UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
DEPARTAMENTO DE INFORMÁTICA

JULIANO VICTOR SILVA RAMOS

ANÁLISE, IMPLANTAÇÃO E GERENCIAMENTO DE UMA REDE DE COMUNICAÇÃO PARA O PROJETO SELF-HEALING DA CEMAR

SÃO LUÍS
2016

JULIANO VICTOR SILVA RAMOS

ANÁLISE, IMPLANTAÇÃO E GERENCIAMENTO DE UMA REDE DE COMUNICAÇÃO PARA O PROJETO SELF-HEALING DA CEMAR

Monografia do aluno **Juliano Victor Silva Ramos** apresentada ao Curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Carlos Alberto Brandão Barbosa Leite

Coordenador: Prof. Msc. Carlos Eduardo Portela Serra de Castro

SÃO LUIS
2016

JULIANO VICTOR SILVA RAMOS

ANÁLISE, IMPLANTAÇÃO E GERENCIAMENTO DE UMA REDE DE COMUNICAÇÃO PARA O PROJETO SELF-HEALING DA CEMAR

Parte manuscrita do Projeto de Graduação do aluno **Juliano Victor Silva Ramos**, apresentado ao Departamento de Informática do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Maranhão, como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Aprovada em 06 de abril de 2016.

COMISSÃO EXAMINADORA:

Prof. Dr. Carlos Alberto Brandão Barbosa Leite
UFMA
Orientador

Charles Fonseca
CEMAR
Coorientador

Prof. Msc. Carlos Eduardo Portela Serra de Castro
UFMA
Examinador

Prof. Msc. Luiz Henrique Neves Rodrigues
UFMA
Examinador

Ramos, Juliano Victor Silva

Análise, implantação e gerenciamento de uma rede de comunicação para o Projeto *Self-Healing* da CEMAR/Juliano Victor Silva Ramos. – São Luís, 2016.

80f.

Orientador: Carlos Alberto Brandão Barbosa Leite

Monografia (Graduação) – Universidade Federal do Maranhão, Curso de Ciência da Computação, 2016.

1. Smart Grids 2. Self-Healing 3. Redes de Computadores, 4. Gerenciamento de rede

CDU 004.7

À minha família, namorada e amigos por todo o apoio e carinho durante toda esta jornada.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”.

Marthin Luther King

Agradeço primeiramente a Deus pela vida e saúde que me concedeu até hoje.

Agradeço à minha família, em especial à minha avó Graça, meu avô Kleber, minha mãe Juliana e meus tios Kleber Júnior e Gustavo pela força e apoio ao longo dos anos, principais responsáveis por fazer de mim o que sou hoje.

Agradeço à minha namorada Lília Karoline por todo apoio e afeto dado nos últimos meses e por ter tornado meus dias mais felizes.

Agradeço aos muitos amigos da graduação pelo companheirismo ao longo desses cinco anos, pelas ajudas nos momentos de dificuldade e pelos vários momentos de diversão.

Agradeço a todos os professores da UFMA com os quais estudei, que com paciência e dedicação transmitiram todo o conhecimento necessário para que eu chegasse ao fim desta graduação.

Agradeço também aos amigos e companheiros da CEMAR, pela paciência com que me transmitiram todo o conhecimento que adquiri ao longo desses quase dois anos de estágio e pela compreensão nos meus momentos de maiores dificuldades.

Por fim, agradeço a todos que me ajudaram direta e indiretamente ao longo desta jornada.

RESUMO

A qualidade da energia entregue aos clientes das empresas concessionárias de distribuição de energia elétrica é cada vez mais exigida, seja por parte dos clientes ou por parte dos órgãos reguladores. As pressões pela diminuição da duração (DEC) de uma falta de energia ou a sua frequência (FEC) são os maiores desafios dos profissionais incumbidos da manutenção dos sistemas de distribuição. Grandes investimentos em trocas de cabos dos alimentadores e construções de novas subestações já não são suficientes para garantia dessa qualidade. É necessário o desenvolvimento de ferramentas que auxiliem os nessa atividade. Neste cenário nasce a necessidade de investimentos em tecnologias que minimizem as perdas de grandes blocos de clientes em caso de falhas e que consigam reestabelecer o quanto antes a energia para estes quando a falta for inevitável. O Self Healing (SH) é um segmento do Smart Grid que viabiliza as manobras de chaves dos alimentadores com o propósito acima. Uma das garantias que o SH funcione corretamente é este possuir um sistema de comunicação confiável. A proposta desse trabalho é projetar e construir a rede Ethernet sobre fibra óptica e desenvolver um sistema para seu gerenciamento, tendo como prioridades garantir a robustez, segurança, diagnósticos de falhas e correção, contribuindo assim para aumentar a disponibilidade do SH e, consequentemente, a qualidade da energia entregue aos consumidores.

Palavras-chaves: *Smart Grids, Self-Healing*, Redes de Computadores, Gerenciamento de Rede.

ABSTRACT

The quality of energy delivered to customers of electricity distribution companies is increasingly required, by either customers or regulatory agencies. The pressures for shorter duration of a lack of energy (DEC) or frequency (FEC) are the biggest challenges of the professionals in charge of maintenance of the distribution systems. Large investments in cable swapping of feeders and substations new buildings are no longer sufficient to guarantee this quality. It is necessary to develop tools to assist them in this activity. In this scenario arises the need for investments in technologies that minimize the loss of major clients blocks in case of failure and are able to re-establish as soon as possible the power to these when the fault is inevitable. Self-Healing (SH) is a Smart Grid segment that enables maneuvers of feeder's switches for the purpose above. One of the guarantees that the SH function correctly that it contains a reliable communication system. The purpose of this work is to design and build a fiber optic Ethernet network and develop a system for its management, having as priorities to ensure robustness, security, fault diagnosis and correction, thereby increasing the availability of the SH system and, consequently, the power quality delivered to consumers.

Keywords: Smart Grids, Self-Healing, Computer Networks, Network Management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABRADEE	Associação Brasileira de Distribuidores de Energia Elétrica
ANEEL	Agência Nacional de Energia Elétrica
ARPANET	*Advanced Research Projects Agency Network*
BPDU	*Bridge Protocol Data Unit*
BT	Baixa Tensão
CAD	*Computer-Aided Design*
CEMAR	Companhia Energética do Maranhão
CH	Chave
CIDR	*Classless InterDomain Routing*
COELCE	Companhia Energética do Ceará
COI	Centro de Operações Integradas
DEC	Duração Equivalente de Interrupção por Unidade Consumidora
DGC	Desempenho Geral de Continuidade
DIC	Duração de Interrupção Individual por Unidade Consumidora
DNP	*Distribuited Network Protocol*
DoD	*Departament of Defense*
EBITDA	*Earnings Before Interest, Taxes, Depreciation and Amortization*
EUA	Estados Unidos da América
FEC	Frequência Equivalente de Interrupção por Unidade Consumidora
FTP	*File Transfer Protocol*
GPRS	*General Packet Radio Services*
HTTP	*Hyper Text Transfer Protocol*
IED	*Intelligent Eletronic Device*
IEEE	Institute of Electrical and Electronics Engineers
IETF	*Internet Engineer Task Force*
IHM	Interface Homem-Máquina
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MAC	*Media Access Control*
MIB	*Management Information Base*

NA	Normalmente Aberta
NF	Normalmente Fechada
OSI	*Open Systems Interconnect*
PRODIST	Procedimentos de Distribuição do Sistema Elétrico Nacional
RD	Rede de Distribuição
REI	Redes Elétricas Inteligentes
RFC	*Request for Comments*
RL	Religador
SCADA	*Supervisory Control and Data Acquisition*
SE	Subestação
SEP	Sistemas Elétricos de Potência
SH	*Self-Healing*
SMI	*Structure of Management Information*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Mail Protocol*
STP	*Spanning Tree Protocol*
TCP	*Transfer Control Protocol*
TTL	*Time to Live*
UDP	*User Datagram Protocol*
UTR	Unidade Terminal Remota
VLAN	*Virtual Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

Este trabalho visa descrever as etapas de planejamento, implementação e gerenciamento de uma rede de comunicação projetada para atender ao sistema *Self-Healing* da Companhia Energética do Maranhão – CEMAR.

Este primeiro capítulo pretende explicar as demandas atuais do sistema de distribuição de energia elétrica no Brasil, demonstrando a necessidade da utilização de soluções *Smart Grid*, como o *Self-Healing*, além da importância de uma rede de comunicação robusta neste contexto. Demonstra-se ainda o processo de desenvolvimento deste trabalho, sua motivação, objetivos e estrutura.

1.1 Problemática

Uma rede aérea de distribuição de energia elétrica está sujeita a diversos fatores que podem ocasionar a falta de energia. Suas linhas estão expostas a riscos como abalroamento de postes, queda de galhos de árvores e intempéries da natureza, elementos que podem causar faltas permanentes ou temporárias.

O DEC (Duração Equivalente por Unidade Consumidora) e o FEC (Frequência Equivalente por Unidade Consumidora) gerados por essas faltas são um dos principais índices de qualidade para uma distribuidora de energia elétrica. A ANEEL (Agência Nacional de Energia Elétrica), órgão que regulamenta o serviço das distribuidoras em todo o país, controla esses índices e aplica severas multas em caso de violações. Por isso, percebemos que o rápido reestabelecimento de faltas na rede de distribuição e, por conseguinte, a melhora do indicador FEC, impacta diretamente nos valores pagos em multas pela empresa e, logicamente, em seu EBITDA[1], tornando válidos investimos em tecnologias que auxiliem nesta área.

Neste cenário encontram-se as *Smart Grids*, redes de distribuição de energia elétrica inteligentes, que agregam equipamentos e serviços de tecnologia da informação a

[1] Ebitda é a sigla em inglês para *earnings before interest, taxes, depreciation and amortization*, que traduzido literalmente para o português significa: "Lucros antes de juros, impostos, depreciação e amortização" (Lajida).

fim de prover um maior controle da rede e possibilitar a implantação de recursos de automação a esta. Dentro deste escopo, encontram-se as aplicações *Self-Healing*, que permitem, através do monitoramento do estado da rede e a execução de comandos remotos em equipamentos de proteção, a reposição do fornecimento de energia ao maior número de clientes afetados por uma falta no menor tempo possível, remanejando as cargas para outras fontes de suprimento. Com a utilização de equipamentos seccionadores, um sistema SH (*Self-Healing*) pode isolar o trecho comprometido da rede, auxiliando na localização do problema e, consequentemente, tornando mais rápido o reparo definitivo da rede.

1.2 Motivação

A indisponibilidade de comunicação torna um sistema SH inoperante e informações destoantes da realidade podem ocasionar manobras incorretas e até o agravamento da falta existente. Tendo em vista a importância da confiabilidade da rede de comunicação para uma aplicação SH, desenvolveu-se um estudo para a escolha das tecnologias a serem utilizadas na rede de comunicação do projeto *Self-Healing* da CEMAR, de forma que esta atendesse às necessidades, considerando a estrutura já presente na empresa, tanto em relação a equipamentos de comunicação, quanto a equipamentos de proteção da rede elétrica.

1.3 Objetivos

Esta monografia visa relatar o processo de planejamento, implantação, testes e gerenciamento de uma rede de comunicação ethernet via fibra óptica para o projeto *Self-Healing* da CEMAR. Em específico os tópicos:

- Explanar sobre o conceito de Smart Grids e sua aplicabilidade no setor elétrico brasileiro;

- Realizar um breve estudo sobre sistemas elétricos de potência e sistemas de distribuição de energia elétrica;

- Explanar sobre sistemas SCADA[2] aplicados à distribuição de energia elétrica;

- Estudar o conceito de *Smart Grids* e *Self-Healing*;

- Destacar a importância de uma rede de comunicação confiável e robusta para o pleno funcionamento de um projeto SH;

- Estudar os conceitos de Redes de Computadores, abordando áreas como o Modelo OSI, protocolos de comunicação, segurança e gerenciamento, tais como o *Spanning Tree* e SNMP (*Simple Network Management Protocol*) aplicados diretamente à solução SH CEMAR;

- Realizar um estudo de caso sobre o projeto SH na CEMAR, explanando sobre o circuito de manobras do sistema elétrico atual, sistema SCADA Elipse, topologia da rede de comunicação, o processo de implantação do sistema SH, configuração e testes da rede de comunicação;

- Expor os problemas relacionados à segurança de informações críticas, expostas a riscos devido à vulnerabilidade dos equipamentos de comunicação instalados em ambientes abertos e remotos;

- Demonstrar a necessidade do gerenciamento da rede, discorrer sobre a configuração dos equipamentos, criação do módulo de gerenciamento da rede e geração de relatórios integrada ao sistema SCADA, além de demonstrar os resultados do processo.

[2] SCADA é a sigla em inglês para *supervisory control and data aquisition*, que traduzido literalmente para o português significa: “controle supervisório e aquisição de dados”.

1.4 Metodologia

Esta monografia começa com uma base teórica para o trabalho, contextualizando o cenário atual da distribuição de energia elétrica no país e demonstrando como este demanda soluções como o *Self-Healing*. Daí então, se inicia um breve estudo sobre a automação de um sistema de distribuição de energia elétrica, utilizando como referência a arquitetura de automação da CEMAR. Então, inicia-se uma explanação a respeito da solução *Self-Healing*, mostrando a necessidade de sua implantação e como este funciona.

Por ser uma parte fundamental para a automação e implantação de uma solução SH, este trabalho apresentará um estudo sobre redes de comunicação aplicadas à automação de sistemas de distribuição, demonstrando os principais conceitos e tecnologias utilizados atualmente na área.

Em seguida, o trabalho assume um caráter mais prático, realizando um estudo de caso da implantação do sistema *Self-Healing* na CEMAR, demonstrando a arquitetura utilizada, o módulo SH no SCADA Elipse Power e, mais detalhadamente, o processo de planejamento e escolha das tecnologias a serem aplicadas na rede de comunicação.

O estudo de caso também aborda a necessidade de um sistema de gerenciamento da rede de comunicação, demonstrando o processo de desenvolvimento deste, integrado ao sistema SCADA.

Por fim, este trabalho demonstra os resultados deste projeto, relatando uma atuação real do SH e a contribuição do projeto aos indicadores de qualidade de fornecimento de energia da empresa, além das conclusões e sugestões de trabalhos futuros.

2 *SMART GRIDS* E O SETOR ELÉTRICO BRASILEIRO

2.1 Introdução

Com o constante avanço do emprego de novas tecnologias no setor elétrico brasileiro, na última década começou-se a vislumbrar novas perspectivas para a área, fugindo do tradicional conceito que define a automação como a execução de tarefas com o apoio de computadores, minimizando a intervenção humana (SALES, 2014). Sobre esta luz abre-se espaço para o estudo das *Smart Grids*.

Smart Grids ou Redes Elétricas Inteligentes (REI) representam um novo conceito para o setor de transmissão e distribuição de energia, onde se empregam tecnologias digitais avançadas para monitorar e gerenciar o fornecimento de energia elétrica, se utilizando de um fluxo de informação bidirecional entre o sistema de fornecimento de energia e o cliente final (MOURA, 2011). Com este novo conceito, torna-se possível o desenvolvimento de novos serviços adjuntos à distribuição de energia, a melhoria da qualidade do fornecimento e a abertura de novos mercados.

2.2 Aplicações do conceito de *Smart Grids*

Sendo um conceito bastante abrangente, as *Smart Grids* também não têm um foco bem definido, sendo seu foco de aplicação variado em relação a cada país. Nos EUA, por exemplo, as REI tem como foco principal auxiliar na manutenção da rede de distribuição, que já começa a mostrar problemas por conta do envelhecimento, melhorar a qualidade do serviço, como também aumentar a interação com o usuário final. Já a Europa, as *Smart Grids* visam principalmente a questão ambiental, promovendo o uso de energias renováveis e diminuindo o uso de combustíveis fósseis.

No Brasil a aplicação das REI englobam um pouco dos cenários norte-americano e europeu, com destaque para:

- Redução de perdas técnicas e comerciais (fraudes);
- Reduzir custos operacionais;
- Melhorar a gestão de ativos;

- Melhorar a qualidade do serviço prestado pelas distribuidoras;

Dando destaque a este último ponto, visando atender à rígidas regulamentações impostas pela ANEEL, surgem aplicações de REI especializadas em reduzir as duração e frequência das faltas, visando a melhoria dos indicadores de continuidade.

2.3 Indicadores de Continuidade

A interrupção do fornecimento de energia elétrica é um grande causador de prejuízos e desconfortos para os clientes de uma empresa de distribuição. Por isso, surge a necessidade das empresas que mensurar de forma mais eficaz as porções do sistema de distribuição mais efetuadas com interrupções. Além disso, a ANEEL, órgão regulamentador do setor, também tem o interesse em indicadores que possam auxiliar na cobrança de uma qualidade mínima da prestação de serviço à sociedade, inclusive aplicando multas em casos de violações destes índices (ANEEL).

O PRODIST – Procedimento de Distribuição de Energia Elétrica no Sistema Elétrico Nacional – determina que os indicadores de duração e frequência de perdas de uma determinada porção de consumidores devem ser levantados em períodos mensais, trimestrais e anuais, a fim de manter um controle contínuo da qualidade. O DEC (Duração Equivalente de Interrupção por Unidade Consumidora) e o FEC (Frequência Equivalente de Interrupção por Unidade Consumidora) são calculados de acordos com as equações (1) e (2), respectivamente.

$$DEC = \frac{\sum_{i=1}^{k} Ca(i)Xt(i)}{Cc} \quad (1)$$

$$FEC = \frac{\sum_{i=1}^{k} Ca(i)}{Cc} \quad (2)$$

Onde:

DEC = duração equivalente de interrupção por unidade consumidora, expressa em horas e centésimos de hora;

FEC = frequência equivalente de interrupção por unidade consumidora, expressa em número de interrupções e centésimos do número de interrupções;

Ca(i) = número de unidades consumidoras, interrompidas em um evento (i), no período de apuração;

t(i) = duração de cada evento (i), no período de apuração;

i = índice de eventos ocorridos no sistema que provocam interrupções em uma ou mais unidades consumidoras;

k = número máximo de eventos no período considerado;

Cc = número total de unidades consumidoras faturadas, do conjunto considerado, no período de apuração.

2.4 Aplicações *Self-Healing*

Com este intuito, começa-se a desenvolver soluções do tipo *Self-Healing*: aplicações de REI, quem tem como objetivo básico se utilizar de equipamentos de manobras do Sistema Elétrico de Potência (SEP), em especial os localizados nas redes de distribuição, que possuem capacidade de comunicação e manobras remotas, afim de montar uma rede controlada por um sistema central que possa detectar uma falta num trecho e, o mais rápido possível, isolá-lo, reduzindo o número de clientes afetados e agilizando a manutenção.

Antes de aprofundar mais sobre funcionamento de um sistema SH, no próximo capitulo será feita uma explanação sobre o que é um sistema de distribuição de energia e sua automação.

3 AUTOMAÇÃO DE SISTEMAS DE DISTRIBUIÇÃO DE ENERGIA ELÉTRICA

3.1 Introdução

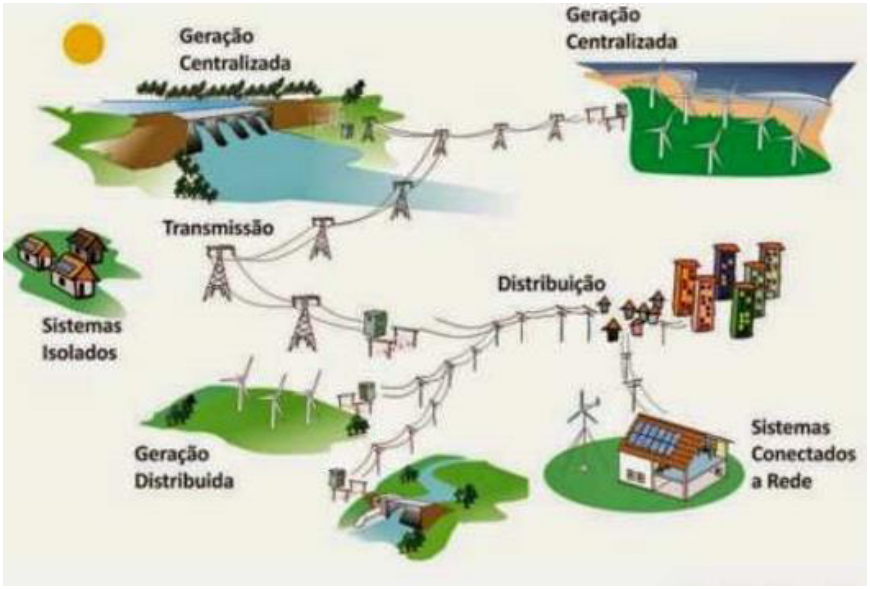
Neste capítulo será explanado o conceito de automação de sistemas de potência, em especial os sistemas de distribuição de energia elétrica, foco principal deste trabalho.

Para entender este conceito é necessário primeiramente compreender o que é um sistema de distribuição e os equipamentos que fazem parte deste, o que será feito no próximo item deste capítulo. Além disto, será demonstrada a arquitetura de automação de subestações e do sistema de distribuição CEMAR.

3.2 Sistemas de Distribuição

Um sistema de distribuição é definido como a parte final de um sistema elétrico de potência (SEP), onde a energia elétrica gerada chega à unidade consumidora, o cliente final, como podemos observar na figura abaixo:

Figura 1- Sistema elétrico de potência.



Fonte: SALES (2014).

Segundo (MOURA, 2011), podemos caracterizar um sistema de distribuição como um conjunto formado por:

- Sistema de subtransmissão: responsável por interligar subestações de transmissão de 230, 500 e 750kV e as subestações de distribuições, cuja tensão geralmente é de 69 ou 138kV.
- Subestação (SE): Utilizada como ponto de interligação, modificando e regulando níveis de tensão e cargas, seccionando linhas de subtransmissão e distribuindo energia para os circuitos alimentadores, utilizando equipamentos de controle e proteção como disjuntores e religadores.
- Alimentadores de distribuição primários: circuitos que conduzem energia aos consumidores de média tensão (13,8kV ou 34,5kV) ou aos transformadores de distribuição.
- Transformadores de distribuição: abaixam o nível da tensão para a faixa de baixa tensão (BT), geralmente 127 ou 220V.
- Alimentadores de distribuição secundários: circuitos que levam a energia em BT para os consumidores finais.

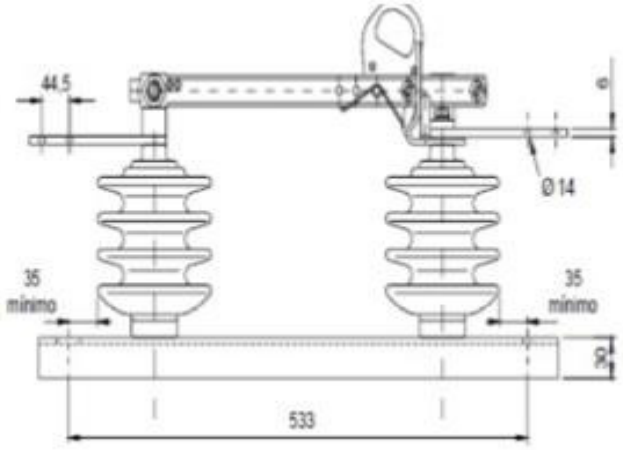
Alimentadores de distribuição podem ser considerados a porção mais complexa de um sistema de distribuição. Para atender a todos os clientes, estes circuitos se ramificam através de ramais alimentadores de distribuição, acompanhando as ruas e avenidas até cada unidade consumidora.

Posto isso, não é difícil imaginar que se este sistema fosse completamente contínuo, ou seja, sem pontos de proteção ou seccionamento, qualquer falha permanente ou temporária em algum ramal acarretaria na atuação do equipamento de proteção do alimentador primário da subestação, ocasionando a interrupção do fornecimento para todo o circuito, gerando severos impactos nos índices de DEC e FEC, visto que um alimentador de uma subestação de médio porte atende em média 10.000 clientes (ABRADEE, 2016).

Por esta razão, são implantados ao longo da rede de distribuição de energia elétrica equipamentos seccionadores, com capacidade de interromper ou permitir a passagem da corrente elétrica, de forma automática ou manual (por comandos locais ou remotos). Dentre estes equipamentos podemos citar (GOMES, 1982):

- Chave Seccionadora: equipamentos que formam um simples contato entre dois trechos da rede, podendo ser abertas (interrompendo a passagem da corrente) ou fechadas (permitindo a passagem da corrente). Tais chaves podem estar normalmente fechadas (NF), quando são utilizadas para seccionamento da rede em caso de falhas, ou normalmente abertas (NA), utilizadas para transferências de cargas entre alimentadores (Figura 2) [1]. Não podem ser abertas com carga, sendo responsabilidade de um religador ou disjuntor de retaguarda efetuar a interrupção de sobrecorrentes em caso de falta.

Figura 2 - Chave Seccionadora



- Chave Fusível: é um equipamento destinado à proteção de sobrecorrentes de circuitos primários (13,8kV no caso da CEMAR). É composta por um componente fusível (Figura 3) que, em caso de sobrecorrente, é aquecido até o seu rompimento, ocasionando a interrupção da corrente.

Figura 3 - Chave Fusível

- Disjuntor: Dispositivo mecânico de manobra semelhante às chaves seccionadoras, porém com a capacidade de conduzir ou interromper correntes de cargas (Figura 4).

Figura 4 - Disjuntor

- Religador: Dispositivo semelhante ao disjuntor, mas com a capacidade de realizar uma sequência de operações de aberturas e fechamentos,

a fim de verificar se a falta foi momentânea (Figura 3.6). Caso o número de repetições termine sem a normalização da falta, o ciclo de religamento é encerrado e a corrente interrompida (Figura 5).

Figura 5 - Religador de Poste

- Relé: Equipamentos responsáveis pelo gerenciamento do circuito elétrico (Figura 6). Normalmente conectado a um disjuntor ou religador, o relé, através da leitura dos valores de tensão e corrente, detecta a ocorrência de um problema. Daí este pode comandar automaticamente a atuação do equipamento de disjunção e/ou sinalizar a existência de uma anormalidade para o controlador do sistema.

Figura 6 - Relé

3.3 Automação de Sistemas elétricos

A automação em um sistema elétrico consiste basicamente na integração de equipamentos de controle, medição e sensoriamento à equipamentos de comunicação e computação que possibilitem a supervisão e o controle de um sistema de transmissão ou distribuição com o intuito de aperfeiçoar a operação, reduzindo o tempo na detecção e resolução de falhas na rede elétrica e reduzindo custos (JARDINI,1996).

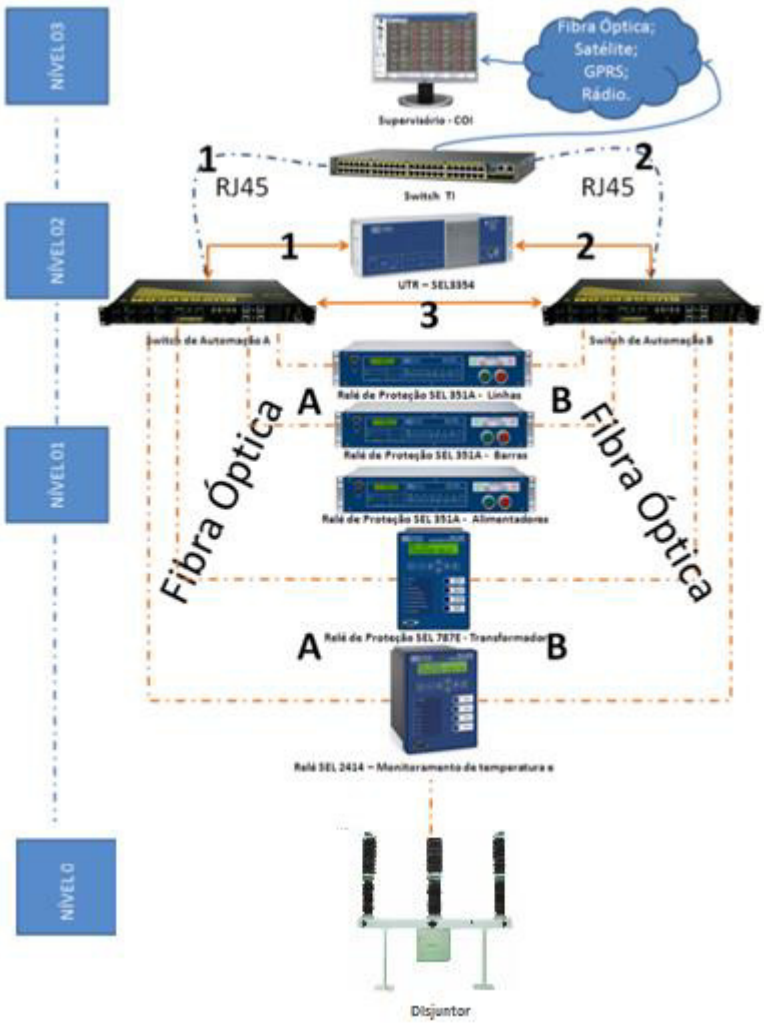
Os sistemas SCADA (*Superisory Control and Data Aquisition*) podem ser definidos como uma arquitetura formada desde os equipamentos ligados diretamente à rede elétrica (como relés de transformadores, barras e alimentadores e medidores de carga), passando por equipamentos de comunicação como switches de comunicação e UTR's (Unidades Terminais Remotas), até chegar às IHM (Interface Homem-Máquina), softwares que condensam e tratam todo o montante de dados recebidos e oferecem ao controlador informações sobre o estado atual do sistema elétrico e a capacidade de executar comandos remotamente.

Este modelo de automação passou a ser aplicado nas subestações da CEMAR em 2012, em substituição à antiga arquitetura que utilizava comunicação GPRS (*General Packet Radio Service*), e que passou a utilizar comunicação via satélite ou fibra ótica (SALES, 2014). Este modelo será explicado de forma mais aprofundada no próximo capítulo.

3.3.1 Automação de Subestações da CEMAR

Sales (2014), subdivide a estrutura de automação da CEMAR em 4 níveis, representados graficamente pela Figura 7.

Figura 7 - Arquitetura de automação de subestações da CEMAR



Especificamente:

- Nível 0: Equipamentos de campo como disjuntores, religadores, transformadores de corrente e tensão.
- Nível 1: IED's (Intelligent Eletronic Devices), mais comumente chamados de relés ou *relays*, que são conectados aos equipamentos de campo a fim de coletar dados ou efetuar comandos.
- Nível 2: UTR's, Switches, concentradores óticos, modems.
- Nível 3: Formado por concentradoras de dados e os servidores da IHM SCADA, no caso da CEMAR o software ELIPSE POWER, que será descrito mais à frente.

A figura acima mostra o cuidado que se tem com a confiabilidade da rede, implantando nos níveis 0 e 1 redundâncias de comunicação. No nível 0 cada IED se comunica os dois switches de automação e no nível 1 a UTR se comunica também com ambos os switches. Tal configuração possibilita que a rede funcione mesmo em caso de falhas como rompimento de fibra ou falha das portas de IED's ou switches.

A automação de sistemas de distribuição segue a mesma ideia descrita para as subestações, porém com algumas mudanças no que diz respeito aos equipamentos, visto o ambiente diferenciado das linhas de distribuição.

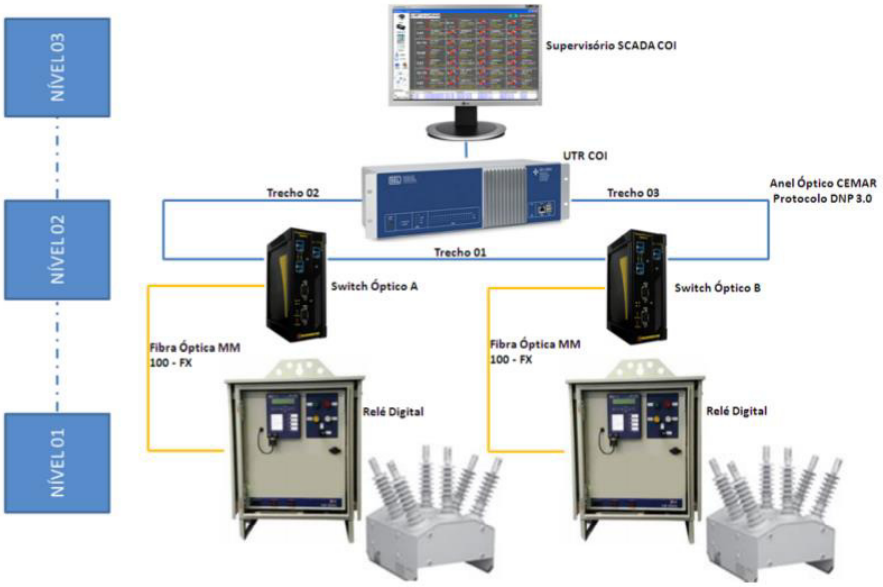
3.3.2 Automação de Sistemas de Distribuição

Semelhante ao que acontece na automação de subestações, nos sistemas de distribuição equipamentos de campo controlados por IED's se comunicam com equipamentos de comunicação como switches e UTR's a fim de que a IHM possa oferecer ao controlador total ciência do estado da rede de distribuição e possibilitar intervenções remotas.

Entretanto, os equipamentos de um sistema de distribuição não estão concentrados em um só espaço geográfico controlado como o de uma subestação. Religadores, chaves e transformadores estão espalhados por ruas e avenidas ao longo de quilômetros, acompanhando a configuração da rede e expostos à diversos riscos, desde de abalroamentos de postes a até tentativas de invasões da rede de comunicação por indivíduos mal-intencionados.

No caso da CEMAR, (SALES, 2014) classifica a automação da distribuição de energia em 3 níveis, como mostrado na Figura 8:

Figura 8 - Arquitetura da automação de sistemas de distribuição da CEMAR



Na figura acima podemos notar que, diferentemente do que ocorre em subestações, onde cada IED se comunica com dois switches para garantir a redundância da comunicação, no cenário dos sistemas de distribuição, a redundância se baseia numa arquitetura em anel, que possibilita que cada switch tenha dois caminhos diferentes para trafegar os dados. Mais detalhes sobre este tipo de arquitetura de comunicação serão apresentados nos próximos capítulos.

3.3.3 Sistemas SCADA

Os sistemas SCADA (*Supervisory Control and Data Acquisition*) ou, em uma tradução literal, sistemas de supervisão e aquisição de dados constituem uma parte fundamental e complexa da arquitetura de sistemas de potência. Sistemas SCADA podem ser definidos como sistemas que, a partir de dados provenientes de campo (no caso desde trabalho, IED's em subestações ou na rede de distribuição), podem fornecer informações valiosas, através de interfaces gráficas, que facilitam a prevenção, detecção e resoluções de falhas (PENIN, 2012).

Além do aspecto supervisório, ou seja, a capacidade de, a partir de dados "crus" de equipamentos de campo, construir informações sobre o estado do sistema supervisionado para o controlador, os sistemas SCADA podem fornecer o controle

destes equipamentos, possibilitando comandos remotos que diminuem drasticamente o tempo necessário para realizar uma atividade.

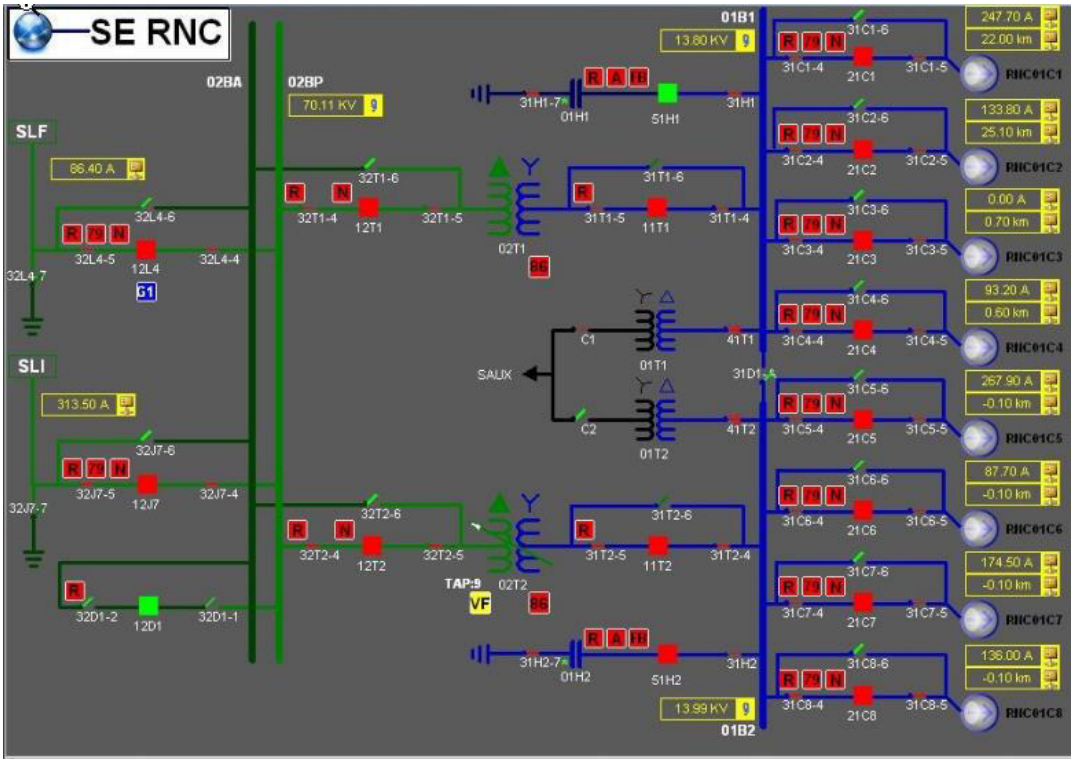
Em sistemas de potência, como subestações e sistemas de distribuição, cada segundo se torna valioso para quem os opera, seja por conta dos prejuízos que podem ser causados aos consumidores com as faltas de energia, como queima de aparelhos, à empresa, com o impacto nos indicadores de qualidade ou avaria de ativos, ou seja por conta do risco que estes sistemas podem representar no caso de uma falha ou acidente, como um cabo ao solo. Por esta razão, a aplicação de sistemas SCADA nesta área se torna imprescindível para diminuir os impactos causados por estas ou outras situações possíveis.

Num exemplo prático, imagina-se o seguinte cenário: em um dia de forte chuva, um carro derrapa na pista e abalroa um poste, ocasionando o rompimento de uma linha de 13kV que, por algum motivo, não foi desligada pela proteção automática. O cabo elétrico se encontra ao solo, efetuando descargas que representam um sério perigo às pessoas próximas, devendo a linha ser desligada o quanto antes. O tempo que um controlador de um COI (Centro de Operações Integradas), detectando a anomalia na linha por um alarme sinalizado pelo SCADA, levaria para enviar um comando remoto ao relé do disjuntor da linha seria muito menor do que o que ele levaria para contatar o operador em campo e solicitar a abertura manual do equipamento. Tal exemplo demonstra a fundamental importância desse tipo de sistema no setor e o porquê desta tecnologia ser amplamente utilizada.

3.3.3.1 Sistema SCADA Elipse Power

Na CEMAR, o sistema SCADA utilizado é o Elipse Power da empresa Elipse Software. O Elipse Power oferece um ambiente que integra comunicação, modelagem e análise, possibilitando o desenvolvimento de uma ferramenta de supervisão para subestações e redes de distribuição (Figura 9).

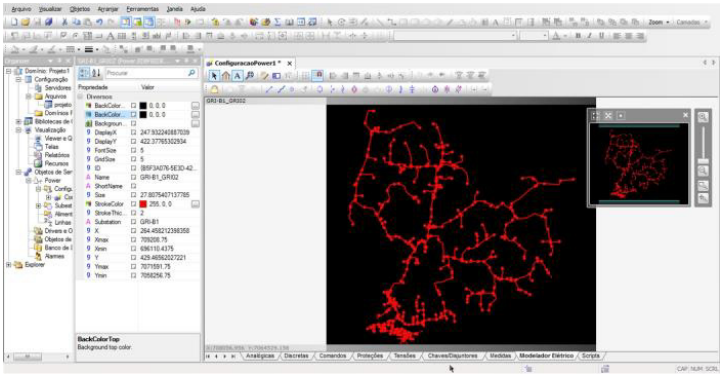
Figura 9 - Tela de supervisão e controle de uma subestação no Elipse Power



Fonte: (ELIPSE, 2016)

Utilizando bibliotecas gráficas inclusas no software, drivers de comunicação com suporte aos protocolos mais utilizados na área como o DNP3, IEC 103, 104 e 61850, suporte a scripts e um modelador de rede elétrica, o Elipse Power permite fácil acesso a todas as informações necessárias para o processo de operação de redes de energia, maximizando a relação custo-benefício, bem como a confiabilidade do sistema (ELIPSE, 2016).

Figura 10 - Elipse Studio: Ambiente de desenvolvimento do Elipse Power



Fonte: (ELIPSE, 2016)

No ambiente de desenvolvimento do Elipse Power o desenvolvedor, além de configurar os drivers de comunicação para obter os dados diretamente dos IED's em campo ou de uma UTR, também pode modelar a rede elétrica, que integra subestações e sistemas de distribuição através do modelador elétrico, mostrado na Figura 10. Estes modelos podem ser apresentados na IHM para o controlador através de objetos gráficos, inclusos na biblioteca padrão ou criados pelo desenvolvedor. O Elipse Power pode ainda registrar eventos e alarmes em banco de dados, gerar relatórios e armazenar históricos de medidas pré-determinadas.

Na CEMAR, o Elipse Power atua com dois servidores:

- Comunicação: Exclusivo para conexão à IED's e UTR's para obtenção de dados e envio de comandos através do protocolo DNP3, que será detalhado mais à frente.
- Aplicação: Aplica os dados provenientes dos servidores de comunicação, relacionando-os com os elementos de tela e apresentando-os através dos objetos gráficos. Armazena rotinas de execução na linguagem de programação *VBScript*, se conecta à banco de dados e até envia informações por e-mail.

Esta arquitetura, como o apoio de um servidor de *backup* para cada um dos servidores principais, possibilita uma divisão de cargas na utilização de cada máquina, o que melhora a performance do sistema, além de diminuir o risco de uma indisponibilidade total deste.

No estudo de caso deste projeto, será mostrada a importância do Elipse Power e sua escalabilidade e capacidade de personalização para o desenvolvimento do módulo de gerenciamento da rede de comunicação do SH integrado ao supervisório do sistema de potência.

4 SELF-HEALING

4.1 Introdução

Em um mercado fortemente regulamentado e competitivo, o desenvolvimento de novas soluções para a automação de sistemas de distribuição vem sendo a principal alternativa das concessionárias de energia para reduzir os custos operacionais e diminuir o tempo de descontinuidade do fornecimento de energia (FALCÃO, 2010).

Com a redução dos preços dos equipamentos necessários para a automação de redes de distribuição pelo crescente número de fabricantes e com o constante surgimento de novas tecnologias, se torna cada vez mais viável investir em soluções mais complexas nesta área, que possam gerar em curto ou médio prazo a melhoria dos indicadores de qualidade do fornecimento, e por consequência, redução de custos.

Intervenções e contingências não programadas na rede de distribuição se tornam problemas constantes pelo fato desta rede estar exposta, ao longo da zona de distribuição, a diversos riscos como condições climáticas, abalroamento de postes ou contato com galhos de árvores (AZEVEDO, 2010). Tais problemas, além dos impactos gerados à concessionária como multas junto ao órgão regulamentador e perdas de faturamento, também geram transtornos à sociedade, como avarias de aparelhos, problemas em hospitais, sinais de trânsito e perda de produção em indústrias.

Isto posto, é notável a necessidade de um sistema de distribuição de energia elétrica moderno, que possa atender aos níveis de confiabilidade, eficiência e segurança exigidos pelo mercado atual. Para isto, torna-se necessário um sistema que combine a aquisição e análise de dados provenientes da rede de distribuição para proporcionar a assistência necessária na automação e controle destas redes.

Sendo assim, surgem as Redes Elétricas Inteligentes (REI). O conceito de rede inteligente é a capacidade de tornar o sistema eficiente e seguro. Quando aplicamos este conceito ao sistema de distribuição, utilizando tecnologias de monitoramento,

processamento de dados e rede de comunicação, pode-se otimizar a sua operação, tem-se a oportunidade de tornar o sistema capaz de monitorar, avaliar e autorregenerar quando da ocorrência de distúrbios no sistema. Pode-se dizer que a automação de uma rede de distribuição de energia elétrica, em forma completa, é capaz de tomar as decisões operativas com o uso de lógica de automação e ferramentas de software de maneira automática em tempo real (FERREIRA, 2010).

Dentro deste conceito de *Smart Grids*, destaca-se a funionalidade de autorregenerar ou *self-healing*, definido por FALCÃO (2010) como sendo a capacidade de um sistema de distribuição de detectar, analisar, responder e restaurar falhas na rede elétrica de forma automática.

OHARA (2009) define o conceito *Self-Healing* como a capacidade que uma rede de distribuição tem de isolar o problema, reduzir ao mínimo possível o número de clientes afetados e restabelecer ao estado normal o mais rápido possível e com a menor intervenção humana possível, de maneira que a Inteligência do sistema defina e execute as decisões, minimizando o deslocamento de equipes

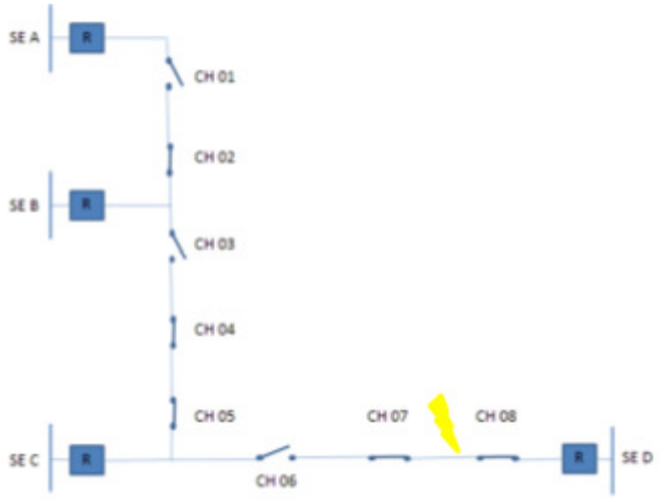
4.2 Recomposição automática de um Sistema de Distribuição

No âmbito dos sistemas de distribuição de energia elétrica, a recomposição do fornecimento em caso de falhas pode ser feita através da reconfiguração da rede através da manobra de equipamentos presentes na rede. Estas manobras podem acontecer através da operação manual de chaves entre alimentadores, operação remota de chaves telecomandadas ou religadores através de um sistema SCADA ou através de um sistema inteligente que possa calcular efetuar os comandos de forma automática (*Self-Healing*) (SALES, 2014).

Os índices DEC (duração da falta) e FEC (frequência da falta) apresentados no segundo capítulo deste trabalho, e que são os principais fatores determinantes das multas pagas por uma concessionária, são afetados por faltas com tempo superior a 3 minutos. Por isto, a velocidade com que uma falta é identificada e o fornecimento é

recomposto ao maior número de cliente possível é de profundo impacto nas metas de uma empresa de distribuição.

Figura 11 - Exemplo hipotético de recomposição de um sistema de distribuição



Fonte: SALES (2014)

No exemplo da Figura 11, tempo um sistema de distribuição hipotético onde ocorre uma falta permanente entre as chaves (CH) 07 e 08, ocasionando a abertura do religador (R) da subestação (SE) D. Este problema acarretaria a interrupção do fornecimento de energia a todos os clientes atendidos por este alimentador, compreendidos pelo trecho entre o religador da subestação D e a CH 06.

A alternativa mais simples e eficaz de recomposição neste cenário se dá por 3 operações:

- Abertura das chaves 07 e 08, isolando o trecho com problema;
- Fechamento da CH 06, recompondo o fornecimento de energia aos clientes que estão entre esta chave a chave 07;
- Fechamento do religador da SE D, recompondo o fornecimento de energia aos clientes entre este religador e a CH 08.

A realização destas operações poderá acontecer nos seguintes cenários:

- CH 06, 07 e 08 são manuais: uma equipe de técnicos terá que ser acionada para efetuar as operações *in loco*;
- CH 06, 07 e 08 são telecomandas: o controlador no COI (Centro de Operações Integradas) identifica a falta e a alternativa de recomposição e efetua os comandos através do SCADA.
- As chaves fazem parte de um sistema inteligente capaz de detectar a falta, calcular a alternativa e realizar as manobras de forma automática (*Self-Healing*).

Não é difícil notar que cada um dos cenários acima descritos irá demandar tempos distintos de operação e, por conseguinte, gerar diferentes impactos aos indicadores da empresa.

No primeiro cenário, entre o tempo de identificação da falha pelo controlador, envio da equipe aos locais das chaves e realização das manobras, pode-se levar de 50 a 80 min (STASZESKY, 2005).

Na segunda opção, com as chaves telecomandas, o operador ainda levaria algum tempo para identificar a falhar, avaliar se o alimentador da subestação C suportaria a carga proveniente da manobra e enviar os comandos, o que poderia facilmente ultrapassar o tempo mínimo para que esta falta seja contabilizada pelo DEC e FEC, que é de três minutos.

No último cenário, um sistema inteligente conectado aos equipamentos da rede elétrica rapidamente iria identificar o problema, efetuar os cálculos necessários e efetuar os comandos, tornando muito difícil o tempo da manobra exceder um minuto, o que não geraria impacto nos índices de continuidade (STASZESKY, 2005).

4.3 Arquitetura de um sistema *Self-Healing*

Para operar, um sistema SH necessita basicamente de um sistema central inteligente conectado à uma rede de distribuição automatizada. O sistema inteligente, podendo ser centralizado em um único ponto (como o próprio SCADA)

ou um sistema distribuído, deve ter a capacidade de, a partir de grandezas provenientes dos equipamentos de campo, como religadores das subestações e religadores na rede de distribuição, detectar a ocorrência de uma falta, o trecho com problema e, caso haja, alguma alternativa possível de manobras, de acordo com os equipamentos seccionadores disponíveis.

Os equipamentos em campo, como chaves telecomandadas ou religadores, devem estar conectados à IED's que permitirão a coleta e envio de grandezas e eventos ao sistema inteligente, além da realização de comandos remotos. É importante ressaltar que tais IED's devem estar operantes mesmo na ausência do fornecimento de energia proveniente da rede, já que esta, em caso de falta, estará desligada. Para isto, é comum a utilização de baterias junto a cada IED a fim de mantê-lo em operação.

5 REDES DE COMUNICAÇÃO

5.1 Introdução

A eficiência da automação de sistemas de distribuição, e em especial as aplicações *Self-Healing*, depende basicamente da capacidade de adquirir dados e transmitir comandos aos equipamentos de controle de forma confiável.

São as redes de comunicação que possibilitam a conexão entre o sistema de controle central da automação e as IED's espalhadas pela rede de distribuição, permitindo o tráfego de dados bidirecional, onde os equipamentos enviam dados ao controle central e este, após realizar as devidas análises, pode enviar comandos aos equipamentos desejados.

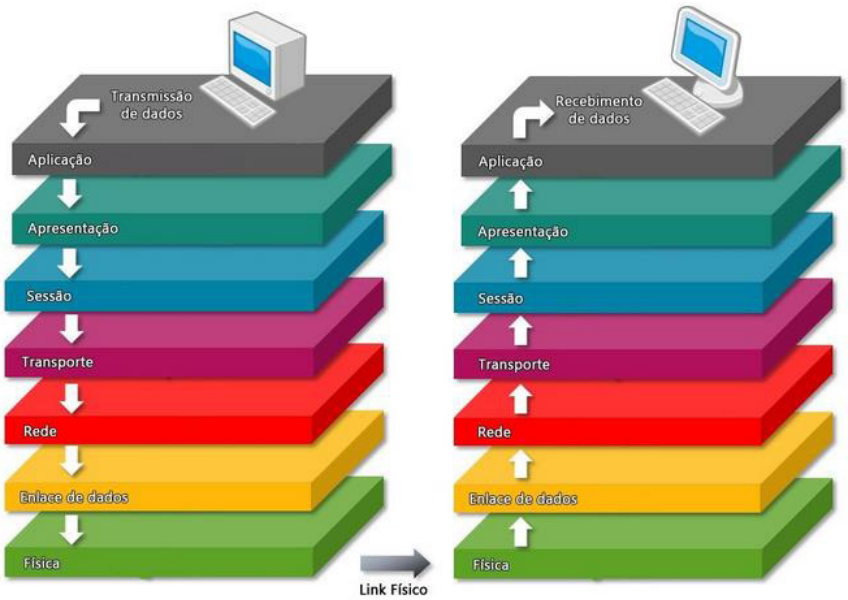
Neste capítulo será feita uma breve análise sobre o conceito de redes de comunicação, modelos, protocolos e tecnologias necessários para o desenvolvimento deste trabalho.

5.2 Modelo OSI

No início do desenvolvimento de grandes redes de comunicação, notou-se alguns problemas com a conexão de diferentes sistemas. Para solucionar isto, a ISO (*International Standards Organization*) iniciou um processo de padronização dos protocolos utilizadas nas camadas de uma rede, criando então o modelo OSI (*Open Systems Interconnection*) ou conexão de sistemas abertos, pois trata da interconexão de sistemas abertos a comunicação com outros sistemas (TANEMBAUM, 1996).

O modelo OSI divide a estrutura de uma rede de comunicação em sete camadas ou *layers* (Figura 12). Cada camada tem uma função própria, aplicando protocolos e fornecendo serviços às camadas superiores. São as camadas do modelo OSI, da de mais baixo nível para a de mais alto nível: física, enlace, rede, transporte, sessão, apresentação e aplicação.

Figura 12 - Ilustração das camadas do modelo OSI



5.2.1 Camada física

Trata-se do meio de transmissão bruto de bits por um canal de comunicação. Nesta camada concentram-se os cuidados em fazer com que um bit enviado de um dispositivo chegue da mesma forma ao dispositivo de destino. Protocolos desta camada devem estabelecer a forma que um bit é representado, seja por meio de sinais elétricos, óticos ou meios sem fio, questões de sincronização e estabelecimento e término de conexão.

Dentro desta camada podemos incluir as tecnologias de transmissão com fio, como cabos coaxiais, cabos de par trançado e fibra óptica, e as sem fio, como ondas de rádio, telefonia móvel e WiFi.

5.2.2 Camada de enlace

A camada de enlace ou *layer* 2 do modelo OSI é responsável por transformar um simples canal de transmissão de dados (enlace), como os implementados na camada física, em uma linha que pareça livre de erros e possa entregar dados confiáveis à camada mais acima (TANEMBAUM, 1996).

Kurose et al. (2000) define os principais serviços oferecidos pela camada de enlace em:

- Enquadramento de dados: Encapsula os datagramas provenientes da camada superior em quadros ou *frames*. Um frame é composto por um cabeçalho que contém os detalhes do *frame* e o campo de dados onde de fato é enviado o datagrama. A estrutura de um *frame* é determinada de acordo com o protocolo utilizado, sendo o protocolo Ethernet o mais conhecido e utilizado.
- Acesso ao enlace: Um protocolo de controle de acesso ao meio (*medium access control protocol* – MAC) controla a forma que um *frame* é enviado por meio de um enlace de um nó ao outro. Em enlaces ponto-a-ponto, onde somente um nó envia e só um nó recebe os dados, o protocolo MAC é bem simples ou, em certos, casos nem é utilizado. Porém, em enlaces de difusão ou *broadcast*, onde o mesmo enlace é compartilhado por vários nós, o protocolo MAC tem a função de coordenar as transmissões.
- Entrega confiável: Alguns protocolos da camada de enlace podem fornecer o serviço de entrega confiável de dados, isto é, garantir às camadas superiores que um datagrama será entregue sem erros ao outro nó. Geralmente este tipo de serviço é implementado na camada de enlace somente quando utilizamos meios de transmissão com muitos erros, como os meios sem fio. Em meios mais confiáveis como os cabos elétricos e fibras ópticas, a verificação de erros acaba gerando uma sobrecarga desnecessária, sendo esta tarefa delegada às camadas superiores, como a de transporte.
- Controle de fluxo: Devido à capacidade limitada dos nós de armazenar e processar os *frames*, um nó emissor pode congestionar um nó receptor, ocasionando a perda de quadros. Para evitar este problema, protocolos da camada de enlace controlam o fluxo de *frames* entre nós.
- Detecção de erros: Como ruídos e interferências nos meios de transmissão pode inverter alguns bits enviados, protocolos da *layer* 2 pode detectar esses erros através do envio de bits de detecção de erros dentro dos quadros. Este tipo de serviço também pode ser encontrado em protocolos da camada de transporte e de rede, entretanto os da camada de enlace são mais sofisticados e implementados em *hardware*.

- Correção de erros: Protocolos deste tipo permitem a camada de enlace não somente detectar erros, como também localizar em que parte do *frame* o erro está e corrigi-lo.
- *Half-duplex* e *full-duplex*: A camada de enlace pode permitir que os nós das extremidades do enlace possam transmitir quadros simultaneamente, quando isto ocorre denominamos as transmissão *full-duplex*. Quando somente um nó pode enviar quadro de cada vez a transmissão é chamada de *half-duplex*.

Protocolos da camada de enlace geralmente são implementados em nível de *hardware*, em *switches* ou comutadores, e compõem parte fundamental de quase toda arquitetura de comunicação moderna. Switches que operam nesta camada utilizam os dados provenientes do cabeçalho do frame para determinar o enlace de destino do quadro.

5.2.3 Camada de rede

A camada de rede ou *layer* 3 do modelo OSI tem como princípio básico garantir de um pacote de dados de um *host* a outro na rede (TANEMBAUM, 1996). Para isto, duas funções básicas da camada de rede são (KUROSE, 2000):

- Repasse: Operação de direcionar para o enlace de saída apropriado um pacote que chega em um enlace de entrada, a fim que este pacote consiga alcançar seu destino. Geralmente protocolos de repasse utilizam uma tabela armazenada no dispositivo para, a partir de um endereço de camada de rede (como o endereço IP que será mostrado mais à frente) contido no datagrama, diga a qual enlace este deve ser enviado.
- Roteamento: Consiste num processo mais abrangente da rede, que determina qual o percurso que um pacote de dados deve percorrer para sair do seu remetente e chegar ao seu destinatário. Os algoritmos que calcula essas rotas são chamados de algoritmos de roteamento. Estes algoritmos podem ser centralizados, onde o algoritmo roda em um local central e descarrega as informações de roteamento em cada roteador, ou descentralizados, onde

cada roteador calcula o trecho de roteamento que é responsável e atualiza sua tabela de repasse.

5.2.4 Camada de transporte

Esta camada, considerada a *layer 4* do modelo OSI, tem como objetivo fornecer uma comunicação lógica entre processos, isto é, tornar transparente todo o processo de conexão, fazendo parecer que estão conectados diretamente um ao outro (KUROSE, 2000).

A camada de transporte fornece um canal de comunicação de um *host* para outro *host* (ponto a ponto) ou a difusão para diversos *host*, podendo este canal ser confiável, quando ocorre quando uma baixíssima taxa de erros e com uma garantia da ordem de entrega, ou não confiável, quando os pacotes de dados são transmitidos sem estas preocupações. Mais à frente veremos exemplos de protocolos que proporcionam estes tipos de conexão, no modelo TCP/IP.

5.2.5 Camada de sessão

Tanembaum (1996) define a camada de sessão como a responsável por permitir o estabelecimento de sessões de comunicação entre dispositivos. Uma sessão pode oferecer serviços como:

- Controle de diálogo: Determinar quem deve transmitir em cada momento;
- Gerenciamento de símbolos: Impedir que duas partes tentem executar a mesma operação crítica ao mesmo tempo;
- Sincronização: Verificação periódicas de transmissões longas, a fim de, em caso de falha, retoma-las de onde pararam.

5.2.6 Camada de apresentação

Esta camada, ao contrário das mais baixas, não se preocupada com a movimentação de bits, mas sim com a apresentação da sintaxe e semântica dos dados. A partir dos protocolos desta camada, torna-se possível a comunicação entre computadores com diferentes representações de dados. Para isso, a camada de

apresentação transforma os dados a serem enviados em uma representação abstrata, enviando também a informação de qual é a codificação que será utilizada durante a conexão.

5.2.7 Camada de aplicação

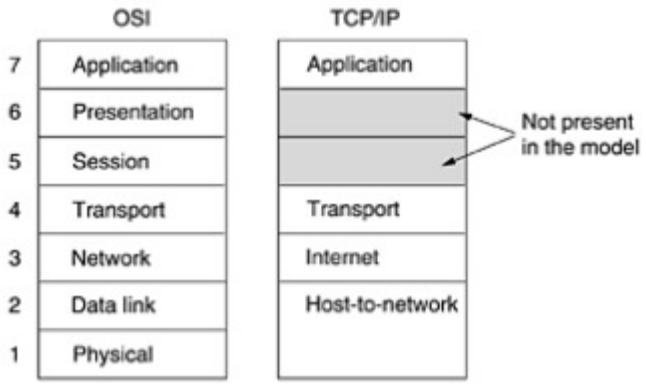
Camada de mais alto nível do modelo OSI, provendo serviços diretamente às aplicações e usuários. Tem como objetivo tornar totalmente transparente todo o processo de comunicação estabelecido pelas camadas inferiores. Protocolos desta camada proveem serviços como a requisição de páginas web (HTTP), transferências de arquivos (FTP), troca de e-mails (SMTP), dentre outros (TANEMBAUM, 1996).

5.3 Modelo TCP/IP

Baseado no modelo OSI, o modelo TCP/IP foi desenvolvido pelo Departamento de Defesa dos Estados Unidos (DoD) com o intuito de desenvolver uma arquitetura que pudesse conectar várias redes de maneira uniforme, além de possibilitar a "sobrevivência" da rede mesmo com a perda de algumas máquinas ou linhas intermediárias (TANEMBAUM, 1996). O nome TCP/IP vem dos seus dois principais protocolos.

Definido pela primeira vez por (CERF e KAHN, 1974), este modelo possui apenas 4 camadas, análogas às camadas do modelo OSI, como mostra a Figura 13. A Internet, como a conhecemos hoje, só foi possível com o desenvolvimento deste modelo, surgindo a partir da sua antecessora, a ARPANET (*Advanced Research Projects Agency Network*), uma rede criada para ligar os principais supercomputadores das universidades dos EUA.

Figura 13 - Camadas do Modelo TCP/IP



Fonte: (TANEMBAUM, 1996)

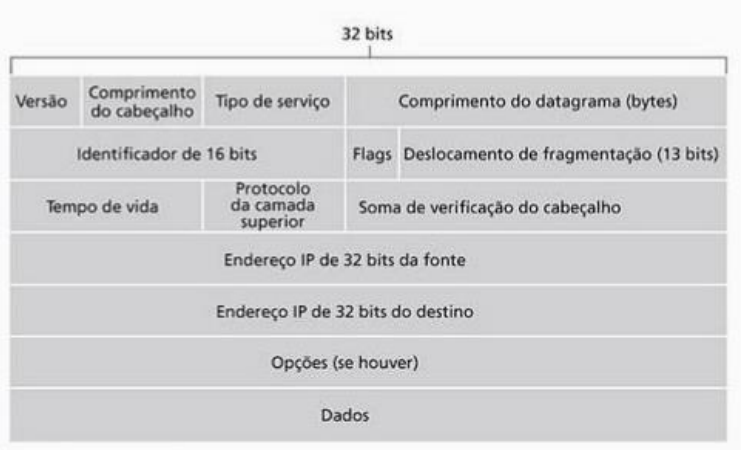
5.3.1 Camada de internet

Camada principal deste modelo, a camada de internet tem como objetivo possibilitar que um *host* injete pacotes de dados em uma rede e estes sejam transmitidos de forma independente até o seu destino. Para isto, esta camada define um formato de pacote oficial e um protocolo chamado IP (*Internet Protocol*).

5.3.1.1 Protocolo IP

Principal protocolo da camada de internet e do próprio modelo TCP/IP, o protocolo IP fornece um serviço de datagramas para a troca de pacotes de dados entre *hosts*. Os datagramas IP tem como característica ter um cabeçalho e o campo de dados, como mostra a Figura 14.

Figura 14 - Ilustração de um datagrama IPv4.



Fonte: (KUROSE, 2000)

O protocolo IP possui duas versões principais em uso atualmente: IPv4 e IPv6, sendo a primeira a dominante na maioria das redes. A principal diferença entre elas é o campo de endereçamento com 96 bits a mais na versão 6. Este trabalho se limitará a falar apenas da versão 4.

Dentre os elementos contidos no datagrama IP descritos por (KUROSE, 2000), podemos destacar:

- Versão: Especifica a versão do protocolo IP, geralmente 4 ou 6;
- Tipo de serviço: Bits que servem para diferenciar os tipos de datagramas IP. Por exemplo, alguns datagramas podem ser destinados à aplicação em tempo real como comunicação por voz ou aplicação que não são em tempo real mas necessitam de um alto grau de confiabilidade, como aplicações FTP.
- TTL (*Time-to-live* ou tempo de vida): Número máximo de saltos que o datagrama pode dar para chegar ao seu destino. Valor utilizado para evitar que um datagrama trafegue para sempre na rede, em caso de cair em um *loop*. A cada salto o TTL é decrescido, se chegar a 0, o datagrama é descartado.
- Protocolo: Define para qual protocolo o datagrama irá quando chegar ao seu destino, por exemplo, TCP ou UDP, protocolos que serão abordados mais à frente neste trabalho.

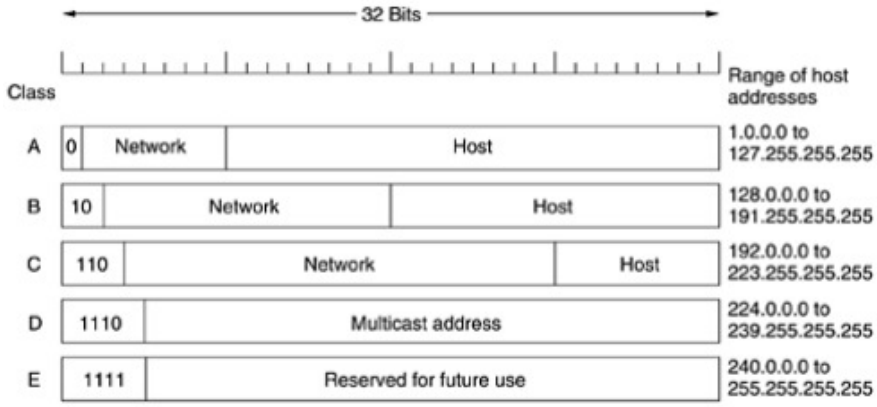
- Endereços IP de fonte e destino: Quando um *host* cria um datagrama, ele insere o seu endereço IP e o endereço IP do destino. O endereço IP é um identificador de 32 bits atribuído a cada nó da rede. O capítulo 5.3.1.2 falará um pouco mais a fundo sobre este endereçamento.
- Dados: Os segmentos de dados a serem transmitidos.

5.3.1.2 Endereçamento IP

O Endereço IP é um segmento de 32 bits incluso em qualquer datagrama IP que tem como finalidade identificar uma interface entre um *host* ou roteador com o enlace físico. Um exemplo de endereço IP em notação decimal separada por pontos é: 193.32.216.9, que em binário resultaria em: 11000001 00100000 11011000 00001001. Na notação decimal separada por pontos, cada byte (conjunto de 8 bits), é separado representado em sua forma decimal e separado dos demais bytes por pontos.

De acordo com seu formato, os endereços IP foram, por muitas décadas, divididos em classes, como mostra a Figura 15:

Figura 15 - Classes de endereços IPv4.



Fonte: (TANEMBAUM, 1996)

Os endereços das classes A, B e C podem fornecer 128 redes com 16 milhões de *hosts* cada, 16.384 redes com mais de 64.000 *hosts* e 2 milhões de redes com 256 *hosts*, respectivamente. Os endereços de classes D são destinados à multidifusão, quando um datagrama é destinado a mais de um *host* (TANEMBAUM, 1996).

Alguns endereços IP são destinados a funções específicas, são os chamados endereços especiais. O endereço 0.0.0.0 é utilizado quando o host está sendo inicializado. Endereços que tem 0 como o número de rede se referem a *hosts* na rede local. O endereço 255.255.255.255.255 permite a difusão de pacotes para a rede local, enquanto endereços que espeficificam a rede mas tem todos os bits de *host* com o valor 1 permitem a difusão em redes distantes. Endereços com o formato 127.xxx.xxx.xxx são chamados de endereços para *loopback*, onde os pacotes são enviados para o próprio host e tratados como pacotes de entrada.

5.3.1.3 Sub-redes

Como foi visto no capítulo anterior, o endereçamento IP possibilita a criação de um elavado número de redes com um determinado número de *hosts* em cada. Entretanto, com a impantação de redes IP em universidades e empresas, por exemplo, notou-se a dificuldade de se distribuir uma única rede para um grande número de *hosts* distantes fisicamente.

Tanembaum(1996) cita o exemplo fictício de uma universidade que detentora de uma rede Classe B (capacidade de mais de 64 mil *hosts*). Conforme mais depertamentos desta universidades desejavam entrar na rede, mais repetidores precisivam ser instalados, até chegar ao limite máximo recomendado de 4 repetidores por segmento para redes Ethernet. Pedir outro endereço de rede classe B seria um desperdício, visto que o limite de mais de 64 mil *hosts* não estaria nem perto de ser atingido.

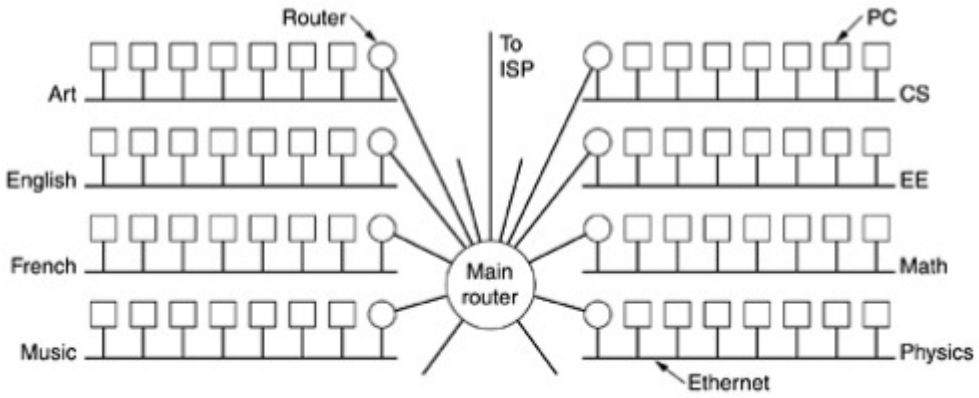
Para resolver problemas como este, contruiu-se o conceito de sub-redes onde seria possível dividir uma rede maior em outras menores e utilizar roteadores para interliga-las. Assim, ao receber um pacote de dados externo, o roteador principal da rede se preocuparia de saber apenas a qual roteador de sub-rede deveria entraga-lo, e este sim o levaria até o *host*.

Uma notação que auxilia na definição do limite de *hosts* de uma rede ou sub-redes são as máscaras de rede. Uma máscara é um conjunto de 32 bits, semelhante ao endereço IP, onde os bits com valor um (localizados à esquerda) representam os bits do endereço IP destinados à definir qua é a rede e os com valor zero defines os bits destinados aos endereços de *hosts*. Por exemplo, uma rede classe C teria uma máscara 11111111.11111111.11111111.00000000 (ou 255.555.255.0), que define que a rede tem apenas 8 bits para endereço de *hosts*, resultando na capacidade de 254 *hosts*, excluindo o 0 que indentifica a própria rede e o 255 que tem função de *broadcast* (KUROSE, 2000).

Em substituição à antiga notação em classes, apresentada no capítulo anterior, com o advento das sub-redes surgiu a necessidade de uma nova notação para os tipos de redes. Por isso, o CIDR (*Classles InterDomain Routing*), um novo padrão de roteamento definido pela RFC 1519 que possibilitava a implementação das sub-redes, definiu uma nova notação que, em vez de utilizar classes pré-definidas para identificar uma determinada rede, utilizava o número de bits no endereço IP usados para definir a rede. Por exemplo, uma rede classe C se tornaria uma rede /24, visto que os primeiros 24 bits do seu endereço IP representam a própria rede.

Voltando ao exemplo citado anteriormente, se a universidade desejasse dividir sua rede Classe B (rede /16), poderia fazê-lo, instalando, por exemplo, 8 roteadores espalhados por seus departamentos, onde cada um controlaria uma sub-rede /19, com capacidade para 8.192 *hosts* cada, como ilustra a Figura 16.

Figura 16 - Divisão de uma rede para departamentos de uma universidade.



Fonte: (TANEMBAUM, 1996)

5.3.2 Camada de transporte

Similiar à camada homônima do modelo OSI, a camada de transporte do modelo TCP/IP também tem como objetivo criar um canal de comunicação entre dois *hosts* indenpendente de toda estrutura que está presente nas camadas mais baixas. O modelo TCP/IP possui dois protocolos principais nesta camada: o TCP e o UDP.

5.3.2.1 Protocolo TCP

O TCP (*Transmission Control Protocol*) ou protocolo de controle de transmissão é dito um protocolo da camada de transporte orientado a conexão (TANEMBAUM, 1996). Isto porque este protocolo estabelece uma “conversação” entre os dois *hosts* que iniciarão uma transferência de pacotes.

O protocolo TCP oferece um serviço de transmissão de pacotes fiável, isto é, ele garante que os pacotes de dados chegarão ao destino na ordem correta. Para isto, este protocolo divide os dados provenientes da camada de aplicação, divide-os em pedaços menores que caibam nos frames ethernet, adiciona um cabeçalho com dados que possibilitarão o controle da transmissão e o encapsula em um datagrama IP.

Após a conexão entre dois *hosts* ser estabelecida e os parâmetros da transmissão serem determinados, o envio e recebimento de pacotes é iniciado, onde o TCP irá

acionar mecanismos para confirmar a entrega e o recebimento, a integridade e a ordenação correta dos pacotes. Após o *host* de destino sinalizar o recebimento do último pacote da transmissão, o *host* emissor finaliza a conexão (KUROSE, 2000).

5.3.2.2 Protocolo UDP

Outro protocolo principal da camada de transporte do modelo TCP/IP é o protocolo UDP. Diferente do TCP, o UDP (*User Datagram Protocol*) não estabelece qualquer conexão entre os *hosts*. Os datagramas de aplicações são encapsulados em um datagrama UDP com um cabeçalho simples, contendo a porta de origem dos dados, a porta de destino, o comprimento da mensagem e o *checksum*, uma sequência de 16 bits utilizada para verificação de erros (POSTEL, 1980).

Apesar de não-fiável, o protocolo UDP é a melhor opção para aplicações que necessitam de comunicação em tempo real ou com broadcast de dados, como conversasões por voz e vídeo ou *streamming* de vídeos ou músicas.

5.3.3 Camada de aplicação

Tanembaum (1996) afirma que com a experiência com o modelo OSI notou-se que as camadas de sessão a apresentação eram raramente utilizadas nos projetos de redes reais. Por isso, o modelo TCP/IP resolveu excluir estas duas camadas, restando apenas a camada de aplicação acima da camada de transporte.

Na camada de aplicação se encontram os protocolos de mais alto nível, que fornecem serviços diretamento à aplicações e usuários. Exemplos conhecidos de protocolos de aplicação utilizados pelo TCP/IP são:

- TELNET: Protocolo de terminal virtual. Permite o acesso e controle de uma máquina remota;
- FTP (*File Transfer Protocol*): Protocolo para transferência fiável de arquivos;
- SMTP (*Simple Mail Transfer Protocol*): O correio eletrônico foi estabelecido incialmente pela troca simples de arquivos. Posteriormente, o SMTP foi desenvolvido como uma alternativa mais robusta para a troca de mensagens.

- HTTP (*Hyper Text Transfer Protocol*): Protocolo básico para a requisição de páginas WEB na internet.

5.3.4 Camada de host/rede

O modelo TCP/IP não especifica o que deve acontecer abaixo da camada de internet, exceto o fato de que o *host* precisa se conectar à rede por algum protocolo que permita o envido de datagramas IP. Atualmente a grande maioria das redes que se baseiam no modelo TCP/IP utilizam o protocolo Ethernet na camada de enlace, utilizando um endereço de 48bits (MAC) para identificação de cada ponto de rede.

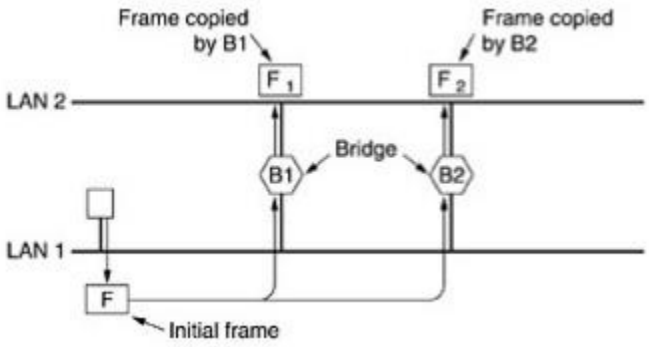
5.4 Spanning Tree Protocol

Em projetos de redes de comunicação, em especial para sistemas críticos como um sistema *Self-Healing*, a disponibilidade da rede torna-se uma das principais preocupações. Para garantir que a comunicação possa continuar operando mesmo em caso da perda de algum enlace ou dispositivo de conexão, muitas redes de comunicação são construídas com rotas alternativas de transmissão, isto é, uma sub-rede pode enviar frames para outra por mais de um caminho.

Entretanto, a inserção de rotas alternativas pode ocasionar problemas de *loops* ou ciclos na topologia.

A Figura 17 ilustra um exemplo fictício proposto por Tanenbaum (1996), onde duas redes locais (LAN) são conectadas por dois *bridges*, equipamentos semelhantes a *hubs*, utilizados para conectar LAN's. Quando um *frame* F de destino desconhecido é enviado da LAN 1 para a LAN 2, os *bridges* B1 e B2 fazem cópias deste e, seguindo o procedimento de encaminhamento de quadros desconhecidos, os inundam na rede. Então, B1 detecta o *frame* de destino desconhecido F2 e B2 detecta F1, cópias de F, e os encaminham de volta para a LAN 1. Este ciclo acontece infinitamente, prejudicando o funcionando das redes.

Figura 17 - Exemplo de loop entre redes.



Fonte: (TANEMBAUM, 1996)

Para evitar problemas de *loops* em topologias com rotas redundantes foram desenvolvidos os protocolos de prevenção de *loops*. O mais conhecidos deles é o STP (*Spanning Tree Protocol*).

O STP utiliza o algoritmo *spanning tree* ou árvore de extensão para, a partir de um nó raiz ou *root*, definir um conjunto de ligações com custo mínimo, que alcance todos os outros nós da rede e que seja livre de *loops*.

Para isto, o STP utiliza *frames* chamados BPDU (*Bridges Protocol Data Units*), que são enviados para a rede para possibilitar a troca de informações como o identificador dos bridges e o custo até o *root*. Após o cálculo da topologia, outros BPDU's são enviados, determinando se determinada porta do *bridge* deve entrar em estado de encaminhamento, possibilitando o recebimento e envio de *frames*, ou bloqueio, onde esta só recebe *frames* BDPU para uma ocasional mudança de topologia.

O recurso da redundância é mantido pela capacidade que o protocolo STP tem de, ao detectar uma mudança de topologia, provavelmente causada pela indisponibilidade de algum enlace ou *bridge*, recalcular a árvore de expensão para a nova configuração da rede e modificar os estados das portas de alguns *bridges*, se for necessário.

5.5 VLAN

As VLANs (*Virtual Local Area Network*), ou redes locais virtuais, é uma subdivisão lógica de uma rede local. Kurose (2000) diz que as VLANs foram criadas para solucionar 3 problemas principais de redes locais compartilhadas por muitos usuários de perfis distintos:

- Falta de isolamento de tráfego: Informações que não são de interesse ou não devem ser acessadas por todos trafegam pela rede e podem ser capturadas utilizando analisadores de pacotes;
- Uso ineficiente de comutadores: Para isolar o tráfego poderia se utilizar comutadores que separassem os grupos de usuários. Porém, se existissem muitos grupos, um número muito grande de comutadores seria necessário, tornando o projeto de rede caro e ineficiente;
- Gerenciamento de usuários: Se temos usuários que trocam de perfil ou tem mais de um perfil diferente, o que pode ser feito?

Switches com a capacidade de trabalhar com VLANs podem dividir uma única rede física em várias outras redes virtuais, atribuindo algumas de suas portas a elas. Com este recurso dados provenientes de uma VLAN não são compartilhados por outra VLAN, mesmo as duas estando compartilhando o mesmo switch.

Em relação à escalabilidade da rede, surgiram problemas ao conectar comutadores com várias VLAN's. Para tentar solucionar isso poderia-se criar uma porta de conexão para cara VLAN de um comutador ao outro, porém esta solução requer uma porta para cada rede virtual diferente de cada switch. Como solução, surge o conceito de porta *trunk* ou tronco, uma porta do comutador que quando configurada com esta função permita o repasse de pacotes de qualquer VLAN. Com isto, para conectar dois comutadores bastaria configurar uma porta *trunk*.

Para a identificação de uma VLAN durante o repasse entre portas tronco, o IEEE definiu um novo campo para os quadros Ethernet, adicionando um campo de identificação de quatro *bytes*, que é inserido quando o frame chega na pronta tronco de saída e removido no processamento da porta tronco de entrada.

Entretanto, para repassar dados de uma VLAN para outra é necessário um *router* ou um *firewall*, dispositivos da *layer* 3 com capacidade de roteamento e controle de acesso.

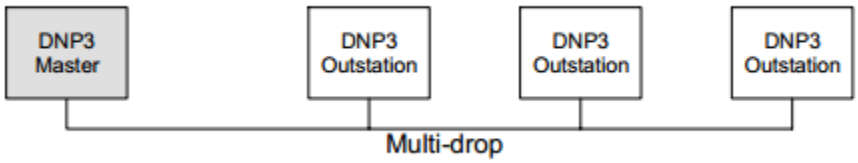
5.6 Protocolo DNP3

O DNP (*Distribuited Network Protocol*) é um protocolo de comunicação de código aberto amplamente utilizado na automação de sistemas elétricos. Ele estabelece uma arquitetura mestre-escravo entre estações.

Uma estação mestre (*Master*) é um dispositivo com inteligência para coletar e processar dados e interligar dispositivos remotos. Uma estação escrava (*Outstation*) são dispositivos de campo como relés e medidores inteligentes que transmites dados para uma estação mestre (DNP GROUP USERS).

Dentre as topologias possíveis dentro do protocolo DNP3, a mais utilizada é a *multi-drop*, onde uma estação mestre recebe dados de várias estações escravas, como ilustra a Figura 18.

Figura 18 - Topologia multi-drop do protocolo DNP3.



Fonte: (DNP GROUP USERS)

Uma das principais características do protocolo DNP3 é sua biblioteca de objetos, cujos tipos de dados podem ser divididos, entre outros tipos, em:

- Entradas analógicas: Representam valores escalares provenientes de uma *outstation*;

- Entradas digitais: Variáveis binárias provenientes de uma outstation;
- Saídas digitais: Comandos binários enviados da estação mestre para a escrava;
- Saídas analógicas: Valores escalares enviados do mestre para o escravo.

Apesar do protocolo DNP3 ter sido concebido inicialmente para estabelecer uma conexão *serial* ponto-a-ponto, novas versões do protocolo possibilitam o encapsulamento dos dados em segmentos TCP/IP, permitindo a aplicação do DNP3 em redes Ethernet (CLARKE e REYNDERS, 2004).

5.7 SNMP e o Gerenciamento de rede

Com o desenvolvimento de redes de comunicação, estas se tornaram estruturas cada vez mais complexas. Se antes, ao detectar uma falha na rede, testes simples como um *ping* e análise manual da rede eram suficientes para identificar as causas de um problema, atualmente, redes com um grande número de roteadores, *switches* e *hosts* necessitam de um gerenciamento mais sistemático (KUROSE, 2000).

Um sistema de gerência de rede possibilta a um administrador uma maior facilidade em:

- Detecção de falhas: Uma entidade de rede como um roteador, *switch* ou *host* pode avisar o administrador que uma de suas interfaces de rede não está funcionando, auxiliando na detecção e correção de falhas na rede;
- Monitoramento de rotas: O administrador pode detectar mudanças constantes nas rotas e tabelas de roteamento da rede, o que indicaria uma má configuração ou mal funcionamento de um roteador;
- Detecção de intrusos: O administrador da rede pode avaliar o tráfego de dados de uma fonte suspeita ou tipos suspeitos de pacotes;

A *International Organization for Stardardization* (ISO) criou um modelo de gerenciamento de redes, dividindo-o em cinco áreas (KUROSE, 2000):

- Gerenciamento de desempenho: O gerenciamento de desempenho tem como meta quantificar, medir, informar, analisar e controlar o desempenho da rede.

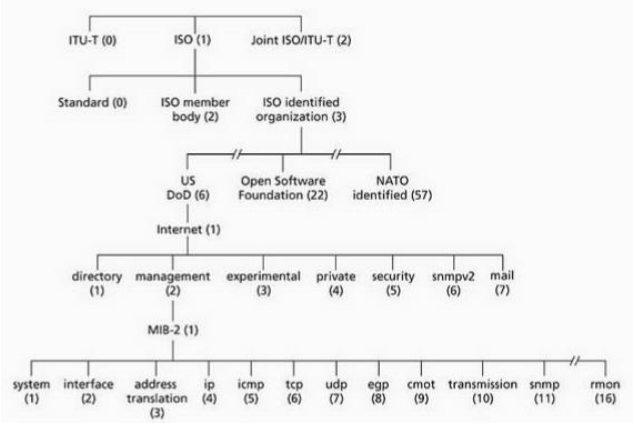
Por exemplo, ferramentas deste tipo podem informar o nível de utilização e vazão da rede;

- Gerenciamento de falhas: Tem como objetivo detectar, registrar e reagir a falhas na rede, como a indisponibilidade de um *host*, *switch* ou todo um enlace;
- Gerenciamento de configuração: Permite que o administrador saiba quais são os dispositivos conectados à rede e suas configurações de hardware e software.
- Gerenciamento de segurança: Pretende controlar o acesso a recursos da rede de acordo com uma política de segurança definida.

Para efetuar o devido gerenciamento das redes de comunicação necessitou-se da criação de protocolos com esta devida finalidade, surgindo então o SNMP. Conhecido como o "protocolo de gerenciamento padrão da internet", o SNMP (*Simple Network Management Protocol*) foi definido pela IETF na RFC 3410 (HARRINGTON, PRESUHN e WIJNEN, 2002) como uma ferramenta para monitorar redes IP. Baseado numa arquitetura gerente-agente, onde cada ator hora pode ser cilente e hora pode ser servidor, dependendo da ação executada, o SNMP tem sua estrutura constituída em quatro partes (KUROSE, 2000):

- Objetos de Gerenciamento da rede: Os objetos MIB (*Management Information Base*), ou base de informações de gerência, são definições de variáveis que serão acessadas pelo sistema de gerenciamento. Estes objetos formam um banco de dados virtual, organizado em uma estrutura hierárquica em árvore e indexado por um identificador único, como mostra a Figura 19. Para, por exemplo, acessar os dados referentes ao protocolo TCP, utilizaríamos os objetos com ID de prefixo 1.2.6.1.2.1.3. Os valores dos objetos MIB podem ser acessados através da operação GET ou modificados através da operação de SET. Além disso, alarmes denominados TRAP's podem ser configurados para alertar o administrador em caso de mudanças em valores de objetos MIB.

Figura 19 - Árvore de objetos MIB.



Fonte: (KUROSE, 2000).

- Linguagem de definição de dados: A SMI (*Strutcture of Management Information*) define os tipos de dados, modelos de objetos MIB e regras para escrever e revisar informações de gerenciamento.
- O protocolo: O próprio protocolo SNMP, ou seja, a forma como dados são recebidos e enviados ao dispositivo.
- Segurança e administração: A segunda versão do SNMP, o SNMPv2c, implantou um mecanismo de autenticação por meio de comunidades. As comunidades são *strings* definidas no agente que servem como uma espécie de senha para que gerentes possam acessar ou modificar dados. Já o SNMPv3 conta com um sistema mais robusto de segurança, definindo um conjunto de usuários autenticados com senha e um sistema de *views* que limitam o que cada usuário pode ler ou alterar.

6 ESTUDO DE CASO: SELF-HEALING CEMAR

6.1 Introdução

Como relatado no início deste trabalho, num setor altamente competitivo e regulado como o da distribuição de energia elétrica, as empresas vem procurando novas soluções para melhorar seus indicadores de qualidade, como o DEC e o FEC, e, por conseguinte, alcançar ganhos em redução de multas e aumento da energia vendida.

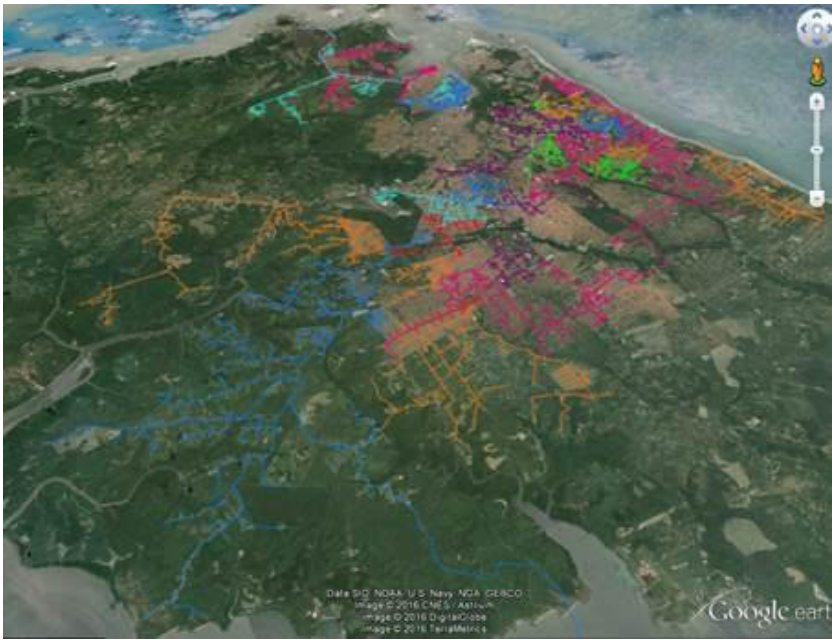
Com este intuito, em 2014 a CEMAR (Companhia Energética do Maranhão) iniciou a implantação do Projeto *Self-Healing*. Neste projeto, vislumbrou-se a recuperação, realocação e implantação de equipamentos automatizados na rede de distribuição (RD), possibilitando o desenvolvimento de um sistema SH que permitisse a recomposição automática de trechos de alimentadores com grande número de clientes na cidade de São Luís.

6.2 Arquitetura do Projeto SH CEMAR

Após estudos de viabilidade realizados juntamente com a equipe de Planejamento, as ondas, como foram denominados os conjuntos de alimentadores inclusos em um circuito de manobras, foram definidas e iniciou-se o processo de estruturação dos equipamentos da rede elétrica, instalando-se ou realocando-se religadores e chaves telecomandas.

A Figura 20 ilustra a distribuição dos alimentadores (separados por cor) inclusos no projeto, cobrindo boa parte de região urbana da cidade.

Figura 20 - Alimentadores do Projeto SH CEMAR.



6.2.1 Modelo SH

Baseado no estudo feito por Sales (2014), decidiu-se optar por modelo de *Self-Healing* centralizado, utilizando o sistema SCADA Elipse Power como centro de controle responsável por todo o processamento das manobras.

Dentre os fatores que influenciaram na decisão por este modelo, pode-se destacar a facilidade de configuração do sistema concentrado em uma só plataforma, a familiaridade com o ambiente de desenvolvimento do SCADA que já era utilizado pela equipe da Automação e capacidade de integração com recursos já aplicados à automação de subestações.

6.2.2 Módulo SH Elipse Power

Para o controle do sistema *Self-Healing*, foi utilizado um novo módulo para o sistema SCADA Elipse Power já utilizado pela CEMAR. Esta solução se baseia no Elipse Power CAD Editor, um novo modelador elétrico semelhante ao modelador de subestações, mas que possibilita a representação da topologia e parâmetros elétricos de uma rede de distribuição, gerando um banco de dados com as informações necessárias para executar os algoritmos de análise. O CAD Editor

(Figura 21) também permite a criação automática de telas (Figura 22), diagramas de operação e objetos de dados para utilização no SCADA.

Figura 21 - Ambiente de modelagem CAD Editor.

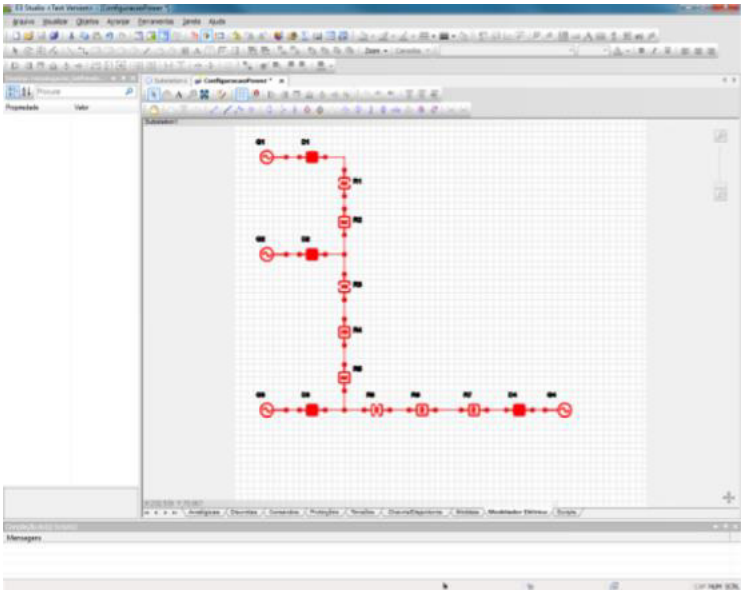
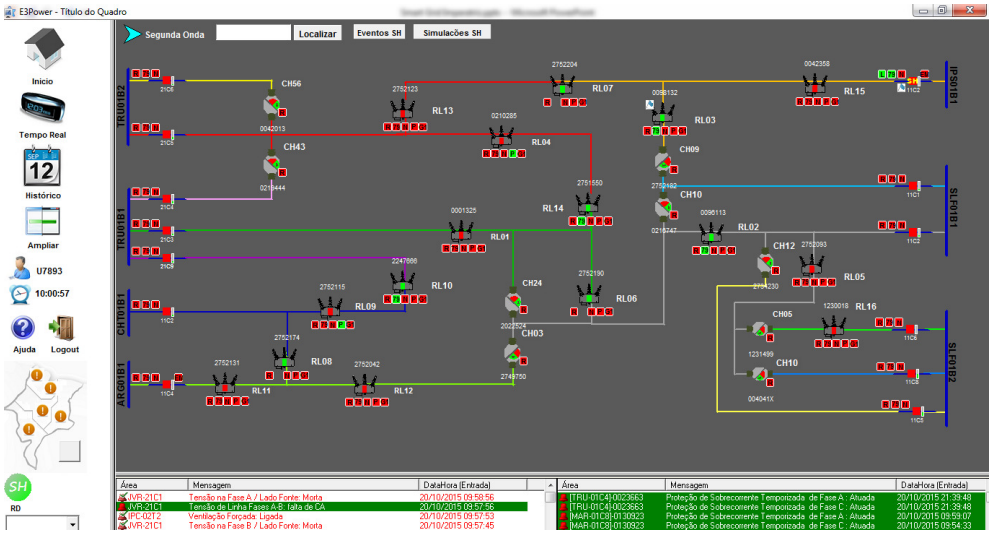


Figura 22 - Tela de operação e monitoramento de uma onda SH no SCADA.



Com a rede de distribuição modelada, variáveis do SH podem ser configuradas em cada objeto (representação dos dados dos equipamentos de campo), como a disponibilidade deste para uma recomposição automática e limite de corrente suportado.

Após a configuração dos equipamentos o módulo SH monitora o estado dos equipamentos de campos procurando identificar uma falta ou situação de sobrecorrente. Quanto identificada uma situação passível de atuação, o sistema efetua os cálculos e estabelece a ordem de manobras e tenta executa-las. Durante a sequência de manobras, se algum equipamento não receber ou executar o comando, toda a sequência é abortada e o administrador avisado.

6.3 Rede de comunicação

Parte fundamental de um sistema *Self-Healing* e principal objeto de estudo deste trabalho, a rede de comunicação para o Projeto SH da CEMAR foi projetada de modo que todos os requisitos básicos fossem atendidos, mantendo-se uma relação custo-benefício aceitável.

Neste capítulo serão descritas quais tecnologias foram adotadas na implantação da rede e as principais razões para as escolhas. Serão destacados pontos-chave da estrutura da rede, como o meio de transmissão utilizado, a arquitetura na qual se baseou a rede e a ferramenta de gerenciamento desenvolvida.

6.3.1 Meio de transmissão

Depois de estabelecidos todos os equipamentos que deveriam se comunicar com o sistema SCADA, necessitou-se decidir qual o meio de transmissão seria utilizado na rede de comunicação.

A princípio, duas opções foram propostas: a conexão com fio por meio de fibra óptica e a comunicação sem fio via rádio. Ambas as opções teriam a capacidade de conectar todos os equipamentos necessário nada rede, mesmo os mais distantes. A Tabela 1 mostra um breve comparativo entre os dois meios:

Tabela 1 - Comparação em fibra óptica e rádio.

	Fibra Óptica	**Rádio**
Alcance	Até 5km sem repetidores	Dezenas de quilômetros.
Infraestrutura	Complexa	Simples
Velocidade	Altíssima	Alta
Interferências	Quase inexistentes	Alta
Vulnerabilidade da estrutura	Alta	Baixa
Custo	Alto	Médio

Podemos analisar que a comunicação via rádio resultaria numa implantação mais simples com, teoricamente um custo mais baixo. Entretanto, o principal fator a ser levado em consideração no projeto de uma rede de comunicação para um projeto SH é a confiabilidade. Como já foi dito neste trabalho, a comunicação compõe parte vital no sucesso de sistema *Self-Healing* e um alto grau de indisponibilidade e falhas pode comprometer todo o projeto.

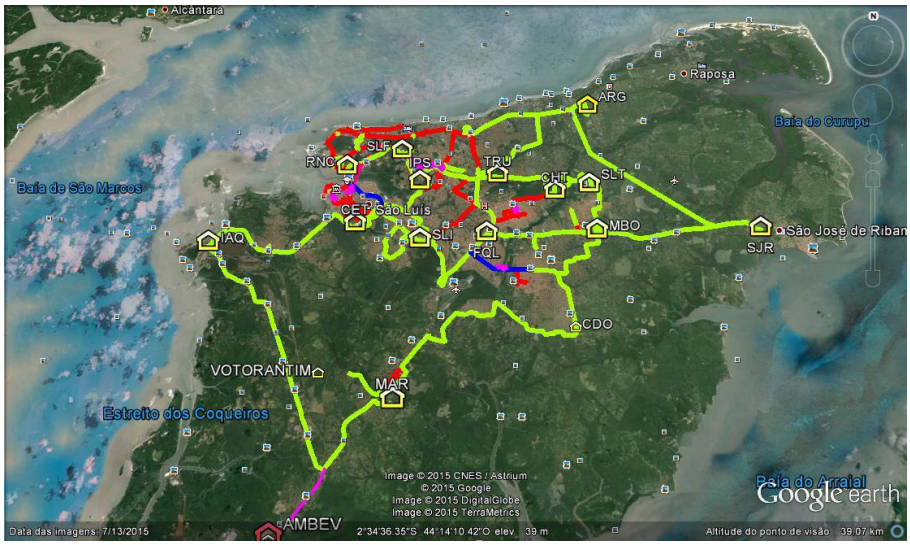
A grande vantagem da fibra óptica sobre a transmissão via rádio é a sua baixíssima suscetibilidade à interferência por fatores externos, como clima e campos elétricos. Com equipamentos de comunicação tão próximos da rede elétrica, transmissores de rádio podem sofrer grandes interferências, gerando ruídos na transmissão e até indisponibilidades. Além disso, em períodos de fortes chuvas, onde as falhas na rede elétrica são maiores e um sistema SH se torna ainda mais necessário, as ondas de rádio tem seu alcance prejudicado, reduzindo sua confiabilidade.

Em relação à infraestrutura, transmissores de rádio novamente levariam vantagem por não necessitar de uma estrutura de suporte física, como é o caso das fibras ópticas. Entretanto, no caso da automação de sistemas de distribuição, cabos de fibra óptica podem fazer uso da estrutura dos cabos da rede elétrica, visto que não sofrem interferências de campos elétricos.

Quanto ao custo, a compra de extensos cabos de fibra óptica e *switches* com suporte à essa tecnologia resultaria em gastos muito maiores do que a compra de

transmissores de rádio adequados. Porém, foi importante levar em conta que a CEMAR já dispunha de uma rede de fibras ópticas que conectavam algumas de suas subestações, como mostra a Figura 23:

Figura 23 - Rede via fibra óptica entre subestações CEMAR.



Fazendo uso desta estrutura, as alterações necessárias seriam reduzidas e, por conseguinte, os gastos também cairiam, tornando-os equiparáveis aos gastos com uma rede via fibra, como mostra a Tabela 2:

Tabela 2 - Comparativo de custos entre Fibra Óptica e Rádio.

	Custo - Materiais	**Custo – Mão-de-Obra**	**Custo - Total**
Fibra Óptica	R$ 373.800,00	R$ 550.000,00	R$ 923.800,00
Rádio	R$ 612.320,00	R$ 187.500,00	R$ 799.820,00

De acordos como os custos orçados, nota-se que uma rede com transmissão via rádio custaria R$ 123.980,00 a menos que uma rede de fibra óptica, uma economia de apenas 13% que não compensaria as desvantagens em relação à tecnologia mais cara, porém mais eficaz.

Por estes fatores, decidiu-se pela implantação de uma rede de comunicação via fibra óptica que, apesar de ter um custo ligeiramente maior, proporcionaria uma confiabilidade muito maior para o sistema.

6.3.2 Arquitetura

Após a definição do meio de transmissão, precisou-se definir qual seria a arquitetura lógica da rede. Os principais fatores a se considerar nesta decisão foram:

- Suporte à topologia: A arquitetura precisaria ser robusta suficiente para permitir a conexão de todos os equipamentos espalhados de forma irregular pela rede, inclusive suportando a implantação de caminhos redundantes para aumentar a confiabilidade.
- Alto desempenho: Em redes de comunicação para sistemas comuns, atrasos de algumas centenas de milissegundos são aceitáveis e raramente notados. Entretanto, em sistemas SH a resposta da rede deve acontecer em, no máximo, dezenas de milissegundos, pois quando tratamos de distribuição de energia cada fração de segundo se torna importante. Por isto, a arquitetura da rede deveria proporcionar transmissões rápidas, com poucos atrasos e uma alta vazão.
- Segurança: A rede de comunicação deveria dispor de mecanismos de segurança de dados, visto que sua estrutura está exposta, muitas vezes em locais remotos e isolados. O acesso à dados críticos do sistema de distribuição a indivíduos não autorizados e mal-intencionados poderia acarretar em sérios problemas.

Além desses fatores, a arquitetura deveria fornecer suporte ao modelo TCP/IP, possibilitando a integração à rede já existente na empresa.

Por isto, decidiu-se utilizar uma arquitetura baseada em *switches layer* 2. Comutadores que operam nesta camada do modelo OSI são mais simples que roteadores, efetuando o controle do tráfego de pacotes baseado apenas em endereços MAC e em VLAN's. Os *switches layer* 2 proporcionam os seguintes benefícios:

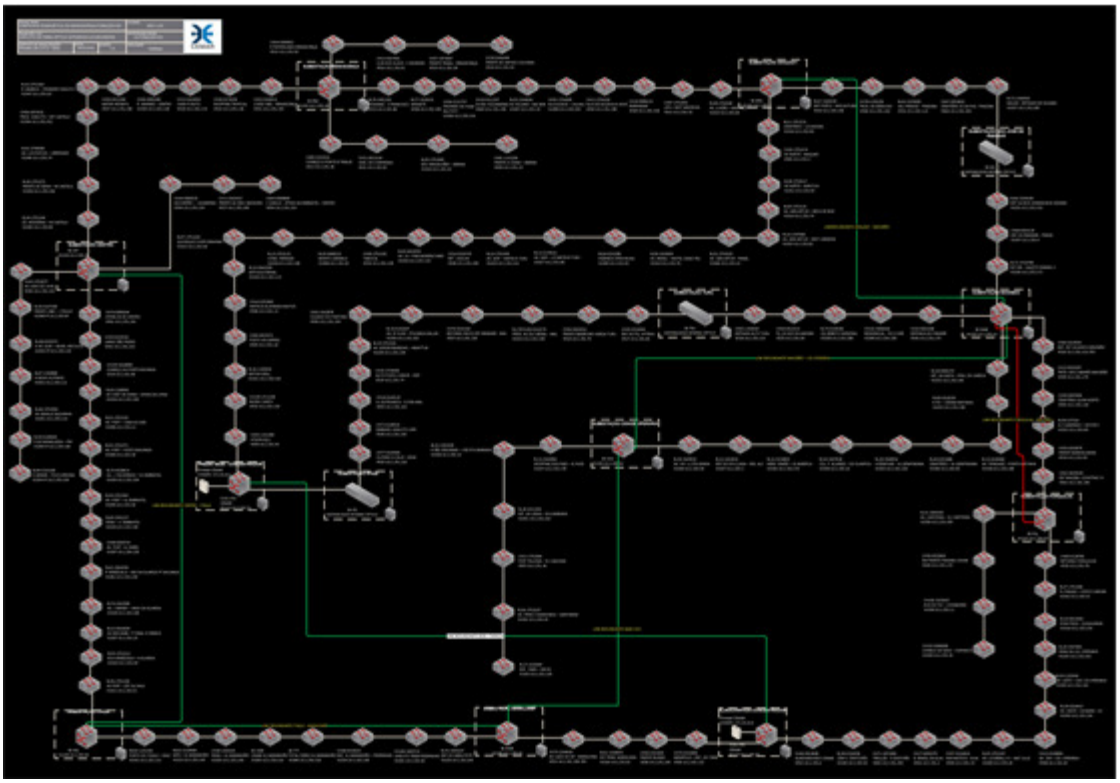
- *Bridging* de sub-redes baseado em hardware;
- Alta velocidade de processamento de pacotes;
- Baixa latência;
- Baixo custo;

- Não necessita de acesso à camada de rede.

Por motivos de segurança e isolamento de tráfego, cada *switch* e o equipamento de campo que este está conectado pertenceriam a uma VLAN única de máscara /30. Com isto, um indivíduo mal-intencionado que conseguisse se conectar ao *switch* não teria acesso aos pacotes provenientes dos outros *switches*, além de ter seu acesso à rede principal da CEMAR bloqueado por *firewalls* instalados na sede e no almoxarifado da empresa, de onde os dados sobem para as camadas superiores até chegar ao sistema SCADA. Além disso, a máscara de rede com apenas 2 bits para endereçamento de *hosts*, limitariam o número de endereços IP a 4, facilitando o monitoramento dos dispositivos conectados.

Em relação à topologia, a Figura 24 mostra que a rede possui um amplo conjunto de caminhos redundantes para o tráfego de dados, inclusos para aumentar a confiabilidade da rede.

Figura 24 - Topologia da rede de comunicação do projeto SH.



Além das ligações à equipamentos adjacentes, foram construídas conexões redundantes entre as subestações, a sede da empresa e o almoxarifado, utilizando a estrutura de fibra já existente. Com a inserção destas redundâncias, cria-se a possibilidade de *loops* entre as VLAN's, o que poderia ocasionar o mal funcionamento da rede.

Para sanar este problema, os *switches* da rede deveriam suportar o protocolo STP que, após definido o *switch* da sede como *root*, calcularia a melhor rota entre os equipamentos e reconfiguraria a rede, eliminando os *loops*. Além disso, o STP reconfiguraria a rede automaticamente em caso de falha em algum *switch* ou trecho de fibra.

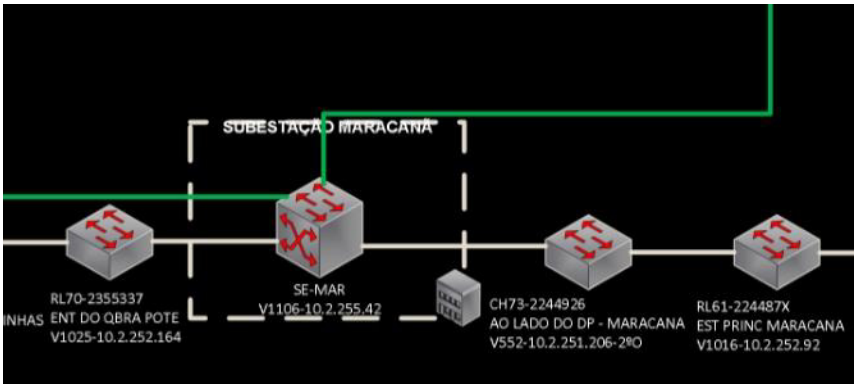
Como forma de evitar problemas de roteamento devido à utilização de VLAN's, todas as portas dos *switches* dos equipamentos de campo deveriam ser configuradas para a função de tronco ou *trunk*, isto é, permitir a passagem de pacotes de outras VLAN's, porém sem acessa-los.

Com esta arquitetura, a rede de comunicação do projeto SH da CEMAR, além de conectar com alta performance todos os equipamentos necessários, funcionaria de forma robusta, menos suscetível a falhas e mais segura.

6.3.3 Gerenciamento

Com uma rede de grande porte, composta por mais de 150 *switches* e com estrutura complexa, notou-se a dificuldade de detecção e correção de falhas na comunicação. Um exemplo simples pode ser dado analisando o trecho ilustrado pela Figura 25:

Figura 25 - Trecho da rede de comunicação.



Imaginando um problema fictício no trecho de fibra que liga a CH73 à subestação Maracanã, o *Spanning Tree Protocol* notaria a falha e reconfiguraria a rede para que a CH73 enviasse e recebesse seus dados pela conexão com o RL61. Entretanto, este problema dificilmente seria notado pelo administrador sem uma ferramenta de gerenciamento da rede, já que rapidamente o funcionamento da rede seria recomposto de forma automática. Com isto, o trecho permaneceria em falha até que a redundância, por acaso, também falhasse e a CH73 ficasse sem comunicação.

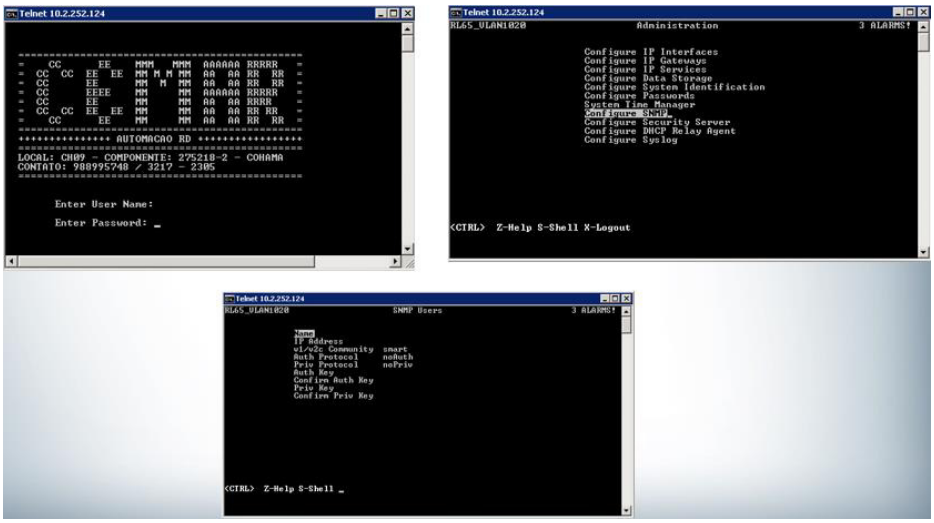
Além de casos com o apresentado anteriormente, detectar falhar apenas com simples testes de *ping*, sem uma referência mais gráfica do problema, atrasavam e muito a detecção e resolução de uma falha.

Pensando nestas necessidades, elaborou-se um sistema de gerência da rede de comunicação baseado no protocolo SNMP, integrado ao sistema SCADA Elipse Power.

A escolha do protocolo foi simples por este ser o protocolo mais completo e mais utilizando na área de gerência de redes de comunicação. Aproveitando o suporte dado pelo Elipse Power a este protocolo, o sistema de gerenciamento foi construído integrado ao SCADA, fazendo uso de recursos como bibliotecas gráficas e de dados e criação simplificada de telas, o que facilitou bastante o processo de desenvolvimento.

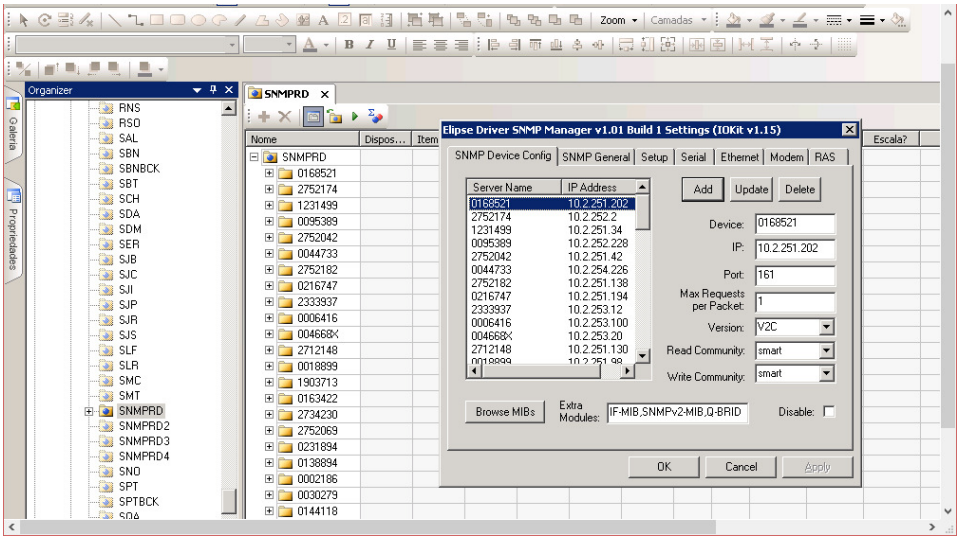
Primeiramente, para habilitar o monitoramento dos *switches*, precisou-se configurar o protocolo SNMP em cada um deles. A Figura 26 mostra o acesso feito via terminal remoto aos equipamentos e a configuração dos parâmetros do protocolo, como o endereço IP do gerente e a comunidade de acesso aos dados.

Figura 26 - Telas de configuração do SNMP nos switches.



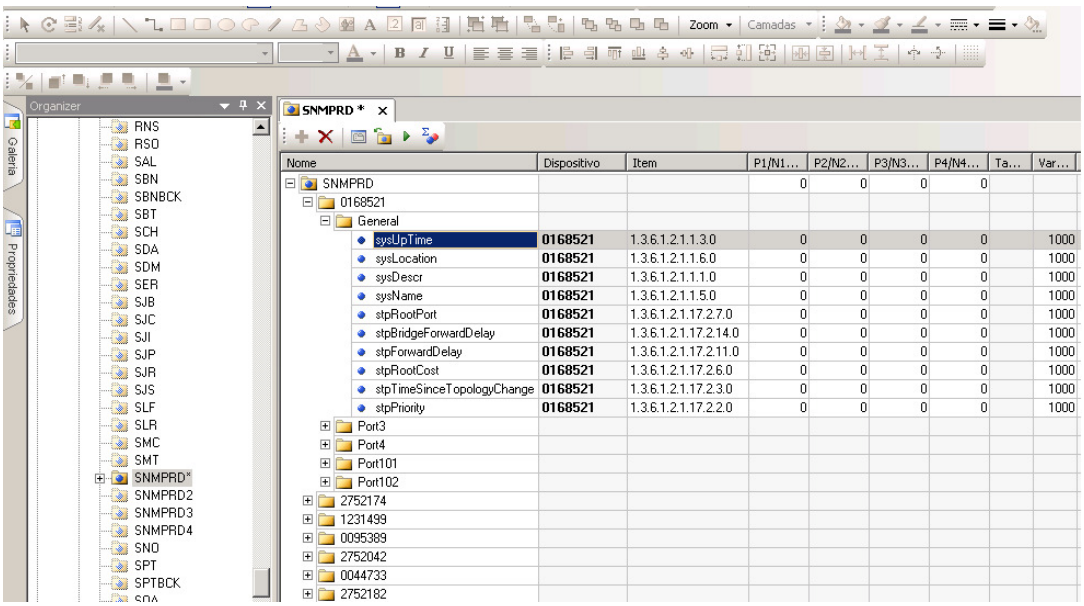
A próxima etapa baseou-se na configuração do driver do protocolo SNMP no servidor de comunicação do SCADA, configurando o endereço IP de cada *switch* juntamente com a comunidade de acesso (Figura 27).

Figura 27 - Configuração do driver SNMP no Elipse Power.



Ainda no servidor de comunicação do Elipse Power, são criados os pontos de comunicação, representando as variáveis que se deseja monitorar, identificados pelos ID's dos objetos da MIB, como mostra a Figura 28.

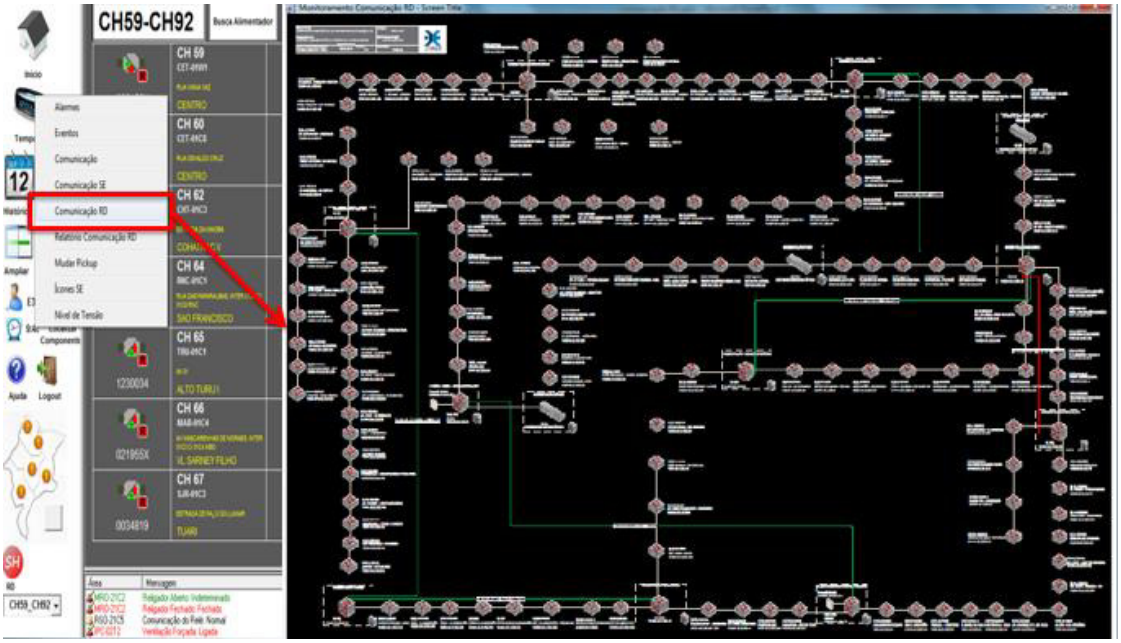
Figura 28 - Criação de pontos de comunicação SNMP.



A última etapa do desenvolvimento do sistema de gerenciamento da rede de comunicação foi a criação de objetos de dados que pudessem receber e tratar os

dados provenientes de cada equipamento gerenciado e a representação de informações numa tela sinótica, como mostra a Figura 29.

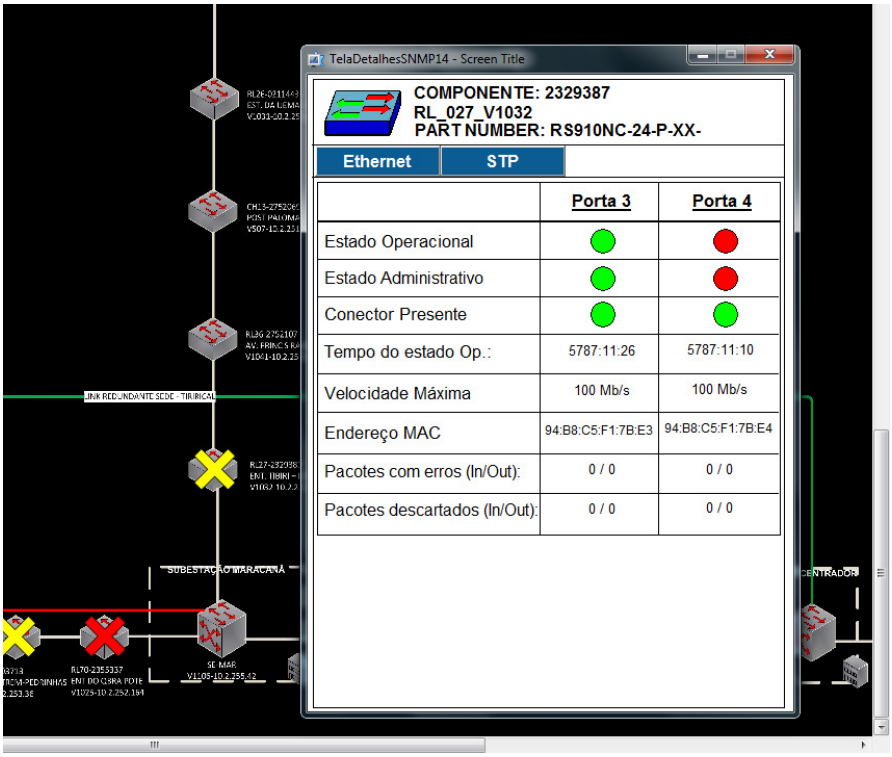
Figura 29 - Acesso à tela de monitoramento da rede pelo SCADA.



Cada equipamento na tela principal tem três sinalizações: falha em uma porta, sem comunicação e bloqueado para manutenção (Figura 30). Informações detalhas como tempo do estado atual de cada porta do equipamento, velocidade máxima, erros em pacotes e dados do STP podem ser obtidas clicando no equipamento (Figura 31).

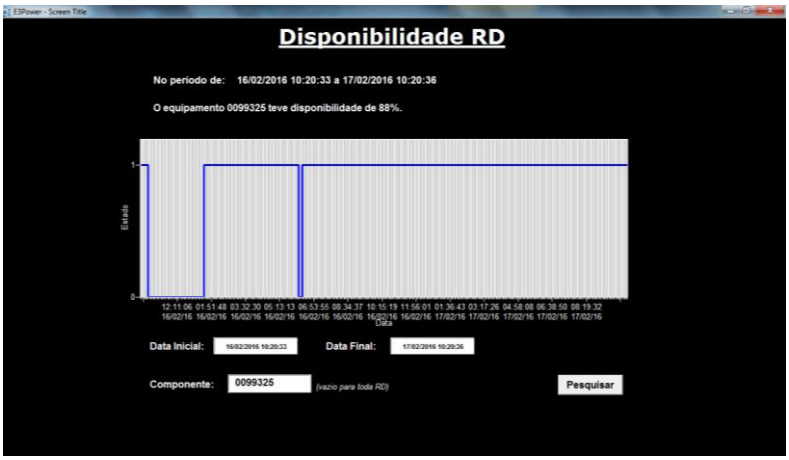
Figura 30 - Sinalizações dos equipamentos de comunicação.

Figura 31 - Detalhes de um equipamento de rede.



Além do monitoramento dos equipamentos, outro recurso importante implementado no sistema de gerência da rede de comunicação do projeto SH da CEMAR foi uma ferramenta de geração de relatórios rápidos de disponibilidade (Figura 32). Informações da disponibilidade de um equipamento em específico ou de toda a rede de distribuição podem ser obtidas em forma de relatório ou planilha.

Figura 32 - Tela de relatórios de disponibilidade da rede.



6.3.4 Resultados

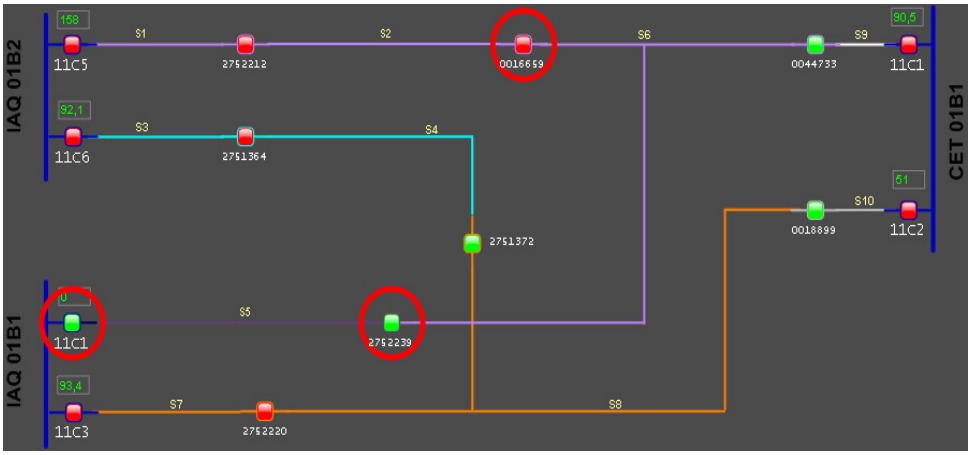
Como resultados deste trabalho, podemos destacar o impacto de uma atuação real do sistema *Self-Healing* quando suportado por uma rede de comunicação confiável.

No dia 03 de fevereiro de 2015, o contato de um galho de árvore com a rede de distribuição ocasionada por uma chuva forte, fez com que a proteção automática do disjuntor 11C1 da subestação Itaqui atuasse e o abrisse, causando a falta de energia para 9.756 clientes atendidos por este alimentador.

Ao detectar que o ciclo que religamento do disjuntor 11C1 não conseguiu recuperar o fornecimento de energia, o controle central do SH iniciou os cálculos de manobras possíveis e detectou que, comandando dois equipamentos, poderia recuperar boa parte do trecho atingido, redirecionando parte da carga para o alimentador 5 também de Itaqui.

A Figura 33 mostra o trecho depois da atuação do SH, que comando a abertura do equipamento de componente 2752239 para isolar o trecho do problema e o fechamento do equipamento de componente 0016659, realimentando parte do trecho.

Figura 33 - Manobras efetuadas em atuação do sistema SH.



O cálculo da manobra levou cerca de 1,5 segundos e a execução das manobras cerca de 10 segundos. O fornecimento de energia foi recomposto a 9.463 clientes, 97% do total de cliente afetados.

Também é possível notar os impactos da automação do sistema de distribuição na melhoria dos índices de continuidade DEC e FEC da CEMAR. Todos os anos a ANEEL (Agência Nacional de Energia Elétrica), órgão regulamentador das empresas de distribuição de energia, elabora um ranking das melhores concessionárias, de acordo com a média de seus índices DEC e FEC, chamada de DGC (Desempenho Global de Continuidade).

No ano de 2014, a CEMAR ocupava o 3º lugar no ranking, atrás da Companhia Força e Luz Santa Cruz e da Companhia Energética do Ceará – COELCE. Já no ano seguinte, após a implantação do sistema SH e da melhoria da automação do sistema de distribuição da capital, a CEMAR assumiu a liderança do ranking, se tornando a empresa com o menor índice de faltas em todo o país.

7 CONCLUSÃO

Este trabalho demonstrou o processo de planejamento, implantação e gerenciamento de uma rede de comunicação para o Projeto *Self-Healing* da CEMAR. A princípio foram explanados os conceitos de *Smart Grid* e *Self-Healing*, destacando a importante de soluções deste tipo para uma empresa de distribuição de energia elétrica no cenário nacional.

Foi feita uma análise básica sobre sistemas de distribuição de energia e sua automação, com destaque ao funcionamento de um sistema de recomposição automática. Além disso, foram descritos os conceitos básicos de uma rede de comunicação e das tecnologias utilizadas no trabalho.

Durante a execução do projeto ficou evidenciada a importância do planejamento de uma rede de comunicação que possa atender a todas as características demandados por um sistema SH e como o avanço de soluções *Smart Grid* estão aproximando cada vez mais as áreas da Tecnologia da Informação e da Engenharia Elétrica.

Notou-se também o impacto de uma ferramenta de gerência de rede na manutenção de uma rede de comunicação ampla e complexa, principalmente quando esta requer um alto grau de disponibilidade, como é o caso da rede descrita neste trabalho.

Como trabalhos futuros é possível considerar a ampliação da rede para atender novos trechos de alimentadores, melhorias no sistema de gerenciamento, adicionando novas informações e funcionalidades, além da implantação de projetos SH em outros municípios do estado que possam demandar tal solução, como Imperatriz e Timon.

8 REFERÊNCIAS

ABRADEE. **A distribuição de energia**. Disponivel em: <http://www.abradee.com.br/setor-de-distribuicao/a-distribuicao-de-energia>. Acesso em: 02 de março de 2016.

ABREU, Y. V. D. **A Reestruturação do setor elétrico brasileiro: Questões e perspectivas**. São Paulo: USP, 1999. 184 p.

ANEEL. **Indicadores Coletivos de Continuidade (DEC e FEC).** Disponivel em: <http://www.aneel.gov.br/indicadores-coletivos-de-continuidade>. Acesso em: 15 de maço de 2016.

AZEVEDO, F. A. **Otimização de Rede de Distribuição de Energia Elétrica Subterrânea Reticulada através de Algoritmos Genéticos**. Universidade Federal do Paraná. Curitiba, p. 140. 2010.

CERF, V.; KAHN, V. **A Protocol for Packet Network**. IEEE Trans on Comm., v. Vol. Com-22, 1974.

CLARKE, G.; REYNDERS, D. **Pratical Modern SCADA Protocol**. Mumbai: Elsevier, 2004. 66-164 p.

DNP GROUP USERS. **Distributed Network Protocol**. Disponivel em: <http://www.dnp.org.>. Acesso em: 28 de março de 2016.

DUARTE, D. P. **Automação como recurso de planejamento de redes de distribuição de energia elétrica**. Universidade de São Paulo. São Paulo, p. 127. 2008.

ELIPSE. **Elipse Power**. Disponivel em: <http://www.elipse.com.br/port/power.aspx>. Acesso em: 19 de março de 2016

FALCÃO, D. **Integração de Tecnologias para Viabilização da Smart Grid**. Anais do III Simpósio Brasileiro de Sistemas Elétricos (SBSE). 127 f. Belém. 2010.

FERREIRA, F. A. L. F. **Metodologia para reconfiguração de redes de distribuição trifásicas assimétricas e não balanceadas com geração distribuída**. Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre. 2010.

GOMES, D. S. F; MACEDO, F. F.; GUILLIOD, S. M. **Proteção de Sistemas Aéreos de Distribuição**. Rio de Janeiro: Editora Campus / Eletrobrás, 1982.

HARRINGTON, D.; PRESUHN, R.; WIJNEN, B. **RFC: 3411: An Architecture for Describing Simple Network Management Protocol (SNMP)**. Management Frameworks. IETF, 2002.

HE, Y.; SODER, L.; ALLAN, R. N. **Distribution automation: impact of communication system on reliability of automatic control**. Power Tech Proceedings. Porto: IEEE. 2001.

JARDINI, J. A. **Sistemas digitais para automação da geração, transmissão e distribuição de energia elétrica**. São Paulo: FCA, 1996.

KUROSE, J. F. E. R. K. W. **Redes de Computadores e Internet – Uma abordagem Top-Down**. 3ª. ed. Ed. Pearson, 2000.

MENDES, M. F. **Proposta de Metodologia e de Modelo para Modernizações de Sistemas de Automações de Unidades Geradoras Hidráulicas de Grande Porte**. USP. São Paulo, 2000.

MOURA, C. J. D. S. **Estudo para implantação de um sistema de recomposição automática para a rede de distribuição do campus PICI**. p. 77. Universidade Federal do Ceará. Fortaleza, 2011.

OHARA, A. T. **Sistema de Recomposição Automática de Redes de Distribuição – A aplicação do Conceito de Self-Healing**. Seminário Internacional sobre –Smart-Grid em Sistema de Distribuição de Transmissão de Energia Elétrica. Belo Horizonte, 2009.

PENIN, A. R. **Sistemas SCADA. 3ª ed.** MARCOMBO. Barcelona, 2012.

PERLMAN, R. **An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN**. ACM SIGCOMM Computer Communication Review 15. 44-53.

POSTEL, J. **RFC: 768: User Datagram Protocol**. IETF, 1980.

SALES, R. **Estudo comparativo de soluções tecnológicas para implementação de Self-Healing como apoio à tomada de decisão na implantação da Rede Elétrica de Média Tensão da CEMAR**. São Luís - MA. 2014.

SANTOS, M. D. M. **Redes Elétricas Inteligentes:** Contexto nacional. Centro de Gestão e Estudos Estratégicos. Brasília, 2012.

SOUSA, L. B. D. **Redes de Computadores – Dados, Voz e Imagem**. 7ª. ed. Editora Érica, 2004.

STASZESKY, D. M. . C. D. . B. C. Advanced Feeder Automation is Here. **IEEE Power & Energy Magazine**, 2005.

TANEMBAUM, A. **Computer Networks**. 3º. ed. Prentice Hall. Amsterdã, 1996.