possui duas tarefas: gerenciamento das mensagens duplicadas e gerenciamento da redundância. No entanto, para as camadas superiores esse gerenciamento é transparente. Quando uma mensagem é recebida através das camadas superiores, o LRE envia essa mensagem através das duas portas quase ao mesmo tempo. As duas mensagens trafegam através das duas redes com diferentes atrasos [96].

Quando mensagens são recebidas através das duas redes A e B, o LRE encaminha a primeira mensagem recebida para as camadas superiores e descarta a mensagem duplicada, caso a mesma chegue. Para o gerenciamento da redundância, o LRE adiciona ao cabeçalho

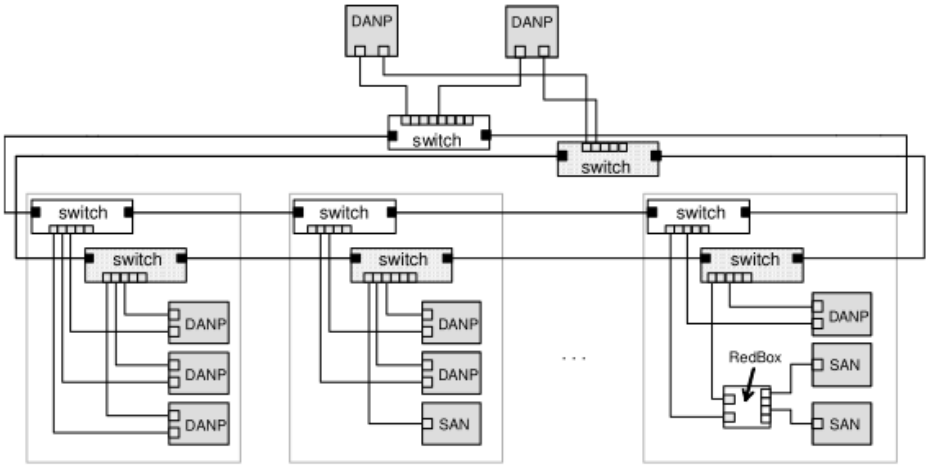


Figura C.4: Rede redundante PRP com topologia em anel [84].

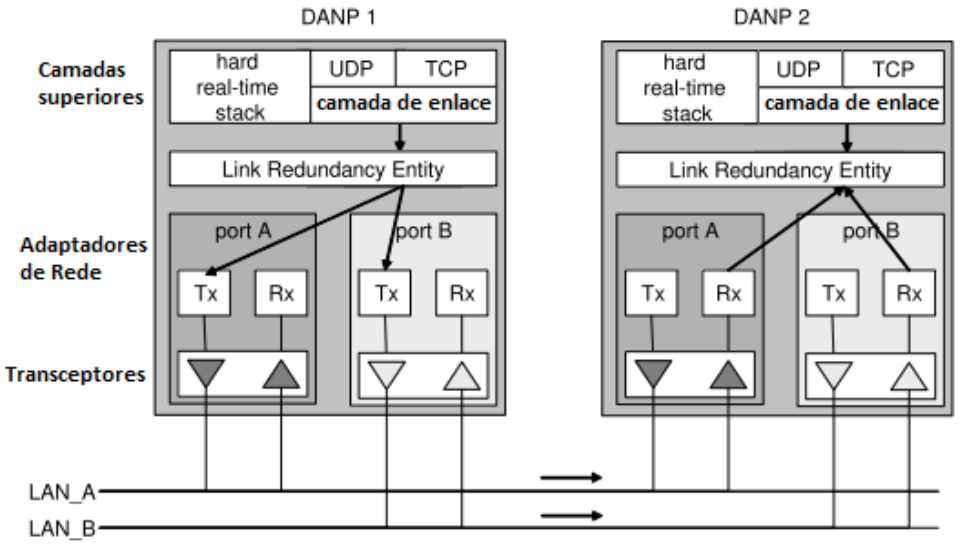


Figura C.5: Rede redundante PRP com topologia em anel [84].

da mensagem o *Redundancy Check Trailer* (RCT), incluindo um número sequencial nas mensagens duplicadas que são enviadas, para rastreamento das mesmas.

A cada mensagem enviada por um DANP, ele aumenta um número sequencial e envia as duas mensagens (quase idênticas) através das duas redes. Adicionalmente, o LRE envia periodicamente mensagens de supervisão PRP e avalia a supervisão PRP dos outros DANPs [96].

C.2.1 Compatibilidade entre SANs e DANPs

Dispositivos SANs, são dispositivos que conectam-se a apenas uma das redes por não terem suporte ao protocolo PRP. Um SAN conectado a uma LAN não pode comunicar-se com outro SAN diretamente conectado à outra LAN. No entanto, um SAN pode se comunicar com todos os DANPs conectados às duas redes. Apesar dos SANs não possuírem suporte

ao PRP, os DANPs geram mensagens que os SANs compreendem, pois eles ignoram o RCT presente nas mensagens geradas pelos DANPs. Também os DANPs compreendem as mensagens geradas pelos SANs, uma vez que apenas não existe o RCT anexado à mensagem. Se um DANP não identifica que o dispositivo remoto emissor/receptor da mensagem é um DANP, ele o considera um SAN [84].

C.2.2 Vantagens e Desvantagens

Um dos benefícios do uso do método de redundância PRP é a disponibilidade de todo o sistema. Isso é possível pela existência de duas redes totalmente independentes entre si onde, no caso de ocorrência de falha em uma das redes, a comunicação ainda é possível através da outra rede sã. A conexão de novos dispositivos às redes é uma tarefa simples, desde que os novos dispositivos falem PRP. Basta conectar o dispositivo DANP a uma das redes e o mesmo já estará pronto para iniciar a comunicação. Caso seja necessário conectar um SAN, que não tem o PRP, o mesmo conecta-se a um RedBox e, a partir deste, conecta-se a ambas as redes. Nesse caso, também não é necessária nenhuma configuração adicional da rede, porém é necessária a inclusão de mais um dispositivo.

Há, no entanto, de se considerar as desvantagens de uma arquitetura com o uso do PRP. Como nesse método as mensagens precisam ser duplicadas, existe a necessidade de fabricação de *switches* mais robustos, pois as mensagens precisam ser processadas duas vezes no recebimento e precisam ser geradas duas vezes no envio. Para que o tempo de vida útil destes equipamentos não seja afetado, o projeto de construção dos DANPs e RedBoxs precisa levar em conta essa característica para produção de equipamentos com componentes duplicados e mais robustos. Caso contrário, a vida útil do equipamento e o tempo para processar mensagens será comprometido, o que afeta diretamente a rede da subestação.

Também, em redes onde seja necessário o uso de um dispositivo RedBox para conexão de um SAN às redes redundantes, uma falha simples nesse dispositivo gera a perda de comunicação com o SAN a ele conectado. Caso esse dispositivo SAN seja responsável, por exemplo, por fornecer as informações de supervisão ao centro de controle do sistema elétrico, haverá a perda dessa supervisão e, consequentemente, grande impacto ao processo de gerenciamento do sistema elétrico regional ou, até mesmo, nacional. Na prática, acrescenta-se um ponto de falha na rede único, sem redundância, quando o RedBox é usado.

Outra característica é que as duas redes não possuem conexão entre si e são, portanto, consideradas como independentes em relação a falhas. No entanto, a redundância pode ser eliminada em caso de falha em pontos comuns, como fontes de alimentação compartilhadas entre os dispositivos conectados à essas redes.

C.3 Método de Redundância HSR

Assim como acontece no método de redundância PRP, um dispositivo *Doubly Attached Node with HSR Protocol* (DANH) possui duas portas que operam paralelamente.

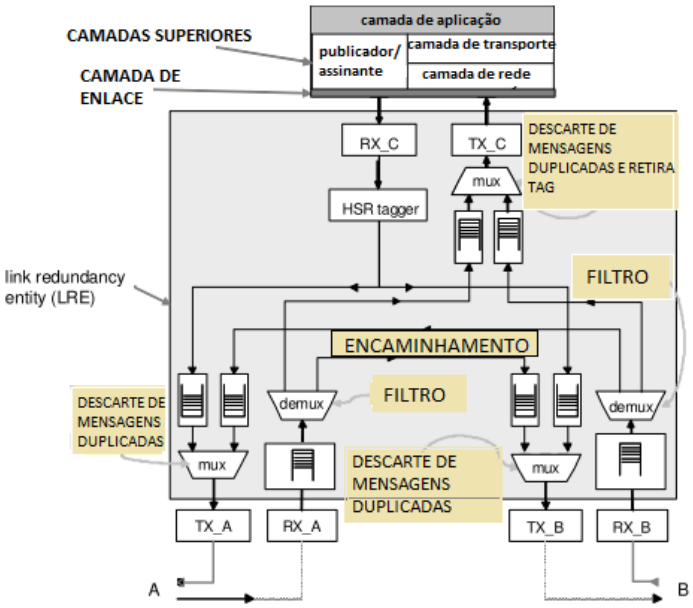


Figura C.6: Estrutura conceitual de *switches* de um dispositivo DANH [84].

Uma topologia básica de uma rede HSR consiste de elementos DANH interligados em anel através de conexões full-duplex (transmitem e recebem dados). Podem existir dois tipos de comunicação: multicast, onde a mensagem tem vários destinatários ou *unicast*, onde a mensagem possui um destinatário único. As Figuras C.6 e C.7 mostram redes HSR com comunicação *multicast* e *unicast*, respectivamente [84].

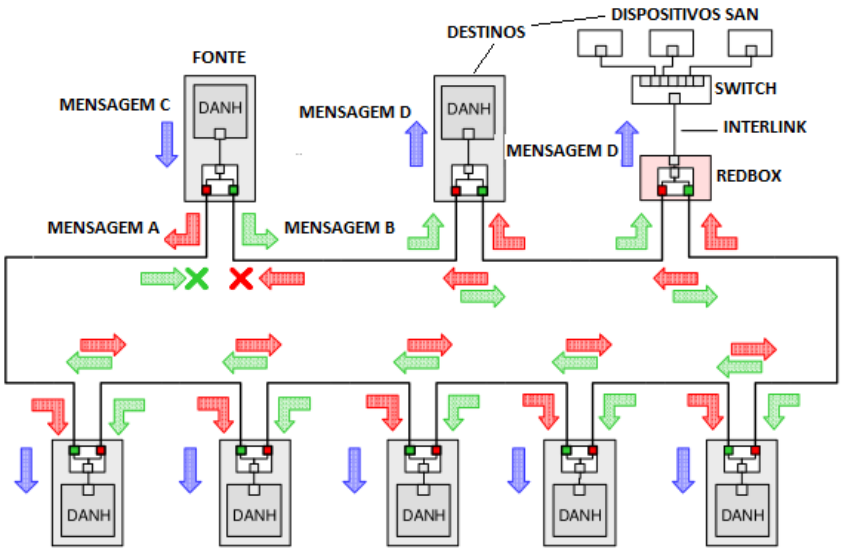


Figura C.7: Exemplo de HSR em configuração anel, com comunicação *multicast* [84].

Em ambos os tipos de comunicação, um dispositivo DANH, fonte da informação, envia uma mensagem recebida das camadas superiores camadas de transporte e rede, insere uma tag HSR contendo um número sequencial, que possibilita a identificação de mensagens duplicadas pelos receptores das mesmas, e envia essa mensagem pelas duas portas disponíveis, criando uma "Mensagem A" e uma "Mensagem B". Um dispositivo DANH de destino recebe pelas suas duas portas, duas mensagens A e B dentro de um certo intervalo. Após esse recebimento, o DANH de destino retira o tag HSR da primeira mensagem recebida e passa a mensagem às camadas superiores que utilizarão a informação, descartando então qualquer mensagem duplicada (Mensagem B) [84].

Os DANHs possuem suporte à funcionalidade bridge (IEEE 802.1D) e encaminham mensagens de uma porta para outra, exceto se uma mensagem já foi enviada para uma direção anteriormente [95].

No caso de DANHs de destino em uma comunicação *unicast*, a mensagem não será encaminhada para os outros dispositivos subsequentes conectados ao anel, uma vez que ele é o único destinatário da mensagem.

Um dispositivo DANH possui uma estrutura, de forma conceitual, evidenciada pela Figura C.6. As duas portas A e B e a porta C do dispositivo são conectadas através do LRE, que possui uma matriz de comutação que permite encaminhar mensagens de uma porta à outra. O LRE apresenta às camadas superiores a mesma interface que um transceptor Ethernet apresentaria, como se o processo de identificação e duplicação das mensagens fosse transparente para essas camadas.

Nas Figuras C.7 e C.8 pode-se ver exemplos de topologia em anel para uso do método de redundância HSR, para comunicações *multicast* e *unicast*, respectivamente.

As setas vermelhas representam a Mensagem A, as setas verdes a Mensagem B, e as setas azuis as mensagens que não são HSR e são trocadas entre os dispositivos e o anel. A cruz é e mensagem removida do anel, que nesse caso voltou ao destinatário.

Outra possibilidade de topologia é ter-se dois anéis HSR, que devem ser conectados através de dispositivos chamados de *QuadBox* (*Quadruple Box*). Esse método é usado quando a capacidade de tráfego de um anel único é superada. Pode-se também utilizar dois *QuadBoxes*, como na Figura C.9, para manter a rede ativa em caso de uma falha simples em um dos *QuadBoxes*.

Um dispositivo DANH pode operar em diversos modos de encaminhamento de pacotes, que podem ser alterados em tempo real utilizando comandos de gerenciamento. Mas o modo padrão nos dispositivos DANH é o modo H. Nesse modo, o DANH encaminha mensagens com tag HSR. Para o encaminhamento e descarte de mensagens duplicadas o seguinte roteiro é seguido:

1. Se o DANH é o nó de destino:

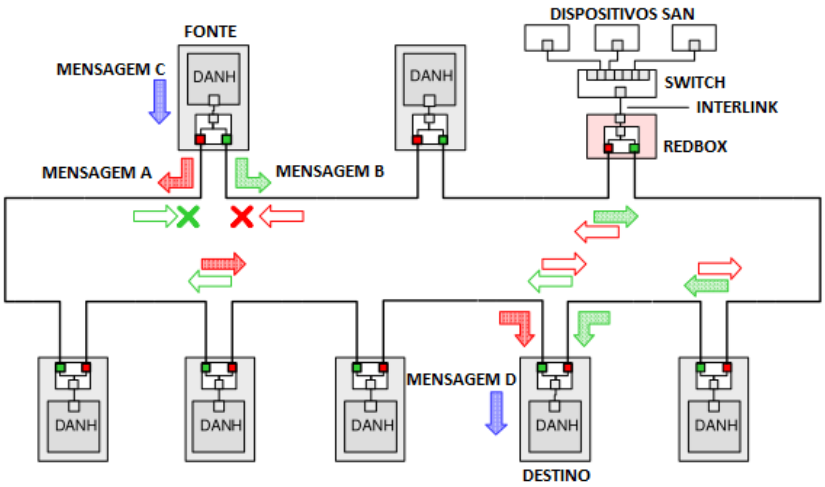


Figura C.8: Exemplo de HSR em configuração anel, com comunicação *unicast* [84].

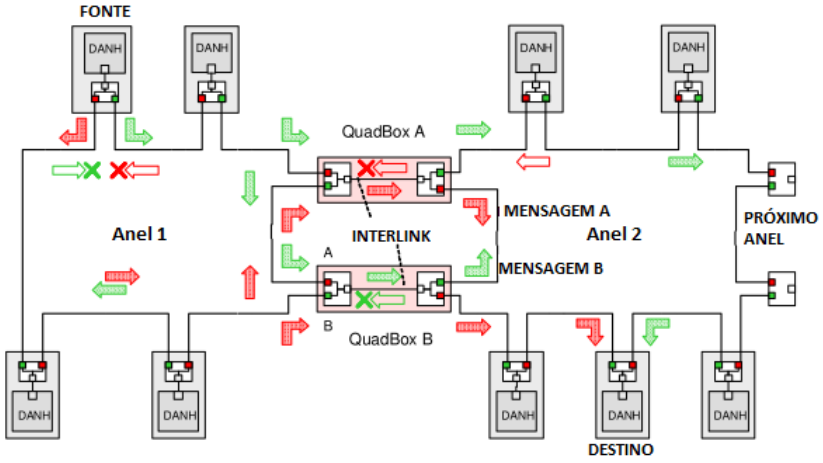


Figura C.9: Exemplo de HSR com dois anéis [84].

- Se for a primeira ocorrência da mensagem na interface da camada de enlace: Registra a ocorrência da mensagem e remove o tag HSR para passar a mensagem modificada à camada de enlace.
- Senão (essa não é a primeira ocorrência da mensagem na interface da camada de enlace): Registra a ocorrência da mensagem; Não passa a mensagem para a camada de enlace.

2. Senão (o DANH não é o nó de destino): Não passa a mensagem para a camada de enlace.

3. Se esse DANH não for o único destino (*multicast* ou *unicast* para outro nó):

   - Se essa é a primeira ocorrência da mensagem na segunda porta: Registra a ocorrência da mensagem; Coloca na fila a mensagem inalterada (com tag HSR) para encaminhamento pela segunda porta.

- Senão (essa não é a primeira ocorrência da mensagem na segunda porta): Registra a ocorrência da mensagem; Descarta a mensagem.

C.3.1 Vantagens e Desvantagens

Em comparação ao PRP, o método de redundância HSR permite reduzir pela metade o tamanho da infraestrutura de rede, uma vez que se baseia na interligação de dispositivos em anel e dispensa o uso de *switches* ao longo dessa rede, uma vez que o encaminhamento das mensagens se dá pelos próprios dispositivos da rede (DANH's). Isso é possível pois esses dispositivos possuem a funcionalidade de *switch* em suas portas. Para aumentar a confiabilidade dessa rede, pode-se criar um segundo anel, interligando os dois anéis através de dispositivos QuadBox, porém a vantagem de redução da infraestrutura seria perdida.

A desvantagem reside na topologia em anel da rede HSR, que limita o número de dispositivos que podem compor a rede, uma vez que a taxa de ocupação da banda de comunicação é proporcionalmente aumentada com a inclusão de mais dispositivos na rede.

Além disso, os dispositivos sofrem a mesma sobrecarga descrita no método PRP, e por isso precisam de um *switches* mais robusto que possam processar a duplicação pedida pelo método. Porém, no HSR tem-se um agravante. Como o método não precisa de *switches* os IEDs participantes da rede processam todo o tráfego como se fosse *switches*, o que aumenta ainda mais a sobrecarga nos IEDs que tem *switches* embarcados mais fracos.

Ademais, o carregamento da rede é demasiadamente grande pois ocupa-se pelo menos a metade da banda da rede apenas com mensagens duplicadas que serão descartadas. Consequentemente, a latência da comunicação é prejudicada, podendo não atingir os requisitos dos protocolos da norma IEC 61850, que exigem tempos de entrega de mensagens de até 3 milissegundos, no caso de mensagens GOOSE.