TRABALHO DE CONCLUSÃO DE CURSO

Desenvolvimento de uma solução integrada de monitoramento para gerência de instalações elétricas de infraestruturas de redes, Data Centers e Smart Grids

Lucas Coelho de Almeida

Brasília, junho de 2019

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO DE CONCLUSÃO DE CURSO

Desenvolvimento de uma solução integrada de monitoramento para gerência de instalações elétricas de infraestruturas de redes, Data Centers e Smart Grids

Lucas Coelho de Almeida

Trabalho de Conclusão de Curso submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Rafael Timóteo de Sousa Jr, Ph.D, FT/UnB _____
Orientador

Prof. Kleber Melo e Silva, Ph.D, FT/UnB _____
Examinador interno

Prof. Alexandre Nery Solon, Ph.D, FT/UnB _____
Examinador interno

FICHA CATALOGRÁFICA

ALMEIDA, LUCAS
Desenvolvimento de uma solução integrada de monitoramento para gerência de instalações elétricas de infraestruturas de redes,Data Centers e Smart Grids [Distrito Federal] 2019.
xvi, 95 p., 210 x 297 mm (ENE/FT/UnB, Engenheiro, Engenharia Elétrica, 2019).
Trabalho de Conclusão de Curso - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Monitoramento	2. SNMP
3. Consumo	4. Energia Eletrica
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

ALMEIDA, L.C. (2019). *Desenvolvimento de uma solução integrada de monitoramento para gerência de instalações elétricas de infraestruturas de redes,Data Centers e Smart Grids*. Trabalho de Conclusão de Curso, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 95 p.

CESSÃO DE DIREITOS

AUTOR: Lucas Coelho de Almeida
TÍTULO: Desenvolvimento de uma solução integrada de monitoramento para gerência de instalações elétricas de infraestruturas de redes,Data Centers e Smart Grids.
GRAU: Engenheiro de Redes de Comunicação ANO: 2019

É concedida à Universidade de Brasília permissão para reproduzir cópias desto Trabalho de Conclusão de Curso e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Os autores reservam outros direitos de publicação e nenhuma parte desso Trabalho de Conclusão de Curso pode ser reproduzida sem autorização por escrito dos autores.

Lucas Coelho de Almeida
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

Agradeço a Deus pela maravilhosa e inexplicável sequência de coincidências que me trouxeram até aqui. À minha família, que me inspira a buscar o impossível sem me cansar. Aos meus professores e amigos, que me possibilitam saber mais hoje que ontem, e ter esperança de saber mais amanhã do que sei hoje.

RESUMO

As infraestruturas de comunicações e dados vêm passando por evoluções das mais diversas, atingindo desde a capacidade de processamento, passando pela larga cobertura geográfica, até chegar à resiliência e redundância exigidas nas aplicações atuais. No entanto, problemas físicos, como a geração excessiva de calor e o crescente consumo de energia continuam a se tornar cada vez mais presentes. Inspirando-se na evolução do conceito de redes elétricas inteligentes, ou "*Smart grids*", abordar-se-á a implementação de um sistema integrado de monitoramento e medição de variáveis de consumo de energia elétrica usando hardware e bibliotecas de software aberto, e apoiando-se em padrões extensivamente adotados pela indústria ao longo de mais de 30 anos, tais como Ethernet (IEEE 802.3) e o protocolo SNMP (RFC 1157). Desenvolvido para atuar de forma segura, com baixo custo e altamente integrável com outras ferramentas e sistemas, seu uso é o primeiro passo na direção da gerência completa de uma infraestrutura física de Tecnologia da Informação e Comunicação. O resultado obtido ao fim dos trabalhos foi um padrão de projeto capaz de medir corrente elétrica de forma não invasiva e disponibilizar esses dados via rede, seja numa infraestrutura local, seja em uma arquitetura distribuída, atendendo, portanto, desde pequenos data centers locais até enormes projetos distribuídos como as "*Smart grids*".

SUMÁRIO

1 INTRODUÇÃO 1
1.1 CONTEXTUALIZAÇÃO 1
1.2 DEFINIÇÃO E RELEVÂNCIA DO PROBLEMA 1
1.3 PROPOSTA DE SOLUÇÃO 3
1.4 ORGANIZAÇÃO DO TRABALHO 4

2 FUNDAMENTAÇÃO TEÓRICA E ESTADO DA ARTE 5
2.1 DATA CENTERS E INFRAESTRUTURAS DE COMUNICAÇÃO 5
2.2 *Smart grids* 10
2.3 IOT E INDÚSTRIA 4.0 14
2.4 GERÊNCIA DE REDES E AS CLASSES DE SOFTWARES NMS, APM E DCIM 17
2.5 BASES DE DADOS, MIB E SMI 25
2.6 ÁRVORES DE NOMES 27
2.7 PROTOCOLO SNMP 30
2.8 MICROCONTROLADORES 42
2.9 O USO DE TRANSFORMADORES DE CORRENTE NA MEDIÇÃO NÃO-INVASIVA DE VARIÁVEIS EM CIRCUITOS ELÉTRICOS 48

3 PROPOSTA DE PROJETO 51
3.1 PROJETO DO SISTEMA 51
3.1.1 REQUISITOS E ESPECIFICAÇÕES 51
3.1.2 CONCEITOS APLICADOS E MONTAGEM - HARDWARE 55
3.1.3 CONCEITOS APLICADOS E DESENVOLVIMENTO - SOFTWARE EMBARCADO 59
3.2 METODOLOGIA DE APLICAÇÃO DO PROJETO 67
3.2.1 INFRAESTRUTURAS COBERTAS POR REDES LOCAIS 67
3.2.2 INFRAESTRUTURAS MASSIVAS DISTRIBUÍDAS GEOGRAFICAMENTE 68

4 RESULTADOS OBTIDOS E DISCUSSÕES 71
4.1 MONTAGEM DO SISTEMA 71
4.2 APLICAÇÃO DO SISTEMA 77

5 CONCLUSÃO 87
5.1 TRABALHOS FUTUROS 87

REFERÊNCIAS BIBLIOGRÁFICAS 90

LISTA DE FIGURAS

2.1 Um dos primeiro computadores funcionando à base de transistores, o TX-0, desenvolvido no MIT (Computer History Museum,1960) [1]. 6
2.2 Imagem de um dos corredores de um dos data centers da empresa Equinix em Santana de Parnaíba, estado de São Paulo (Datacenter Dynamics,2019) [2]..... 7
2.3 Representação da extensão da rede da empresa Telecomunicações Brasileiras (TELEBRAS,2019) [3]..... 8
2.4 Ilustração de um possível esquema de distribuição de rede de uma empresa de telecomunicações e dentro dos prédios/clientes. 9
2.5 Estados atingidos pelo blecaute de 21 de janeiro de 2002 (Folha de SP,2002) [4].... 12
2.6 Ilustração mostrando as três fases da infraestrutura da rede elétrica e o cálculo das perdas estimadas para o exemplo (ANEEL,2019) [5]. 13
2.7 Imagem explicando o processo básico e os benefícios da microgeração para o caso da energia solar (CERNE,2018) [6]. 14
2.8 Ilustração de um processo de fabricação alinhado com os conceitos da Indústria 4.0 (3D Printing Industry,2016) [7]. 17
2.9 Apresentação das cinco camadas da pilha TCP/IP e das sete camadas do modelo OSI/ISO. 21
2.10 Arquitetura e conversação básica de um esquema de gerência baseado no framework SNMP [8]. 24
2.11 Detalhe da árvore de OID's partindo do nó da ISO até uma parte do ramo da MIB-II (J. C. S. Freitas,2000) [9]..... 26
2.12 Árvore Filogenética da Biologia (Wikipédia,2008) [10]. 28
2.13 Topo da hierarquia de nomes da árvore de objetos SMI(O'Reilly and Associates,2002) [11]. 29
2.14 Exemplo de estrutura que satisfaz os critérios de uma árvore AVL (P. Feofiloff,2018) [12]. 31
2.15 Estrutura básica de um segmento UDP (K. W. Ross e J. F. Kurose,2000) [13]..... 33
2.16 Campos e estrutura geral de uma PDU dos tipos "get" ou "set" do SNMPv1 (C. M. Kozierok,2005) [14]. 35
2.17 Campos e estrutura geral de uma PDU dos tipos 'trap" do SNMPv1 (C. M. Kozierok,2005) [15]..... 37
2.18 Esquema geral do funcionamento do protocolo SNMPv1 (CooperaTI,2019) [16]. .. 38
2.19 Resumo ilustrando todos os campos e tipos de mensagens do SNMPv1 (CooperaTI,2019) [16]. 38
2.20 Ilustração do funcionamento de um NAT (D. A. Santos e L. Silva,2019) [17]. 39
2.21 Resumo do funcionamento de um gerente segundo o SNMPv3 (H. Fassi,2008) [18]. 40
2.22 Resumo do funcionamento de um agente segundo o SNMPv3 (H. Fassi,2008) [18]. 41

2.23 Vários exemplos de válvulas termiônicas, os dispositivos que faziam o papel dos transistores (S. Riepl,2008) [19]. 42
2.24 À esquerda, exemplo de EPROM, memória que só podia ser apagada com o uso de luz ultravioleta; à direita, exemplo de EEPROM, memória apagável eletricamente que revolucionou a Eletrônica (Tech Difference,2019) [20]. 44
2.25 Foto de um dos primeiros microcontroladores amplamente distribuídos, o Intel P8051 (K. Lanzet,2008) [21]. 44
2.26 Estrutura básica que representa a maioria dos microcontroladores disponíveis (CircuitsToday,2018) [22]. 46
2.27 Diferença entre um processador e um microcontrolador (CircuitsToday,2018) [22]. 47
2.28 Ilustração da Lei de Faraday. 49
2.29 Exemplo de funcionamento de um transformador de corrente. 49

3.1 Esquemático e explicação do circuito auxiliar para a interface entre a placa Arduino Mega e o sensor "SCT-013 100A:50mA"(Open Energy Monitor,2019) [23].. 57
3.2 Diagrama do projeto de hardware completo. 58
3.3 Árvore de nomes da ISO (no canto inferior direito, encontra-se o protocolo SNMP). 62
3.4 Detalhe das especificações de tipos definidos pela ISO "ASN.1". 62
3.5 Detalhe da topologia típica do protocolo SNMP, e circulado em vermelho, o papel assumido pelo sistema proposto nessa estrutura. 62
3.6 Árvore de nomes definidos e padronizados para o sistema proposto..... 64
3.7 Fluxograma proposto para o funcionamento do software embarcado do projeto. 65
3.8 Exemplo de aplicações do Zabbix Proxy para resolver o já citado problema do NAT (Zabbix SIA,2019) [24]. 70

4.1 Visão em perspectiva da montagem. 72
4.2 Visão em perspectiva dos conectores e as ligações internas ao enclausuramento. 72
4.3 Visão aérea da montagem..... 73
4.4 Visão frontal dos conectores de comunicação e alimentação do sistema. 73
4.5 Detalhe do sistema encapsulado e fechado. 74
4.6 Detalhe do transdutor do sensor de corrente não invasivo. 74
4.7 Detalhe da montagem do circuito da figura 5.3 dentro do conector XLR3 macho do sensor. 75
4.8 Visão do sensor conectorizado e pronto para uso. 75
4.9 Visão do sistema montado e pronto para uso. 76
4.10 Visão geral do quadro elétrico no qual se encontra o circuito a ser medido. 77
4.11 Visão do sistema instalado e pronto para testes (ao lado, notebook com o software gerente Zabbix em funcionamento). 78
4.12 Visão dos sensores conectados aos condutores das fases e neutro do circuito trifásico de um sistema de refrigeração. 79
4.13 Detalhe da configuração do sistema com um endereço IPv4 fixo via interface serial. 80

4.14 Detalhe da criação de ”host” no software Zabbix [25] para monitoramento do sistema. 80
4.15 Detalhe da criação de item de monitoramento usando o protocolo SNMPv1 [26] e a OID correspondente para obter a corrente da fase 1 sendo medida pela sistema através do sensor 0. 81
4.16 Gráfico sendo plotado com os valores de corrente total medida pelo sistema. 81
4.17 Página web com painel (”dashboard”) para acompanhamento das leituras dos sensores..... 82
4.18 Gráfico conjunto das correntes de todos as três fases, terra e corrente total. 82
4.19 Detalhe da lista das últimas variáveis a serem requisitadas pelo gerente ao sistema. 82
4.20 Gráfico do consumo aparente de energia por fase e total. Observa-se que esse valor é atualizado apenas a cada passagem completa de uma (1) hora. 83
4.21 Comparação entre a leitura do alicate amperímetro e do sistema para a fase 2. O alicate media 3.76A, enquanto o sistema, 3.56A, uma diferença de apenas 5%. 83
4.22 Outra comparação entre a leitura do alicate amperímetro e do sistema, agora para a fase 3. O alicate media 8.68A, enquanto o sistema, 8.43A, uma diferença de menos de 3%..... 83

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

Os antigos ambientes de Centros de Processamento de Dados, com interação de poucos usuários especializados via programas de terminal e grandes computadores, que ocupavam vários metros quadrados dos prédios empresariais acabaram. Em vez disso, a crescente demanda por aplicações de mídia de alta qualidade em transmissões de dados de tempo real em altas velocidades através de redes de longas distâncias (como os portais de vídeos na internet), a criticidade de aplicações de negócios na casa dos centésimos de segundo (como as bolsas de valores e os pagamentos através de cartão), e até mesmo as comunicações dos meios de transportes (como as malhas ferroviárias e os aviões), causaram um crescimento sem precedentes da complexidade e do raio de influência das infraestruturas de comunicação. Hoje, é possível realizar ligações a qualquer hora do dia para qualquer lugar do mundo, e consultar bancos de notícias das menores cidades dos cantos mais remotos do planeta. As distâncias diminuíram, as exigências aumentaram, e seguindo a tendência, as visões gerenciais por trás de todos esses aparatos de engenharia e eletrônica tiveram de buscar novas abordagens. Essa renovação dos processos de gestão e controle é tão intensa, que até mesmo o eterno mundo ”analógico” das redes elétricas viu o futuro chegar por meio de sistemas de monitoramento, automação e controle, supervisão visual de sites espalhados pelo mundo, entre outros, tudo baseado na integração com a Tecnologia da Informação e Comunicação - TIC.

1.2 DEFINIÇÃO E RELEVÂNCIA DO PROBLEMA

O mundo de alguns anos atrás aceitava um gestor que não sabe exatamente quanto custa a operação de sua infraestrutura de Tecnologia da Informação e Comunicação (TIC), entretanto, hoje, um administrador que não saiba justificar sequer o custo de uma única hora do seu data center (e que nem entenda o valor dessa informação) provavelmente estará sendo cotado para ser substituído em breve. Mais que isso, se o profissional não souber os impactos dos sistemas que lhe foram imputados por responsabilidade, pode até ser punido, seja por exceder o consumo de energia acordado com a fornecedora, e portanto, recebendo multas, seja por poluir o meio ambiente que o cerca, seja por infringir os direitos de conforto dos vizinhos (como exceder os níveis sonoros aceitáveis), entres outros. Dentro desse conjunto de cenários e preocupações, todos os gestores são relativamente novos no assunto, afinal, a escassez de energia, água, o aumento das temperaturas, a defesa do ambiente, todos são temas atuais. Uma busca avançada em qualquer

base de dados por artigos e notícias sobre o assunto mostra que o consentimento sobre a importância desses campos tomou força apenas cerca de 20 a 25 anos atrás. O próprio ”Protocolo de Kyoto” é recente, assinado em 1997, sobre os gases de efeito estufa (em grande parte gerados através da queima de combustíveis fósseis para geração de energia), e o "Protocolo de Montreal", o qual trouxe a proibição de vários gases usados corriqueiramente na indústria, nem ao menos terminaram seus ciclos, muitos dos compromissos assumidos pelos países ainda estão por acontecer. Entretanto, mais que incentivar o cuidado pelo ambiente, a sustentabilidade, hoje mais do que nunca, se tornou possibilidade de lucro indireto. Segundo a Ponemon Institute (2016) [27], citada pela empresa Datacenter Dynamics (2016) [28], "os custos operacionais e de energia representam 80% ou mais das despesas anuais do data center", logo, reduzir o consumo de energia reduz a fatia dispendida do orçamento para operações. Ainda além desse fato, trabalhos já surgem alertando sobre o aumento massivo de demanda por energia para processamento em várias partes do mundo. Koomey (2008) [29] diz que a taxa de crescimento da demanda energética de data centers no mundo entre os anos 2000 e 2005 foi de cerca de 16,7% ao ano, e em outro artigo, Koomey (2011) [30] afirma que o crescimento do consumo de energia elétrica em data centers cresceu aproximadamente 78% entre 2005 e 2010. Mesmo olhando mercados de forma isolada, é possível obter os mesmos dados de que o crescimento do uso de recursos energéticos nesse setor é muito grande: segundo Hintemann (2015) [31], a Alemanha é o maior mercado no ramo de data centers da Europa, e apesar de todo investimento em eficiência, layouts ”verdes” e operações sustentáveis, a quantidade de energia consumida por esses gigantes de processamento no país cresceu mais de 14% entre 2010 e 2015. Isso representa um aumento de 1.5 bilhões de kWh consumidos a mais por ano exclusivamente com processamento. A importância desse tema é tamanha que o D.O.E (US Department of Energy - Departamento de Energia dos Estados Unidos) criou uma sessão específica para os data centers, o CoE (Center of Expertise for Energy Efficiency in Data Centers - Centro de Perícia para Eficiência Energética em Data Centers) [32]. O projeto visa fornecer treinamentos, análises, suporte, planejamento e ferramentas para incentivar a redução de consumo de energia em data centers de agências federais e outras organizações governamentais. A última edição do relatório periodicamente divulgado pelo D.O.E, "United States Data Center Energy Usage Report" [33], explana que em 2014, aproximadamente 1.8% do consumo total de energia elétrica dos Estados Unidos era de data centers, e que a taxa de crescimento dessa fatia é muito maior que o restante dos setores.

Sem sombra de dúvida, se antes a preocupação principal dos gestores de TIC era a velocidade e disponibilidade da rede, hoje o dispêndio de energia já está entre as primeiras preocupações. Porém, deve-se lembrar ainda que, num mundo globalizado, órgãos governamentais e empresas multinacionais têm infraestruturas espalhadas geograficamente, e em países de proporções continentais (como o Brasil), são vários os exemplos: procuradorias, agências de controle e fiscalização, tribunais, concessionárias de energia, empresas de telecomunicações, empresas de petróleo e gás... A complexidade dessas instalações acaba se ligando intimamente a outro problema parecido, contudo, ainda maior: a implantação bem sucedida de *Smart grids* de países continentais como o Brasil. Implementar, com sucesso, redes elétricas inteligentes em situações de tamanha

complexidade (milhares de quilômetros quadrados e vários fusos horários, por exemplo) tem se mostrado um assunto amplo e desafiador. A junção, portanto, de todos os cenários abordados converge para o problema a ser enfrentado neste trabalho: como aplicar e implementar conceitos de gerência (incluindo monitoramento) em instalações de infraestrutura de modo a atender desde pequenos data centers, passando por grandes empresas de infraestrutura distribuída e, por fim, aos enormes projetos de *Smart grids*?

1.3 PROPOSTA DE SOLUÇÃO

Sabendo do peso desse tema, o projeto proposto tenta preencher um vazio em quase todas as instalações de TIC atuais no Brasil (e abrir caminho para a evolução das *Smart grids*): o monitoramento de consumo de energia. Apesar de existirem diversos protocolos para IoT (Internet of Things - Internet das Coisas), tecnologias de transmissão wireless e padrões de comunicação serial largamente usados na indústria, é fato que o ambiente do data center médio demorará a incorporar tais tecnologias, afinal, na maioria dos casos, o ROI (Return of Investment - Retorno de Investimento) de tecnologias de eficiência e gerência são desconhecidos e/ou considerados excessivamente baixos pelos gestores, seja por falta de informação, seja por falta de capacitação, seja por falta de estímulos no setor. É certo, porém, que outras tecnologias já largamente aceitas e vendidas no ramo, como SNMP (RFC 1157 [26]) e Ethernet (o famoso padrão IEEE 802.3 [34]), têm fácil adesão, já que boa parte dos equipamentos são monitorados usando esses padrões, logo, não há impacto para implantação e o custo do sistema fica extremamente baixo. Decorre desse projeto que todos os conceitos e motivações abordados se relacionam intimamente com as dificuldades enfrentadas no desenvolvimento de projetos massivos de gerência para redes elétricas inteligentes, podendo, de forma descomplicada, serem reutilizados para tal fim.

Portanto, o objetivo geral do projeto é percorrer os detalhes do desenvolvimento e implementação de um sistema de monitoramento de consumo de energia baseado nesses padrões e usando hardware e software abertos, e também reutilizando o conhecimento de outros projetos e ferramentas importantes e abertas para a comunidade em geral (como a aplicação NMS Zabbix e o projeto Open Energy Monitor). Com esse padrão de projeto, espera-se que os gestores desses ambientes possam absorver mais rapidamente as práticas e o interesse geral pela eficiência energética, além de melhorar seus próprios processos de gerência de custos e investimentos. Em suma, consiste de dispositivos microcontrolados com sensores não-invasivos de corrente programados com MIB's específicas para as variáveis de consumo de energia elétrica usando o protocolo SNMP em fluxos de funcionamento ligeiramente diferentes dos inicialmente projetados para o protocolo, de forma a prover monitoramento tanto para aplicações de redes locais quanto para outras distribuições geográficas diversas. Além disso, boa parte dos grandes órgãos públicos, empresas públicas e multinacionais apresentam infraestruturas distribuídas pelo território, logo, resolver a questão

da gerência desses ambientes implica diretamente em abrir caminho para a solução de um outro tópico de relevância crescente: a gerência nas "*Smart grids*", ou redes elétricas inteligentes.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho está estruturado em cinco capítulos. O primeiro capítulo aborda a contextualização do assunto, a identificação do problema, sua abrangência e apresenta brevemente a solução proposta. O segundo capítulo aborda os conceitos teóricos fundamentais para o entendimento completo das lógicas de projeto usadas, tais como gerência em redes de comunicação, protocolo SNMP, soluções de aplicações de gerência, microcontroladores, ferramentas, projetos abertos à comunidade, entre outros. O terceiro capítulo especifica a proposta de solução unindo conceitos largamente usados na indústria e validados por mais 30 anos de utilização. O quarto capítulo apresenta os resultados da implementação em campo do sistema e discute possíveis arquiteturas para o caso de instalações com pontos de interesse espalhados geograficamente, como é o caso das "*Smart grids*", ou redes elétricas inteligentes. O quinto capítulo discute o futuro das infraestruturas inteligentes e como as lógicas de projeto e padrões estabelecidos neste trabalho podem contribuir para a segurança, gerência e eficiência dessas instalações.

2 FUNDAMENTAÇÃO TEÓRICA E ESTADO DA ARTE

A seguir, abordar-se-á os principais conceitos necessários para o entendimento completo do projeto proposto e suas implicações. As exposições começam por definir, de forma rasa, como devem ser entendidos os data centers e as infraestruturas distribuídas de comunicação. Em seguida, as redes elétricas inteligentes, ou *Smart grids*, são brevemente definidas e relacionadas com as infraestruturas e serviços de comunicação atuais. A título de inspiração para os conceitos e objetivos do projeto, são brevemente explanados os paradigmas por trás dos termos ”IoT” e ”Indústria 4.0”. Logo após, passa-se à explicação dos conceitos chave do projeto, embasados nas soluções de gerência de redes, bases e estruturas de dados (MIB's e SMI) e as estruturas de árvores de nomes (como a da ISO). Em seguida, os conceitos globais são explicados, como o protocolo SNMP, o uso de transformadores de corrente na medição não-invasiva de variáveis em circuitos elétricos, e por fim, uma breve introdução aos microcontroladores e como eles podem ser úteis na resolução dos problemas de gerência dessas instalações.

2.1 DATA CENTERS E INFRAESTRUTURAS DE COMUNICAÇÃO

Este tópico percorre de forma breve a história dos data centers, ilustra suas relações com infraestruturas distribuídas e identifica as vantagens e necessidades de gerência de infraestrutura nesses tipos de instalações.

A história dos grandes data centers atuais não é nova, na verdade, desde os anos de 1960, já explodiam pelo mundo ideias sobre reunir dados e tecnologias de comunicação num único ambiente para fácil acesso, desenvolvimento e difusão. Em 1965, cientistas dos Estados Unidos recomendaram que fosse criado um plano para construção de um data center nacional (chamado ”National Data Center Plan”), o qual armazenaria dados da população norte-americana e permitira grandes avanços sociais. Na época, o projeto foi abandonado por preocupações com a privacidade dos cidadãos, porém, influenciado por iniciativas como essa, ano após ano, o mundo passaria pelas maiores evoluções no mundo das tecnologias de comunicação e informação. Mas como, de fato, começou essa centralização de dados em centros de processamento, os famosos CPD's (Centro de Processamento de Dados)? A resposta mais precisa se apoia no surgimento dos computadores. O termo ”computador” não referenciava, originalmente, o aparelho, mas sim, a pessoa com habilidade para resolver problemas matemáticos e contas. Entretanto, a evolução dessas máquinas tornou as atividades computacionais tão rápidas e descomplicadas, que não restou trabalho para os profissionais computadores de antigamente. Sendo uma aclamada criação conjunta da humanidade, influenciada pelas teorias de vários cientistas, inventores e estudiosos, tais como John von Neumann, Alan Mathison Turing e Charles Babbage, o computador acabou se inserindo em quase

todas as tarefas e trabalhos. A figura 2.1 mostra um dos primeiros computadores funcionando à base de transistores, sistemas que espalharam-se rapidamente pelo mundo.

Figura 2.1: Um dos primeiro computadores funcionando à base de transistores, o TX-0, desenvolvido no MIT (Computer History Museum,1960) [1].

Pouco depois de o computador virar celebridade no mundo tecnológico da época, com a criação da ARPANET (Advanced Research Projects Agency Network - Rede da Agência de Projetos de Pesquisa Avançada) em 1969, para interligar universidades norte-americanas, e a necessidade crescente de comunicação e envio de dados entre as pessoas, a Internet iniciou suas aparições ao mundo. No começo, porém, os computadores eram enormes máquinas, nas quais o técnico tinha que adentrar fisicamente para efetuar qualquer reparo, e estas geravam calor e ruído sem precedentes. Por essas características, ficavam em salas isoladas do restante dos funcionários, e alocados ao redor destas grandes máquinas, os profissionais que prestavam manutenção e desenvolviam programas. O recorrente risco de incêndios e o aumento da geração de calor com a evolução da potência dos computadores levou à criação de salas próprias e infraestruturadas para esses aparelhos. Era apenas questão de tempo até que essas máquinas ficassem menores, mais robustas, e surgissem diversas novas tecnologias, exigindo cabos e conexões mais precisos, alimentação confiável, sistemas contra incêndios, refrigeração e energia ininterruptas, entre outros. Logo, o coração das grandes empresas estaria formado e mantido continuamente por computadores, e as necessidades de redundância, disponibilidade e velocidade ficariam cada vez mais evidentes, nascendo de forma definitiva a importância do que seria chamado ”data center”, ou ”centro de dados”.

Figura 2.2: Imagem de um dos corredores de um dos data centers da empresa Equinix em Santana de Parnaíba, estado de São Paulo (Datacenter Dynamics,2019) [2].

A imagem 2.2 mostra um data center moderno de grande porte. Esse tipo de instalação frequentemente se relaciona com infraestruturas distribuídas, sendo esse um ponto crucial para este trabalho e uma realidade para diversas empresas e órgãos governamentais. Ocorre que, com a evolução das tecnologias de comunicação, padrões para longas distâncias foram implantados com sucesso, permitindo às organizações estruturar sua operação em amplas áreas geográficas. Entretanto, essas tecnologias dependem de pontos físicos de conexão, roteamento de dados, repetição de sinal, entre outros, pontos esses que não necessariamente estarão em um prédio da empresa, mas talvez no meio do mar, ou ao lado de uma rodovia, embaixo de uma ponte, próximo a um rio, entre outros. Não são necessariamente *data centers*, mas sim, salas de redes, por terem objetivos puramente voltados à manutenção do fornecimento de acesso à rede e difusão dessa. Para empresas provedoras de serviços de telecomunicações, por exemplo, o número de salas de rede espalhadas nos mais diversos locais pode chegar facilmente à casa dos milhares, entre pontos de interconexão própria da empresa e PoP's (Point of Presence - Ponto de Presença, locais onde empresas provedoras proveem conexão para os clientes). A imagem 2.3 mostra um exemplo deste cenário, no qual a extensão da rede da empresa Telebras (Telecomunicações Brasileiras) atinge cerca de 26 mil quilômetros de extensão. Portanto, todo um novo conceito de gerência de infraestrutura e logística foi aperfeiçoado para conseguir atender aos requisitos de manter tamanhas operações, muitas vezes da ordem de milhares de quilômetros de extensão, passando por terra, água (doce e salgada), dutos subterrâneos, morros, vales e até montanhas. Tomando por base uma empresa provedora de serviços de comunicação, percorrer-se-á a estrutura básica mantida em sua operação e de uma empresa cliente, alocada num prédio (topologia essa representada na figura 2.4). Essa estrutura é quase a mesma de uma organização estabelecida num grande campus, ou seja, em um conjunto de prédios os quais compartilham infraestrutura básica de energia, água, rede e vias de acesso, tal qual numa grande universidade. Em primeiro

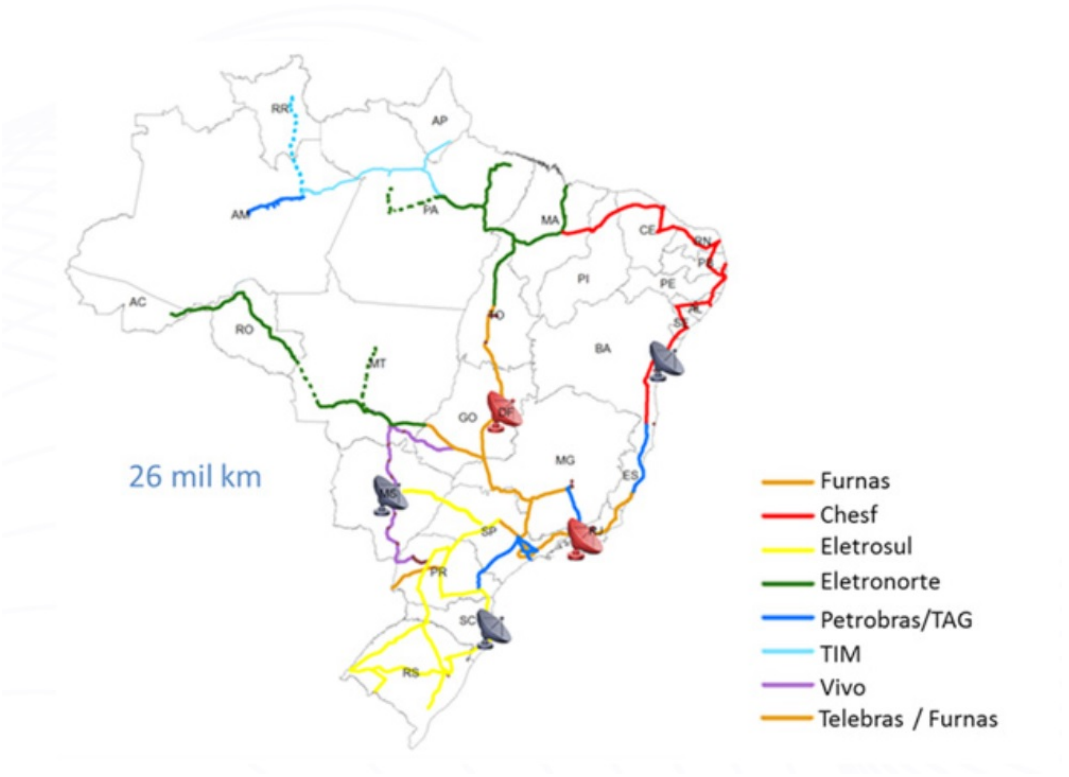

Figura 2.3: Representação da extensão da rede da empresa Telecomunicações Brasileiras (TELEBRAS,2019) [3].

lugar, estarão seus data centers. São ambientes complexos, com diversos equipamentos (para armazenamento, sustentação de serviços em rede, gerência de protocolos e métricas, roteamento de dados, entre outros), os quais constituem o coração da rede e dos serviços providos. Desses data centers, sairão conexões das mais diversas (por fibra óptica e/ou antenas, por exemplo) para várias salas de redes espalhadas geograficamente. Nessas salas, duas situações podem ocorrer: existe outra conexão física para uma sala em outra localidade, ou existirão várias conexões para vários prédios e/ou construções. A organização residente em cada prédio/cliente também terá sua própria infraestrutura de cabeamento: cada prédio/construção terá salas onde esses links entram e são distribuídos para o restante do prédio. Ainda dentro do prédio, da sala de entrada do link sairá o cabeamento vertical para os demais andares, e em cada andar existirá ao menos uma sala (ou armário) de rede, dos quais o cabeamento horizontal se origina e distribui o acesso pelo andar (ou parte dele, no caso de edificações muito amplas com várias salas/armários de rede por andar). As normas internacionais EIA/TIA-568B (Telecommunications Industry Association - Associação de Indústrias de Telecomunicação) e ISO/IEC 11801 (International Electrotechnical Commission - Comissão Internacional Eletrotécnica) definem parte dessa arquitetura para a situação da organização estruturada em campus (situação intermediária em complexidade em relação a uma empresa provedora de serviços de telecomunicações numa região). Por fim, qual a dificuldade no monitoramento e gestão desses ambientes? Por se tratar de um emaranhado de tecnologias e engenharias, envolvendo refrigeração, construções e adaptações físicas, dutos, passagens de cabos, servidores, logística, gestão de contas e energia, gestão de ativo, instalações elétricas de média e baixa tensão, provisão de insumos, entre outros, operar essas infraestruturas

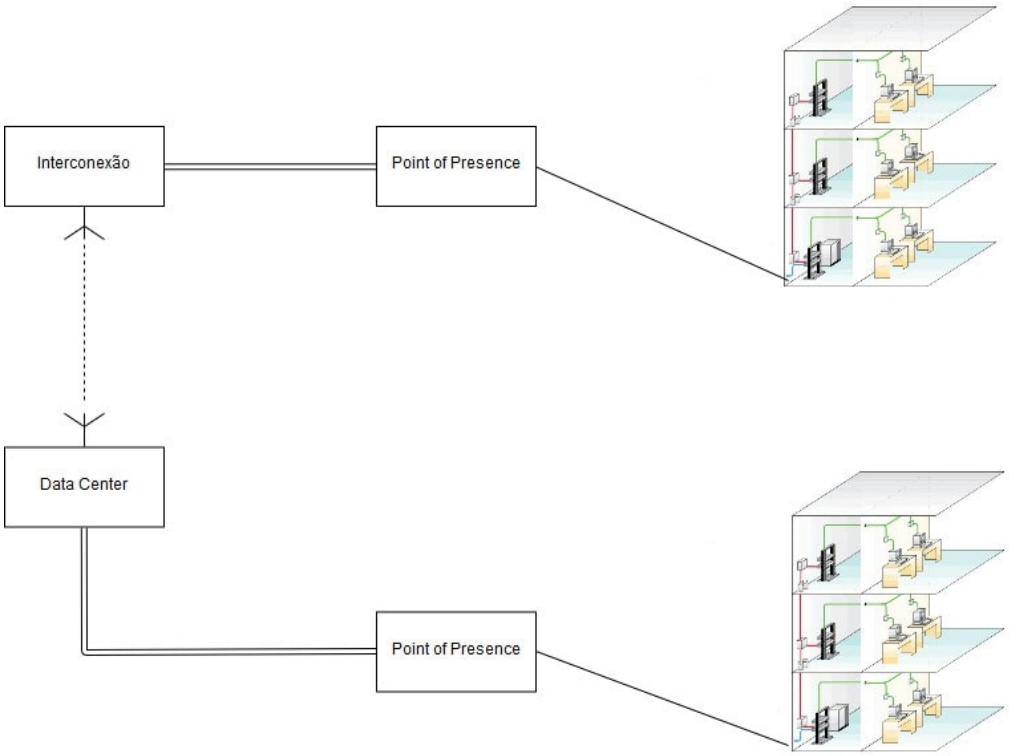

Figura 2.4: Ilustração de um possível esquema de distribuição de rede de uma empresa de telecomunicações e dentro dos prédios/clientes.

se torna oneroso. As normas ANSI/TIA-942-A e ANSI/BICSI-002 (Building Industry Consulting Service International - Serviço de Consultoria Internacional das Indústrias de Edificações) são um compilado de boas práticas e conhecimentos acumulados pelos profissionais envolvidos nos projetos e operações de data centers, e são os documentos mais difundidos no setor. A leitura dessas normas mostra que a multidisciplinaridade dificulta a tomada de decisão, pois a aquisição de informações não é tão clara e muitas vezes, nem imediata (some-se às grandes distâncias e dificuldades de acesso em casos de órgãos de expressão nacional para um grande país). Possível solução, a onda crescente de implementações baseadas em IoT (Internet of Things - Internet das Coisas) e Indústria 4.0 atende, também, a essas gigantescas infraestruturas, porém, ainda são tecnologias caras e exigem investimento grande para compra e instalação. Todavia, apesar de os investimentos nessas tecnologias não serem prioridade em muitas organizações, fica claro que o crescimento do consumo de energia do setor de comunicações é insustentável em todo o mundo, conforme referências citadas no Capítulo 1, seção ”Definição e Relevância do Problema”. Portanto, como um setor tão complexo e com impactos tão grandes pode permanecer sem a gestão adequada de infraestrutura física, por exemplo, consumo de energia? Não bastasse o impacto no meio ambiente, a eficiente gestão de contas e energia pode ajudar a identificar gargalos e excessos, como equipamentos desatualizados, aparelhos sem uso otimizado, dispositivos elétricos com falha, sistemas de alimentação ininterrupta ineficientes, uso incorreto de energia nos horários de ponta (momento em que o custo da energia, segundo a concessionária, é mais caro), entre outros. Resolver esses problemas é, de forma rápida e objetiva, economizar orçamento para operação, ou

seja, reduzir custos indiretos.

2.2 *SMART GRIDS*

Este tópico define o que são as *Smart grids*, percorre as principais revoluções normativas do setor elétrico brasileiro e as usa para explicar como as redes elétricas inteligentes contribuem para a operação sustentável da área.

O relatório do Grupo de Trabalho de Redes Elétricas Inteligentes do Ministério de Minas e Energia do Brasil [35] tem uma definição bastante acertada para o termo redes elétricas inteligentes (tradução adaptada do termo popular "*Smart grids*"):

"Existem várias definições para o conceito de redes inteligentes, mas todas convergem para o uso de elementos digitais e de comunicações nas redes que transportam a energia. Esses elementos possibilitam o envio de uma gama de dados e informação para os centros de controle, onde eles são tratados, auxiliando na operação e controle do sistema como um todo."

De fato, o documento fornece definições gerais de grande relevância sobre os conceitos por trás desse tema, abordando as tecnologias e os planos de implantação em território brasileiro. As redes elétricas eram um dos poucos redutos restantes do mundo analógico, e como tal, vivenciava frequentemente as dificuldades de uma operação complexa e cheia de riscos, falhas, margens de erro e perdas de eficiência. Por outro lado, o mundo das comunicações avançou sobremodo, permitindo até mesmo que setores como o de petróleo e mineração usufruíssem de sistemas de medição e controle de ponta, seja a vários metros abaixo do solo, seja a alguns quilômetros de profundidade no mar (em água salgada com densidade variável, note-se). Mas, será que seria possível às concessionárias de energia e ao mundo sustentável continuar seu desenvolvimento sem uma revolução no setor elétrico? Infelizmente não. O consumo de energia no mundo cresce à taxas maiores do que a capacidade de geração, e a escassez de fontes de energia, aliada aos impactos destes, trouxeram força para as fontes renováveis, que invadiram a sociedade e os canais de informação. Contudo, fontes renováveis sofrem de um problema sério: todas tem algum grau de intermitência. Na eólica, os ventos não são sempre fortes, na solar, não se tem luz o dia todo, e a luminância é variável dada a posição no globo e o clima momentâneo, bem como a presença de nuvens. Ainda, a energia gerada através das marés depende de determinadas épocas do ano e dos momentos de alta e baixa, e assim, pode-se citar cada fonte renovável existente. Como, portanto, utilizar com sucesso essas fontes se não existe controle adequado da geração e da intercalação entre esses métodos? Sob outro ponto de vista, a energia elétrica é um recurso cuja oferta deve ser cuidadosamente projetada, evitando quaisquer perdas, além de ser extremamente recomendável que os consumidores tenham conhecimento tanto de seu consumo, quanto de como

diminui-lo. Hoje, nenhum desses conceitos é uma realidade absoluta: os consumidores só tem real ciência de seu consumo ao fim do mês (com as contas), as redes são projetadas com base em levantamentos que rapidamente se tornam obsoletos, as curvas de carga das localidades variam de forma bastante brusca dados os períodos de calor e/ou os momentos de ponta, como logo após o fim da tarde (por volta de 18 às 21 horas no caso da CEB - Companhia Energética de Brasília), e a rede instalada basicamente não muda seu comportamento, revelando, em determinados locais, superdimensionamento, e em outros, subdimensionamento. As indisponibilidades, comumente, têm de ser comunicadas às concessionárias pelos clientes e, adicionalmente, têm sido frequentes os incidentes em subestações, as quais podem por em risco centenas de funcionário e alimentam bairros inteiros de cidades importantes como São Paulo e Brasília (como a explosão numa subestação da CPFL Energia em São Paulo no fim de outubro de 2018 ou o incêndio numa subestação na capital, Brasília, no fim de maio de 2019). Ainda, segundo o mesmo relatório citado, a ANEEL (Agência Nacional de Energia Elétrica) afirma que a perda média nas linhas brasileiras atinge 16%. Será que a Crise do Apagão, sofrida pelo país na segunda metade de 2001 e início de 2002, teria ocorrido se a rede fosse melhor conhecida, planejada, controlada e dimensionada? Dificilmente. A figura 2.5 mostra a extensão dos impactos da crise citada.

As redes elétricas são compostas, basicamente, por três estágios fundamentais: geração, transmissão e distribuição. Primeiramente, a energia é gerada em grandes usinas, depois, transmitida através de longas linhas para os centros consumidores, e por fim, distribuída, através de subestações, para os usuários finais (sejam empresas ou pessoas). A fase da geração sempre foi a mais bem equipada e controlada, haja vista a criticidade e tamanho da operação e maquinário requeridos. A fase da transmissão, hoje, é suficientemente desenvolvida, de forma que as concessionárias conseguem manejar bem as perdas e os dimensionamentos da rede, esforçando-se em outras frentes, como redundância. Porém, é na distribuição onde se verificam os verdadeiros gargalos da rede. Os consumidores não tem informação alguma sobre seu consumo, somente no momento da tarifação, as concessionárias não tem nível adequado de automatização e monitoramento, e nem sequer conhecem a curva de carga da maioria de seus consumidores, além de não conhecer com precisão as perdas e os locais com distribuição mal dimensionada. O trabalho é, na maioria das vezes, reativo, ou seja, são necessárias reclamações e/ou falhas nos consumidores para que as fornecedoras estudem que providência tomar. A figura 2.6 mostra as três fases do sistema elétrico e revela algumas estimativas de perdas por todo o processo de geração, transmissão e distribuição. A proposta final das *Smart grids* é que as unidades consumidoras, ou seja, as casas e edificações, e as unidades produtoras de energia estejam integradas de modo a prover informações de valor para melhoria da rede, e promover o manejo automatizado das fontes de energia. E, numa realidade ideal, já autorizada pela Resolução Normativa Nº 482 da ANEEL [36], permitir ao consumidor gerar sua própria energia e reduzir sua conta de forma inteligente e automatizada. A interpretação da resolução diz que o cidadão estaria emprestando energia à concessionária e esta, em troca, reduziria a conta referente ao consumo do cidadão. Esse cenário está bastante ligado ao Artigo 14º do Decreto Lei nº 5.163/2004 [37], que define o conceito de ”geração distribuída”:

Figura 2.5: Estados atingidos pelo blecaute de 21 de janeiro de 2002 (Folha de SP,2002) [4].

”Considera-se geração distribuída toda produção de energia elétrica proveniente de agentes concessionários, permissionários ou autorizados [...] conectados diretamente no sistema elétrico de distribuição do comprador[...]”

Portanto, com base na lei e na resolução citadas, abriram-se diversas possibilidades para o setor se tornar muito mais eficiente e moderno. Empresas podem gerar energia em uma localidade e o excedente, descontar do consumo da outra localidade, as casas podem ter seus próprios sistemas de microgeração e reduzir sua conta, além de desafogar as linhas de distribuição permitindo que as unidades consumidoras vizinhas também utilizem da energia fornecida, e as organizações, como um todo, tem mais liberdade para investir em novos modelos de negócio e projetos para a eficiência energética. Contudo, todas essa realidade utópica, na qual todos produzem boa parte de sua energia consumida, a rede trabalha de forma inteligente e conjunta para reduzir as perdas, reduzir os desperdícios, e aproveitar com máxima eficiência as fontes renováveis, só seriam possíveis graças à figura de alguns elementos específicos: os medidores inteligentes, os sistemas de controle e supervisão em rede e os sensores. Com sensores espalhados pela rede, primeiramente, a concessionária não fica dependente de contato dos consumidores para descobrir falhas

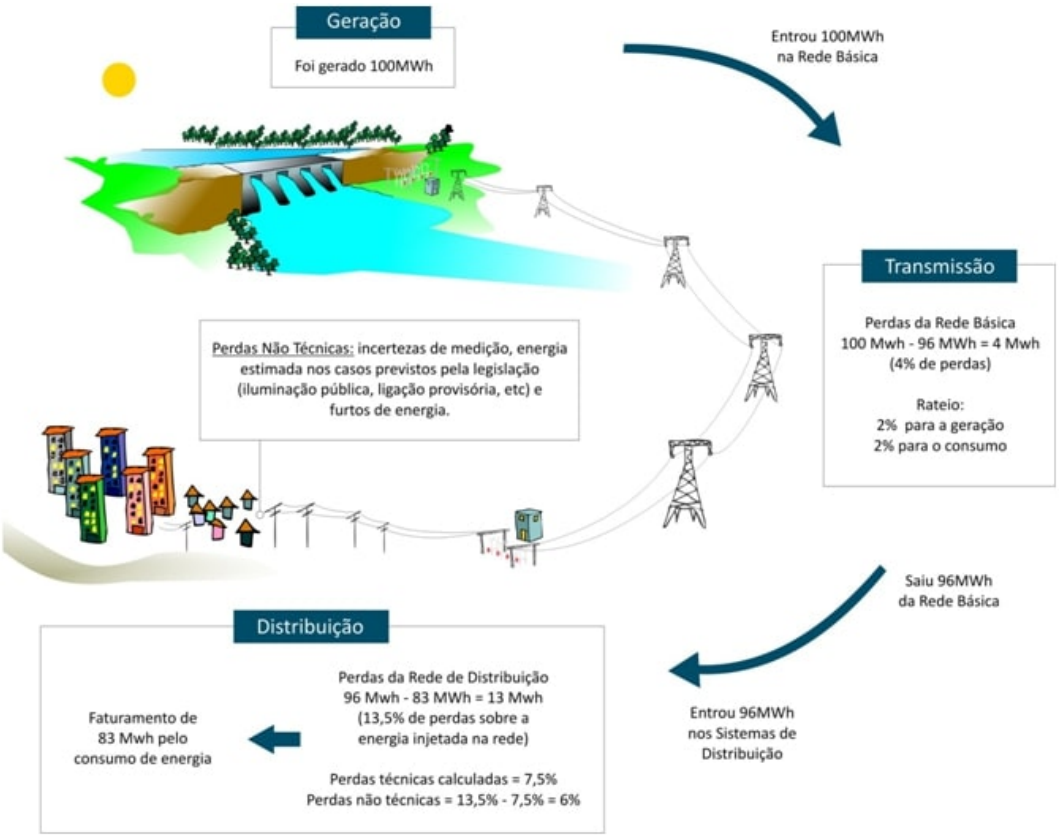

Figura 2.6: Ilustração mostrando as três fases da infraestrutura da rede elétrica e o cálculo das perdas estimadas para o exemplo (ANEEL,2019) [5].

e/ou quedas de energia. Com os medidores inteligentes, não só o perfil de consumo se torna conhecido, mas a qualidade da energia que chega e os fenômenos dos transientes, afundamentos, sobretensão, entre outros, se tornam observáveis, permitindo melhorias certeiras. Além disso, os sistemas de controle e supervisão conseguem alertar, em tempo real, quaisquer mudanças na rede e efetuar procedimentos de restabelecimento e/ou segurança de forma automática, como o desligamento de um cabo partido ou o acionamento de um transformador numa linha reserva, ou ainda o compartilhamento de energia entre diferentes localidades por questões de queda do acesso principal. A figura 2.7 ilustra os benefícios de uma unidade consumidora que usa energia solar na microgeração aliada com medidores inteligentes. Dado que os conceitos e vantagens das *Smart grids* estejam claros, como estas se relacionam com as referidas infraestruturas de comunicações? Ocorre que, nas *Smart grids*, as duas redes, elétrica e de dados, se complementam, auxiliando na gestão e controle. Porém, a maior parte das novidades nessa junção pende para o lado da concessionária, que passa a poder prestar um serviço de qualidade e precisão. De forma semelhante, as grandes infraestruturas proprietárias distribuídas, como as das empresas de telecomunicações de âmbito nacional, têm de gerenciar sua própria operação, que chega a ser comparável ou até mais complexa que a de uma concessionária de energia. Logo, todos os conceitos das *Smart grids* se aplicam, também, a empresas como Telebras, Embratel, Vivo e até órgãos do Estado como Polícia Rodoviária Federal, Aeronáutica, Exército, Agência Nacional de Transportes, Receita Federal, entre outros.

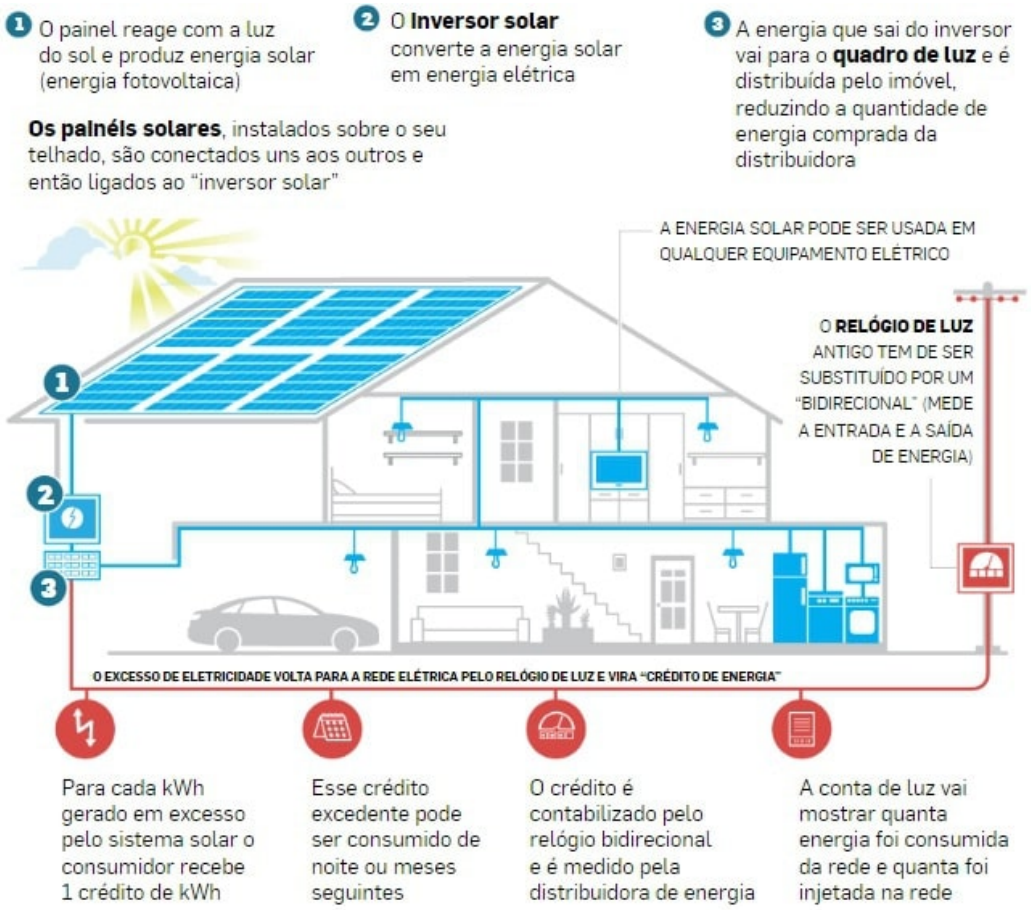

Figura 2.7: Imagem explicando o processo básico e os benefícios da microgeração para o caso da energia solar (CERNE,2018) [6].

Em suma, as *Smart grids* constituem um movimento não apenas inovador, mas necessário para que o restante dos setores e a sociedade continue evoluindo tecnologicamente. A cooperação entre as tecnologias de comunicação e as infraestruturas de serviços, como água, energia e gás, têm revolucionado a forma de gerenciar e manejar recursos, e é sobre esse tema o próximo tópico deste capítulo, o qual aborda a ”Internet das Coisas” e sua relação com o conceito global de ”Indústria 4.0”.

2.3 IOT E INDÚSTRIA 4.0

Este tópico tentará trazer a definição mais acertada atualmente para o termo ”Internet das Coisas” e sua relação com as revoluções iniciadas com o conceito global de ”Indústria 4.0”.

Com a evolução das redes de comunicação, em pouco tempo percebeu-se que a quantidade de

endereços disponíveis no padrão de endereçamento IPv4 (RFC 791 [38]) era insuficiente (RFC - Request For Comments - Requisição de Comentários, são documentos técnicos elaborados pela IETF - Internet Engineering Task Force -Força Tarefa de Engenharia da Internet, para padronizar o setor). O Protocolo IP (Internet Protocol - Protocolo da Internet, padrão da Camada de Rede da pilha TCP/IP usada na Internet), então, chegou à sua sexta versão com o o IPv6 (RFC 2460 [39]), e trouxe a possibilidade de qualquer dispositivo ter seu endereço único no mundo, e ser acessado de qualquer lugar. Esse conceito, ainda que utópico, deu espaço para o fomento de tecnologias de automação, supervisão e sensoriamento, fazendo o mundo vislumbrar um futuro em que tudo e todos estivessem conectados e acessíveis. Dali em diante, o próximo passo seria que cada ”coisa” conectada pudesse, por si só, tomar decisões e interagir com o mundo. Ou seja, os carros (integrados com os semáforos, se é que estes ainda fossem necessários) deveriam dirigir sozinhos, as luzes autorregulariam sua luminosidade, a geladeira faria compras quando percebesse a falta de um item, e assim por diante. Obviamente, os padrões de funcionamento comuns da Internet não tinham sido projetados para atender boa parte das aplicações possíveis num mundo onde tudo está conectado e livre para ser acessado. Hoje, essa ideia não é tão bem vista e encorajada, sendo bem diferente da forma real com que a IoT vem se desenvolvendo. Mas por que ainda não se apresentou uma definição clara sobre o que é a Internet das Coisas? Pelo fato de que ainda não se convergiu de maneira assertiva sobre o tema. Vários artigos foram escritos trazendo definições, porém cada uma tinha uma peculiaridade própria que a outra definição não observava. O documento ”Towards a definition of the Internet of Things (IoT)”, disponível na seção de IoT do site da IEEE [40] define usando o conceito inicialmente descrito, sobre um mundo em que os dispositivos tem ID’s únicos e são acessíveis de qualquer lugar. Diferentemente, o site da organização de consultoria mundial Gartner define IoT [41] com a mesma definição geral de redes de sensores: são, basicamente, dispositivos com tecnologia embarcadas que conseguem interagir, sentir e comunicar-se entre si e com o mundo externo. O conceito real ainda é tão divergente, que o mesmo documento publicado no site da IEEE citado define de forma direta que as *Smart grids* seriam apenas redes de sensores, e não IoT, enquanto todas as empresas e várias partes da comunidade acadêmica pensam o contrário, argumentando que as *Smart grids* interagiriam com equipamentos de microgeração os quais regulariam, de forma inteligente, sua geração (rementendo ao conceito de IoT original, e não de redes de sensores). Apesar dessas divergências, é possível definir que, inicialmente, a Internet das Coisas seria o nome generalizado de todos os sistemas que se utilizariam da Internet para supervisionar, monitorar, controlar e trabalhar em conjunto e de forma autônoma, independente de interação humana. Entretanto, a forma atual das tecnologias de IoT vem se apresentando uma evolução das originais redes de sensores. As redes de sensores são, em geral, redes locais sem fios ”ad hoc”, ou seja, não dependem de estação rádio base para se comunicar, organizando-se como redes ”mesh”, nas quais a informação flui entre os nós da rede. Para comparação, as redes sem fio padrão IEEE 802.11, em sua grande maioria, funcionam com estações rádio-base, ou seja, existe um nó o qual concentra dados e os difunde na frequência de operação. Mas é possível afirmar que as tecnologias de IoT são o mesmo que as das redes de sensores? Não, por motivo de um princípio simples: autonomia na aplicação. Os nós das redes de sensores não contém nenhum tipo de ”inteligência” ou reatividade, apenas

trabalham enviando e recebendo dados. Por outro lado, os dispositivos IoT têm a característica de conterem, em si, boa parte da aplicação sendo performada (ou seja, cada dispositivo preenche um papel na estrutura total), fazendo da comunicação uma forma de melhorar a eficiência e/ou atingir um objetivo o qual não é possível sem a cooperação dos nós da rede. Ou seja, na forma atual, as tecnologias de IoT seriam como ecossistemas completos de cooperação entre dispositivos, enquanto as redes de sensores seriam a composição em malha de um único sistema ou aplicação. Essa seria a definição mais acertada para o estágio contemporâneo dos desenvolvimentos e dos sistemas definidos como ”Internet das Coisas”.

O movimento de empoderamento dos dispositivos promovido com o amadurecimento das tecnologias de IoT trouxe importantes avanços para diversos outros setores, em especial, a Indústria. De forma resumida, sendo a Primeira Revolução Industrial atribuída, entre outros, à invenção da máquina à vapor; a Segunda Revolução Industrial atribuída à eletricidade e ao motor à combustão; e a Terceira Revolução Industrial, relacionada com a informatização dos meios de produção, o que, então, marcaria a chamada ”Indústria 4.0”? Nas mídias populares, comumente é possível ver confusão ao explicar esse termo usando conceitos da Terceira Revolução Industrial. Não se trata apenas de informatizar a produção, afinal, várias fábricas já funcionam de forma autônoma, e são vários os bens cujos estágios de produção são quase inteiramente performados por robôs. O termo, na verdade, se relacionaria com a integração dos dispositivos e da informação resultante dos processos de produção. Ou seja, de forma mais clara, a ”quarta revolução” estaria ligada não ao processo de fabricação em si, mas à quantidade de informação e ao nível de eficiência possível com as ferramentas de supervisão e monitoramento disponíveis. Sob um ponto de vista prático, as perdas seriam reduzidas ao máximo, os acidentes seriam evitados de forma autônoma e a produtividade cresceria de forma orgânica. Numa fábrica de carros, por exemplo, nem mesmo um parafuso seria perdido, o torque do aperto de cada parafuso seria tabelado e garantido, bem como o tempo de produção, a quantidade de tinta gasta seria controlada na ordem das miligramas, e por fim, a própria produção e montagem do veículo se daria sob encomenda e em tempo mínimo, maximizando a utilização dos meios em relação à demanda de mercado. Além disso, uma previsão importante do conceito é que tudo será customizável. Não existiriam mais gargalos de produção, de forma que o comprador poderia definir cores, formas, atributos, capacidades e termos inscritos, e os produtos, fabricados em tempo irrisório, logo lhe seriam entregues (também por métodos automatizados). Grandes reforços desses conceitos residem nas impressoras 3D, nas evoluções das entregas por drones, nos veículos autônomos, nos avanços das técnicas de Machine Learning (ou aprendizado de máquina) e Inteligência Artificial. O governo brasileiro tem uma ”Agenda brasileira para a Indústria 4.0”, disponível em [42], mostrando os objetivos e conceitos apresentados, além de permitir o conhecimento das estratégias do governo para o fomento da aplicação tecnologias. A figura 2.8 ilustra um processo de fabricação alinhado com os conceitos de integração e gerência usando IoT apresentados. Pode-se perceber, por fim, que as expectativas por trás da Internet das Coisas não residem nas tecnologias de forma pontual, mas nas possibilidades de ganhos através da integração completa dos dados e sistemas. Por ganho, entenda-se não apenas dinheiro, mas vários outros retornos, tais como: economia de tempo e recursos, redução

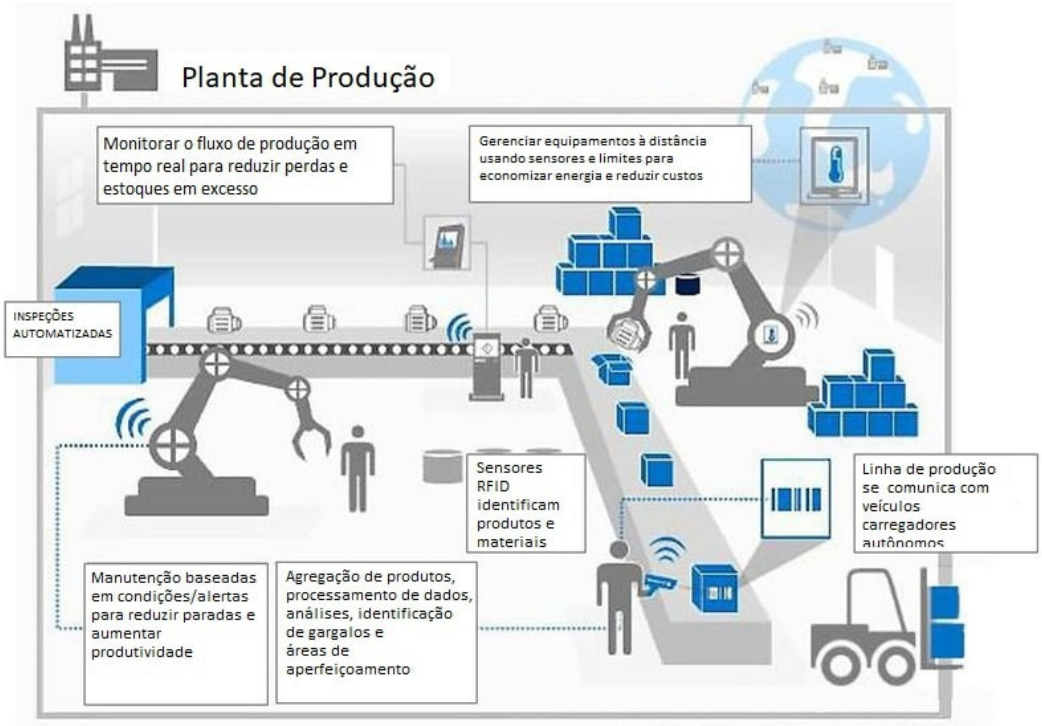

Figura 2.8: Ilustração de um processo de fabricação alinhado com os conceitos da Indústria 4.0 (3D Printing Industry,2016) [7].

dos incidentes e do desperdício geral, ganho de eficiência e controle... Por esse motivo, setores como o energético, industrial, de serviços, público, entre outros, vêm passando por revoluções tecnológicas. A Indústria 4.0 é apenas uma face de um movimento maior, que vem atingindo data centers, redes elétricas, residências e prédios, veículos, e o próprio ser humano, com as tecnologias assistivas.

A seguir, iniciam-se as fundamentações técnicas necessárias para a compreensão das propostas de projeto. O tópico seguinte tratará dos conceitos de gerência de redes e das classes de softwares decorrentes da área.

2.4 GERÊNCIA DE REDES E AS CLASSES DE SOFTWARES NMS, APM E DCIM

Este tópico resumirá a história da Gerência de redes e definirá os principais conceitos e termos da área. Depois, apresentará o esquema padrão de gerenciamento a ser aplicado em qualquer infraestrutura de comunicação e, por fim, apresentará as principais classes de softwares que surgiram no campo e que são importantes para o entendimento geral deste trabalho.

A expansão geográfica e de logística das redes de comunicação, bem como a variedade de sistemas proprietários e serviços providos pela infraestrutura de TIC ressaltou, com o tempo, a necessidade de evolução dos conceitos de gerenciamento de redes. Em primeiro lugar, deve-se

saber separar os conceitos de ”administrar” e ”gerenciar” uma rede. O administrador de redes é responsável por ajustar parâmetros, configurar sistemas, implementar melhorias, realizar alterações na operação, entre outros. O gerenciamento, no entanto, se foca em monitorar e acompanhar os parâmetros de performance e funcionamento da rede (e, mais recentemente, das aplicações), principalmente para garantir os requisitos mínimos de operação definidos, ou melhor nomeados de SLA's (Service Level Agreement - Acordo de Nível de Serviço). Em segundo lugar, deve ficar claro que a operação das redes atuais tem diversas exigências a serem cumpridas para que parâmetros como vazão, latência e disponibilidade estejam sempre dentro do esperado.

O tema de gerenciamento de redes se tornou largamente estudado no mundo, e alguns modelos de gerenciamento foram definidos por grandes entidades, se destacando o padrão TMN (Telecommunications Management Network - Rede de Gerência de Telecomunicações), elaborado pela ITU-T (Telecommunication Standardization Sector - Setor de Padronização de Telecomunicações) e o padrão FCAPS, elaborado pela ISO (International Organization for Standardization - Organização Internacional para Padronização). A seguir, uma breve descrição do modelo FCAPS, o mais relevante e largamente implementado sob o ponto de vista dos fabricantes de equipamentos:

Modelo FCAPS: Fault, Configuration, Accounting, Performance and Security - Falha, Configuração, Contabilidade e Performance, deu origem ao documento ISO/IEC 10040:1998. A ideia básica desse framework está definida na norma ISO 7498-4 e diz que existem cinco campos de gerência nas infraestruturas de comunicação, que podem ser definidos de forma simples como:

1. *Gerência de Falhas:* Detectar, documentar, notificar e resolver condições de operação anormais, as quais impactam na performance e disponibilidade dos serviços de rede (Exemplos de ocorrências relacionadas são os travamentos e desligamentos não programados).
2. *Gerência de Configuração:* Controle, monitoramento e documentação dos parâmetros, esquemas e versões de configuração dos dispositivos e serviços da rede (Exemplos de casos de uso relacionados são a gerência de patches de segurança e de esquemas de ligação do cabeamento entre switches e roteadores).
3. *Gerência de Contabilização:* Monitoramento, registro e notificação das distribuições de recursos e serviços de rede (Exemplos de casos de uso relacionados são a limitação do uso de banda para transmissão/recepção e a quantidade de conexões por ponto de acesso de rede sem fio).
4. *Gerência de Desempenho:* Monitoramento e medição dos parâmetros de performance da rede (Exemplos de dados importantes são taxa de transmissão, latência, descarte de pacotes e curva de crescimento do fluxo de dados numa organização).
5. *Gerência de Segurança:* Monitoramento, restrição, bloqueio e identificação de conexões e tráfegos de dados potencialmente prejudiciais para a continuidade do funcionamento da rede e dos serviços suportados (Exemplos de casos de uso importantes

são bloqueio de sites e endereços e identificação de potenciais atacantes escaneando vulnerabilidades na rede).

O padrão FCAPS da ISO acabou sendo largamente adotado pelos fabricantes e inspirando as grandes entidades de processos e boas práticas em TIC, tais como ITIL (Information Technology Infrastructure Library - Biblioteca de Infraestrutura de Tecnologia da Informação) e COBIT (Control Objectives for Information and related Technology - Objetivos de Controle para Informação e Tecnologias Relacionadas). Por fim, um último detalhe que ajuda a compreender o papel desse padrão é que, se a gerência de redes fosse um sistema tipo ”caixa preta”, o framework (ou modelo de trabalho) FCAPS ajudaria a definir as saídas desejáveis, contudo, não faz parte de seu foco a definição de arquiteturas e padrões técnicos de monitoramento, ou seja, o modo como o sistema dentro da caixa funciona, apenas suas saídas (talvez por esse motivo, tenha sido tão bem aceito na Indústria).

Para contextualização da gerência, será ilustrada de forma breve a estrutura em camadas das tecnologias de redes de computadores. Segundo Kurose (2010) [43], a Internet, hoje, é baseada na pilha de protocolos TCP/IP, que define cinco (5) camadas funcionais:

Camada de Aplicação: É nela onde funcionam os programas e a interação deles com o usuário ocorre. Num processo de comunicação, é nela que se formam as mensagens (unidade de informação da camada), e estas são de livre implementação, de acordo com a aplicação. Aqui, a comunicação é gerida entre aplicações. Existem diversos protocolos da camada de aplicação, e um exemplo é o HTTP (Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto).

Camada de Transporte: Nessa camada, protocolos de transporte realizam o envio de pacotes de dados entre máquinas/hosts. Questões como garantia de taxa de envio, confirmação de recebimento, fragmentação dos dados, remontagem desses, entre outros, ocorrem nela. Nela, a unidade de informação são os ”segmentos”. Existem dois protocolos padrões da Internet: UDP (User Datagram Protocol - Protocolo de Datagramas de Usuário) e TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão).

Camada de Rede: Essa camada é a responsável pela interconexão entre o host e a rede, além do conhecimento de outras redes. Nela, a unidade de informação é o datagrama. É nela que são reconhecidos os endereços de rede. O protocolo mais importante e universal que funciona nesta é o IP (Internet Protocol - Protocolo da Internet).

Camada de Enlace: Esta camada gerencia o envio de dados entre dispositivos diretamente conectados, ou seja, de um nó imediatamente ao próximo no enlace de conexão. Nela, a unidade de informação é chamada de ”quadro”. Os protocolos de controle de acesso ao meio como o CSMA/CD (Carrier Sense Multiple Access / Collision Detection - Acesso Múltiplo Sensível a Portadora / Detecção de Colisão), os quais possibilitam o funcionamento tradicional das redes cabeadas, atuam nesta camada.

Camada Física: Nesta camada, são movimentados bits de informação no enlace/conexão entre dispositivos. Aqui, são aplicadas técnicas de codificação e modulação digital para enviar e receber bits através de um determinado meio, seja um cabo, seja o vácuo (redes sem fio).

Na figura 2.9, além das camadas da pilha TCP/IP, estão representadas as sete (7) camadas do modelo OSI/ISO (Open System Interconnection/International Organization for Standardization - Interconexão de Sistemas Abertos/Organização Internacional para Padronização), proposto em 1984. Apesar de esse modelo não ter se tornado padrão, este serviu (e ainda serve) de guia para o amadurecimento e desenvolvimento de protocolos e aplicações. Contudo, é possível perceber que em nenhum momento citou-se qualquer esforço para gerenciamento dos processos de comunicação. Ainda que, à primeira vista, não pareça fazer sentido incluir a gerência em cada processo de comunicação ocorrido, observa-se que a presença de uma camada de controle a qual acumula e reporta erros, por exemplo, seria de extrema utilidade. Indo além, apesar de a Camada de Transporte oferecer vários serviços à camada de Aplicação, não existe qualquer previsão de implementações de gerência. É interessante notar, como será visto posteriormente, que a gerência de redes começa a tomar força apenas no início da década de 1990, anos depois da padronização em camadas da ISO, e mais de uma década depois da pilha TCP/IP se firmar como padrão da Internet. Por esse motivo, a Gerência de Redes ocorre inteiramente na Camada de Aplicação, apesar de boa parte dos processos de interesse ocorrer nas camadas inferiores. Como dito anteriormente, o modelo FCAPS não define o processo de gerência, apenas as entregas desejáveis. Isso não significa, no entanto, que não existam padrões a serem seguidos. O problema geral se resume à variedade de fabricantes e tecnologias que geram uma imensa massa de dados de gerência em diversos protocolos, métricas e meios de transmissão e a necessidade de operar de forma eficiente e rápida/automatizada com esses dados. De forma básica, o ramo tem terminologias próprias e uma arquitetura básica para qualquer projeto de monitoramento, conhecida como Internet Network Management Framework - Estrutura de Gerenciamento de Rede da Internet, ou SNMP Framework (tendo sua última versão descrita em [44] e [45]). A seguir, os principais termos:

Gerente: Constitui o nó concentrador de informações de toda a rede, é ele o destino final dos dados de gerência de todos os dispositivos. São softwares complexos e com alta carga contínua de processamento. Requisitos mínimos para esses softwares são capacidade de integração com múltiplos protocolos, implementação escalável de rotinas assíncronas de pooling (requisição de dados de agentes), interfaces gráficas com apresentação de logs, falhas, eventos e gráficos em tempo real (comumente denominadas ”dashboards”), além de integração com ferramentas de notificação e automação de processos, como autodescoberta de dispositivos na rede e resolução automatizada de problemas de configuração e atualização de sistemas. Pela complexidade inerente, existe um esforço contínuo de organizações abertas para o desenvolvimento e distribuição de soluções gerente. Exemplos globais são os softwares Zabbix [25] e Nagios [46].

Elemento Gerenciado: Esses são os alvos finais da gerência. Todo dispositivo com algum papel relevante para o funcionamento da rede é um possível dispositivo gerenciado. Note-se, no

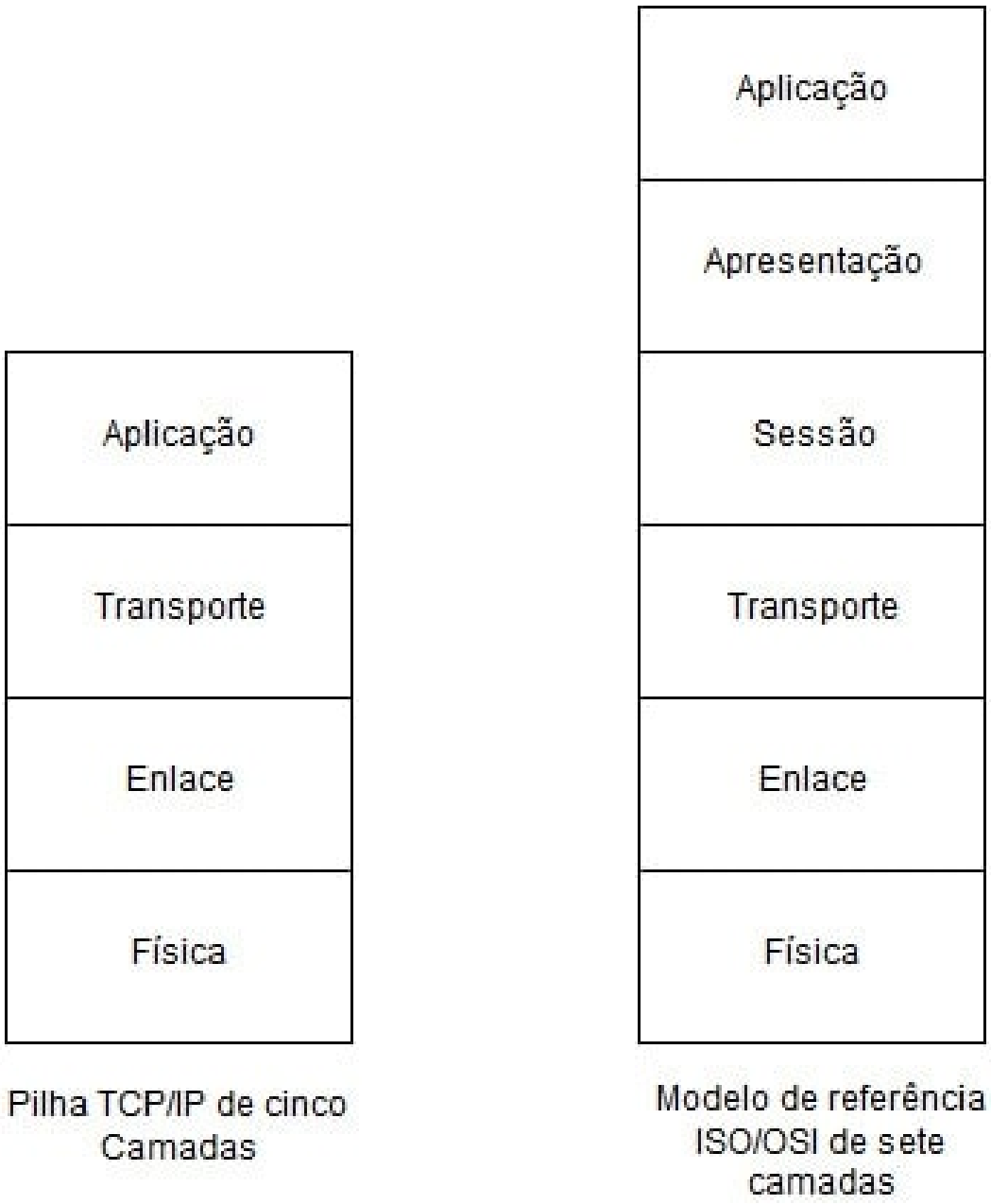

Figura 2.9: Apresentação das cinco camadas da pilha TCP/IP e das sete camadas do modelo OSI/ISO.

entanto, que as redes e tecnologias evoluíram bastante, de forma que hoje existem diversos componentes infraestruturais virtualizados. Dessa forma, a nomenclatura ”dispositivo gerenciado” não é mais universal já que, de fato, pode não haver sempre um dispositivo fisicamente verificável, mas sim, uma entidade lógica. Exemplos são máquinas virtuais, roteadores e pontos de acesso de rede sem fio.

Agente: É comum encontrar textos e apresentações na Internet igualando os conceitos de agente e dispositivo monitorado, no entanto, o modelo Internet Network Management Framework difere os dois de forma bastante clara: enquanto o dispositivo existe de forma lógica na composição dos elementos da rede e/ou dos serviços fornecidos, o agente será um software

o qual coleta as informações de gerência dos dispositivos e os envia para o gerente, podendo estar no próprio dispositivo monitorado ou estar em um único ponto de uma infraestrutura coletando dados de vários dispositivos. Mas, por que acrescentar um elemento entre o dispositivo gerenciado e o gerente? Dois são os principais motivos: integração entre diferentes plataformas e fabricantes e recurso de coleta e acumulação de parâmetros estruturados de forma padronizada. O primeiro, de acordo com os fatos descritos anteriormente sobre o problema da variedade de dispositivos, tecnologias e fabricantes, é fácil de ser interpretado: se existir um programa agente o qual é homogêneo e fala os mesmos protocolos e formatos de dados alocado em todos os dispositivos, a integração desses na gerência será fácil e rápida. O segundo motivo, sobre a acumulação de parâmetros estruturados de forma padronizada, não é trivial e será abordado em mais detalhes durante a fundamentação sobre estruturas de dados no tópico seguinte deste trabalho, denominado ”Bases de Dados, MIB’s e SMI’s”.

Objeto: ”Objeto” é o nome dado ao valor representativo da grandeza gerenciável medida e disponível para consultas. Isso significa que a quantidade de pacotes descartados na interface de um roteador é um objeto, já que esse é um parâmetro medido e gerenciado. Por outro lado, a quantidade de colisões numa dada faixa de frequência para uma antena transmissora de dados não é um objeto, já que essa não é uma grandeza mensurada pelos sistemas comuns e tampouco é gerenciável.

Protocolo de Gerência: Todo esquema de gerência de redes depende de um protocolo. O termo ”protocolo”, por si só, não obriga o uso de um protocolo de Camada de Rede ou de Transporte da pilha TCP/IP, ou ainda um determinado meio de transmissão, na verdade, indica que deve ser usada uma sequência de passos padronizados e previamente definidos para que o processo desenhado sempre atinja seus objetivos de forma igual. O principal protocolo de gerência de redes atual é o SNMP (Simple Network Management Protocol - Protocolo Simples de Gerenciamento de Redes), o qual trabalha baseado no Protocolo da Camada de Transporte da pilha TCP/IP chamado UDP (User Datagram Protocol - Protocolo de Datagramas de Usuário). Contudo, muitos softwares gerentes definem seus próprios métodos de aquisição de dados baseados no Protocolo da Camada de Transporte chamado TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão). No caso do software Zabbix, por exemplo, o usuário pode usar o procolo SNMP ou optar pelo ”Agente-Zabbix” [47], software desenvolvido em linguagem C com versões para várias plataformas e sistemas operacionais que segue uma sequência de passos definidos pelo software gerente tais como o uso da porta 10050, formato dos dados, chaves de envio e identificação do dado requisitado, regras de autodescoberta, entre outros.

MIB: Management Information Base - Base de Dados de Gerência. Como o próprio nome sugere, trata-se de um banco de dados de gerência disposto em cada elemento gerenciado, da qual o agente coleta os dados e os envia para o gerente. O conceito será abordado mais profundamente no próximo tópico deste trabalho, denominado ”Bases de Dados, MIB’s e SMI’s”.

OID: Object Identifier - Objeto de Identificação. É o nome do código que identifica cada objeto dentro da MIB e permite que um agente colete o dado de forma precisa e que o gerente saiba uqe dado é esse sem que os dois tenham que trocar descrições. Esse conceito será abordado de forma mais abrangente no tópico ”Árvores de Nomes”.

SLA: Service Level Agreement - Acordo de Nível de Serviço. Apesar de não fazer parte de forma oficial das definições de gerência de redes, foi absorvida com o tempo. Ocorre que, em várias abordagens de boas práticas em TIC (promovidas por entidades como a ITIL), a gerência é um recurso do setor de infraestrutura a qual atesta se os serviços oferecidos ao restante da organização estão satisfatórios sob o ponto de vista do acordo sobre a qualidade mínima. De forma prática, SLA's são medidas em números (por exemplo, limitação da quantidade de falhas e incidentes registrados a 100 por mês), porcentagens (por exemplo, disponibilidade mínima de um serviço é 95%), e tempo (por exemplo, intervalo máximo de tempo dispendido para restabelecimento de serviço interrompido é 2 horas).

NOC: Network Operations Center - Centro de Operações de Rede. Também não é um termo oficial da gerência, mas acabou se tornando padrão de indústria tal qual o termo ”SLA”. De forma resumida, assume-se que a automação não é totalmente capaz de reagir, informar e identificar todos os possíveis problemas e situações prejudiciais à manutenção das SLA's, e portanto, seria necessário um local físico com operadores e analistas humanos monitorando a(s) saída(s) do(s) software(s) gerente(s) e atuando nos casos necessários.

A figura 2.10 mostra a arquitetura básica. Um ou mais softwares gerentes interagem com agentes instalados nos dispositivos gerenciados, os quais coletam dados de MIB's locais e os enviam. No caso em que se usa o Protocolo SNMP, o envio destes dados seguem uma ”linguagem” específica e universal. Um fato interessante é que, em princípio, os softwares gerentes e as atividades de gerência de redes se baseavam puramente em conhecer e garantir o funcionamento correto e satisfatório da rede. Entretanto, com o avanço das tecnologias de fornecimento de dados via Internet (como as API's - Application Programming Interface - Interface de Programação de Aplicativos) e de armazenamento (como as redes SAN - Storage Area NetworK - Rede de Área de Armazenamento), o monitoramento de aplicações e regras de negócio também foi absorvido pela gerência. Por esse motivo, surgiram várias classes de aplicações, e entre elas, destacar-se-ão três, as quais têm relevância para as discussões deste trabalho:

NMS: Network Management System - Sistema de Gerência de Redes, é o software que faz o papel clássico de gerente descrito anteriormente. Monitora parâmetros de redes, dispositivos e elementos gerenciados como servidores e máquinas virtuais.

APM: Application Performance Management - Gerência de Performance de Aplicação. São softwares extremamente complexos, os quais interagem em camada de aplicação e, não raro, imitam o comportamento de um usuário comum tentando verificar se o serviço provido pela aplicação está dentro dos padrões aceitáveis definidos, ou seja, das SLA's configuradas. É extremamente comum e necessário em organizações cujo núcleo dos negócios reside em

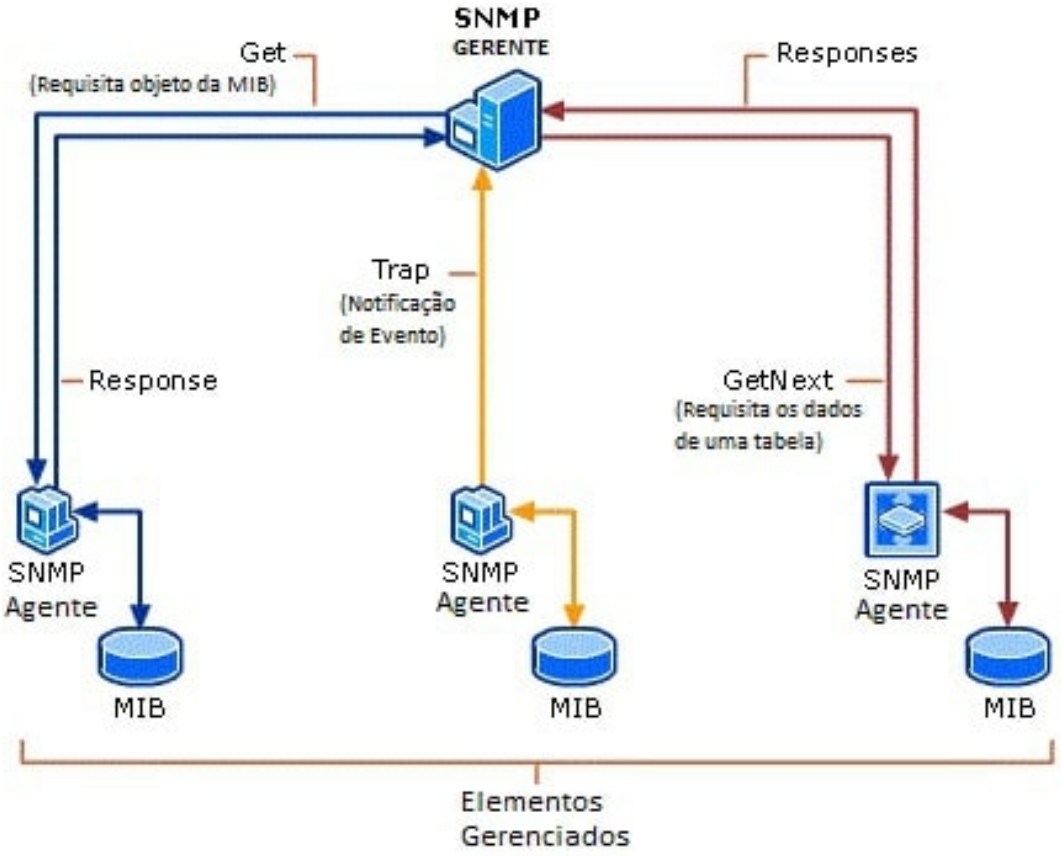

Figura 2.10: Arquitetura e conversação básica de um esquema de gerência baseado no framework SNMP [8].

aplicações via rede tais como órgãos do Poder Executivo, bancos, empresas de prestação de serviços em rede, grandes portais da Internet, entre outros.

DCIM: Data Center Infrastructure Management - Gerência de Infraestrutura de Data Center. Apesar de serem soluções vendidas como exclusivas para data centers, é crescente a quantidade de organizações interessadas em manter uma ferramenta que concentra todas as características e informações de suas instalações, incluindo não somente os data centers, mas as subestações de energia, as salas de redes, a planta elétrica, entre outros. Esse tipo de software age tal qual o NMS, como um gerente, a diferença reside no fato de que os objetos não são grandezas necessariamente de redes e/ou aplicações, mas sim, de infraestruturas e sistemas físicos, tais como acesso a portas, corrente e tensão elétricas, temperaturas, funcionamento de sistemas de refrigeração, acompanhamento de chaves de transferência, alarmes de falta/surto de energia, entre outros.

Por fim, o campo da Gerência de Redes é muito vasto e largamente estudado. Esta seção objetivava puramente alinhar e apresentar os conceitos técnicos e práticos principais que pudessem apoiar as considerações e propostas de projeto apresentadas a partir do terceiro capítulo deste trabalho. A seguir, serão abordadas em detalhes as convenções por trás das bases de dados, MIB's e SMI, fundamentando a organização dos objetos gerenciados no framework padrão da gerência de redes.

2.5 BASES DE DADOS, MIB E SMI

Neste tópico, serão definidos os conceitos de bases de dados, das MIB's, dos padrões de estruturas de dados usados e como estes se alinham para possibilitar o funcionamento do framework padrão de gerência de redes nas mais diversas plataformas e fabricantes.

Bases de dados são comuns e estão presentes em praticamente todos os dispositivos microprocessados com os quais o ser humano interage. O conceito é simples e efetivo: trata-se de um elemento físico ou lógico no qual dados são armazenados de forma organizada e o conhecimento do modelo de organização permite recuperar e/ou escrever esses dados sempre que for necessário de forma estruturada. Não se deve, no entanto, confundir as bases (ou bancos) de dados com os sistemas de gerenciamento de bancos de dados (SGBD's), os quais são sistemas complexos que existem para abstrair a interação com os dados e trazer outras garantias (como redundância e normalização) e boas práticas para o bom funcionamento do processo de armazenagem e recuperação lógica (e, às vezes, física) da informação. São as bases de dados que permitem que uma determinada informação exista num dispositivo e seja usada para algum fim, ou seja, permitem que o dado persista por um momento maior do que o de sua criação (isso não significa que toda base de dados guarda os dados de forma permanente, apenas define que a disponibilidade da informação num sistema se dá através dela).

Sabendo, portanto, do conceito formal de uma base de dados, fica mais fácil compreender uma MIB (Management Information Base - Base de Informações de Gerência). De forma resumida, a MIB é uma organização estruturada dos dados de gerência de um dispositivo e/ou elemento gerenciado. Sendo um padrão tão universal, a MIB-II, como é chamada a base de dados de gerência específica para dispositivos de rede segue a RFC 1213 [48], que veio para acrescentar novidades à RFC 1156 [49].

Como dito, a MIB-II é bem diferente dos bancos de dados comuns das aplicações. Primeiramente, pela forma como está organizada a base: os dados estão dispostos em árvore, contendo cada um seu próprio nome e número de identificação (único). O motivo dessa organização reside na facilidade de implementação e de operação em qualquer plataforma. Uma vez que os dados estão dispostos em árvore, realizar buscas será fácil, rápido e com pouco uso de memória (como discutido na seção "Algoritmos de Busca" mais à frente). Além disso, o fato de cada um ter um número de identificação inteiro e único facilita a implementação, pois não é necessário fazer qualquer conversão entre tipos de dados de diferentes plataformas ou linguagens para realizar buscas, como seria o caso com o uso de strings (palavras). A gerência de um dispositivo não deve, jamais, afetar seu desempenho, por isso, seus requisitos de processamento e uso de recursos como armazenamento e memória devem ser mínimos, bem como o tempo de resposta, o mais rápido possível. A figura 2.11 mostra um detalhe do ramo da MIB-II na árvore da ISO. As estruturas desses dados também merecem destaque e constituem o segredo do sucesso na universalização da MIB-II. Além de cada objeto ter um nome e número de identificação único, também tem uma

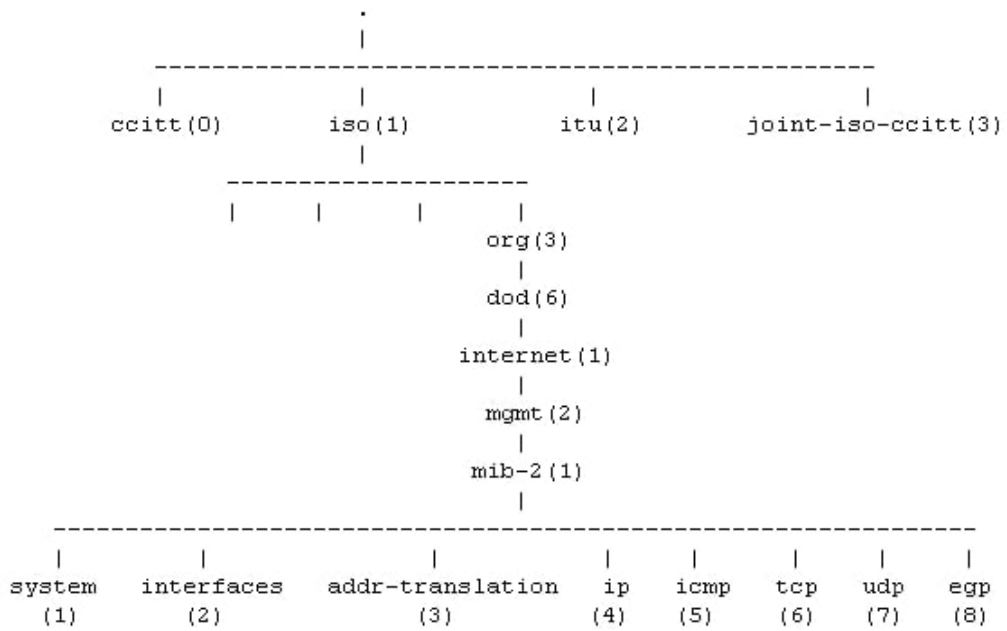

Figura 2.11: Detalhe da árvore de OID's partindo do nó da ISO até uma parte do ramo da MIB-II (J. C. S. Freitas,2000) [9].

codificação própria, baseada no padrão ASN.1 (Abstract Syntax Notation One - Sintaxe de Notação Abstrata Um), o qual é de grande relevância e está descrito até mesmo por uma norma da ISO (ISO/IEC 8824), bem como o processo de envio de dados usando ASN.1 também está descrito em outra norma da mesma organização (ISO/IEC 8825). A RFC 2578 [50] define a segunda versão do padrão SMI, que é a definição, com base no padrão ASN.1, dos subconjuntos da MIB-II.

Afinal, como entender, de forma prática, o que significam essas definições de estruturas de dados? De forma resumida, pode-se definir que todo dispositivo microprocessado funciona com base num software, e esse software, ao ser carregado no hardware, é traduzido em comandos de baixo nível, ou seja, instruções de máquina, e, em último estágio, em binários, de acordo com a arquitetura do hardware, a qual pode diferir entre os fabricantes por diversos motivos que fogem ao escopo deste trabalho. Decorre dessas diferenças o fato de que a representação em nível de circuito físico de um tipo básico de informação num dispositivo pode ser diferente de outro. O exemplo mais comum é o fato de que um número inteiro pode ser representado de forma totalmente contrária dependendo da plataforma. Considerando a memória como uma sequência de blocos lógicos, a notação "big endian" é usada quando os bits nos primeiros no bloco de endereço de memória são os de maior peso no valor do dado representado em relação aos de endereço posterior. Por outro lado, na notação "little endian", os mesmos bits nos primeiros endereços na memória são os de menor peso na representação em relação aos de endereço posterior. Apesar de parecer uma diferença muito pequena e específica, é necessário lembrar que o envio de dados pelas tecnologias usadas atualmente é feito, a nível da Camada Física da pilha TCP/IP, bit a bit, logo, se uma plataforma usa notações totalmente diferentes das outras, como poderão se comunicar de forma apropriada? Uma solução foi proposta com a Camada de Apresentação do modelo

OSI/ISO (Open System Interconnection - Interconexão de Sistemas Aberta) para a Internet. Apesar de não ter sido padronizado formalmente (a pilha TCP/IP é o padrão atual), o conceito das camadas OSI inspirou (e ainda inspira) grande parte dos projetos de engenharia para padronização em redes. A solução funcionaria da seguinte forma: a Camada de Aplicação seria aquela a se preocupar com o serviço o qual interage com o mundo e com os usuários, logo, seu manejo dos dados deveria ser livre, contudo, ao passar os dados para a Camada de Apresentação, estes seriam convertidos usando as notações padronizadas conforme normas já citadas, para então poderem ser enviados adequadamente. Essas notações são chamadas abstratas, e o número um em "ASN.1" significa unicamente que é a primeira e mais básica notação definida. Portanto, o protocolo de gerência SNMP foi concebido para trabalhar usando a primeira e mais básica notação do modelo OSI para facilitar o envio de dados e vencer a barreira das diferenças nos projetos e arquiteturas de hardware.

Apresentada a problemática a qual o padrão ASN.1 resolve, decorre intuitivamente a referência da sigla SMI (Structure of Management Information - Estrutura de Gerência de Informação). Em suma, se a MIB é onde os objetos são guardados e o ASN.1 é a forma como são descritos em memória, o que faz a citada RFC 2578, sobre a segunda versão do SMI, nada mais é do que definir quais são os objetos gerenciados em dispositivos de redes e como eles estão organizados dentro da MIB.

Tendo exposto os conceitos de bases de dados, MIB's e SMI, no tópico a seguir, serão descritos como os objetos gerenciados da MIB se relacionam com outros padrões difundidos pelo mundo, e o que implica o uso de uma árvore de nomenclatura num framework de gerência de redes.

2.6 ÁRVORES DE NOMES

Este tópico introduzirá um conceito extremamente importante para o funcionamento do framework de gerência de redes, que são as árvores de nomes. Além disso, relacionará essas estruturas com definições formais, trará análises breves sobre sua importância na implementação de softwares e projetos e na própria gerência de redes.

Não apenas no setor de telecomunicações, mas em vários outros campos da ciência, existe uma necessidade constante de organização hierárquica de nomes, como pode ser visto na figura 2.12, que mostra a árvore filogenética da Biologia. Tome-se como exemplo a definição de nomes científicos no campo da Biologia: segundo um sistema binomial de nomenclatura, cada espécie tem seu nome formado por duas palavras vindas do Latim, e a primeira delas indica o gênero da espécie, enquanto a segunda diferencia esta espécie das demais. Adicionalmente, existe uma taxonomia universal que segue um hierarquia muito bem definida: reino, filo, classe, ordem, família, gênero, e, por último, espécie. O resultado de toda essa organização é uma estrutura em árvore. Na teoria dos grafos, um árvore é definida como um grafo conexo, não cíclico e no qual, a partir de um nó

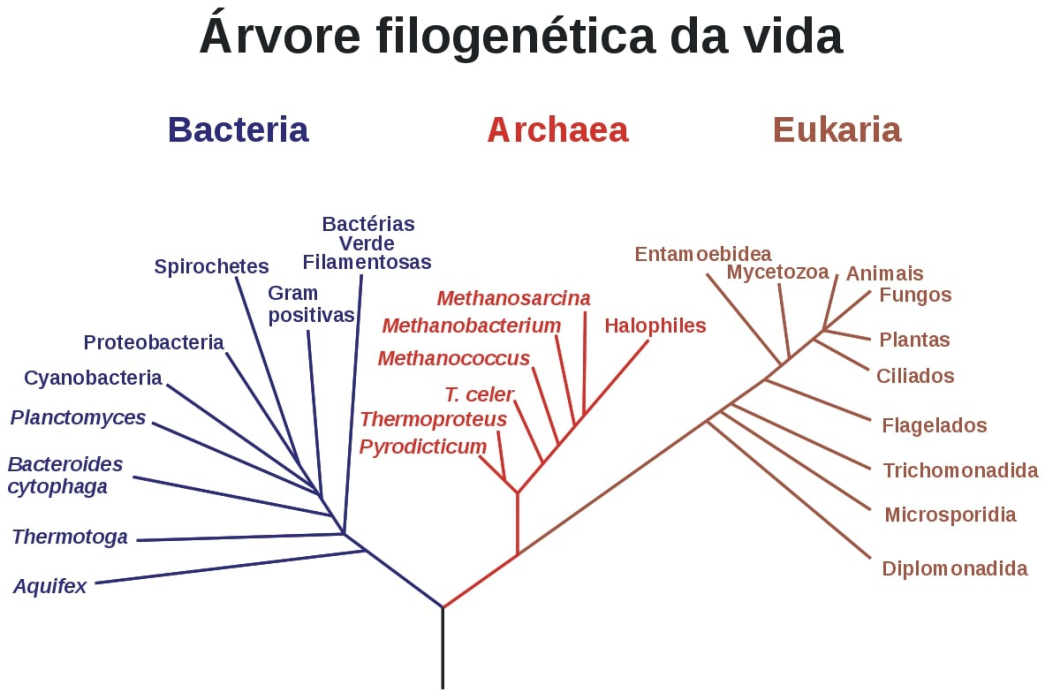

Figura 2.12: Árvore Filogenética da Biologia (Wikipédia,2008) [10].

arbitrário, é possível atingir qualquer outro nó por um, e apenas um, caminho. Além disso, um nó será de grau um (1) se estiver conectado por uma aresta a apenas um (1) outro nó, e portanto, esse nó será uma folha. Também é uma propriedade desses grafos especiais o fato de que, se a árvore possui ao menos uma aresta, então ela possui ao menos uma folha. As definições teóricas de grafos para árvores são extremamente úteis para explicar o sucesso delas na implementação de sistemas hierárquicos. Em primeiro lugar, como existe apenas um caminho com uma única sequência de arestas a partir do nó raiz para cada folha, se as arestas possuírem nomes e/ou números únicos, cada folha poderá ser identificada imediatamente pela junção desses, produzindo um sistema de identificação único de forma automática e inerente à estrutura. Além disso, com o conhecimento prévio do caminho (ou parte deste) para qualquer folha da árvore, o acesso/busca é extremamente veloz e com baixa complexidade computacional. Não é surpresa, portanto, que tenha sido essa a estrutura escolhida para o ”OID Project”, descrito de forma simples e eficiente em [51]. OID’s (Object Identifiers - Identificadores de Objeto) são, como o próprio nome sugere, identificações únicas e sem ambiguidade os quais ajudam a padronizar nomes de forma hierárquica. A ITU-T, em conjunto com a ISO, mantém uma grande árvore de OID’s (existe um repositório aberto com mais de 900.000 registros em [52]) das mais diversas áreas, e todas descritas com base nas recomendações do padrão ”ASN.1”. A relevância desse conceito para o presente trabalho reside no fato de que os objetos gerenciados nas MIB’s dos dispositivos, segundo RFC’s já citadas, obedecem a essa hierarquia, e é daí que vem o tão famoso nome da identificação dos objetos gerenciados no jargão de gerência de redes. Sob o ponto de vista computacional e algorítmico, as estruturas de dados em árvore se tornam interessantes quando obedecem a critérios um pouco mais específicos. Em primeiro lugar, precisam ser árvores binárias (ou seja, cada nó

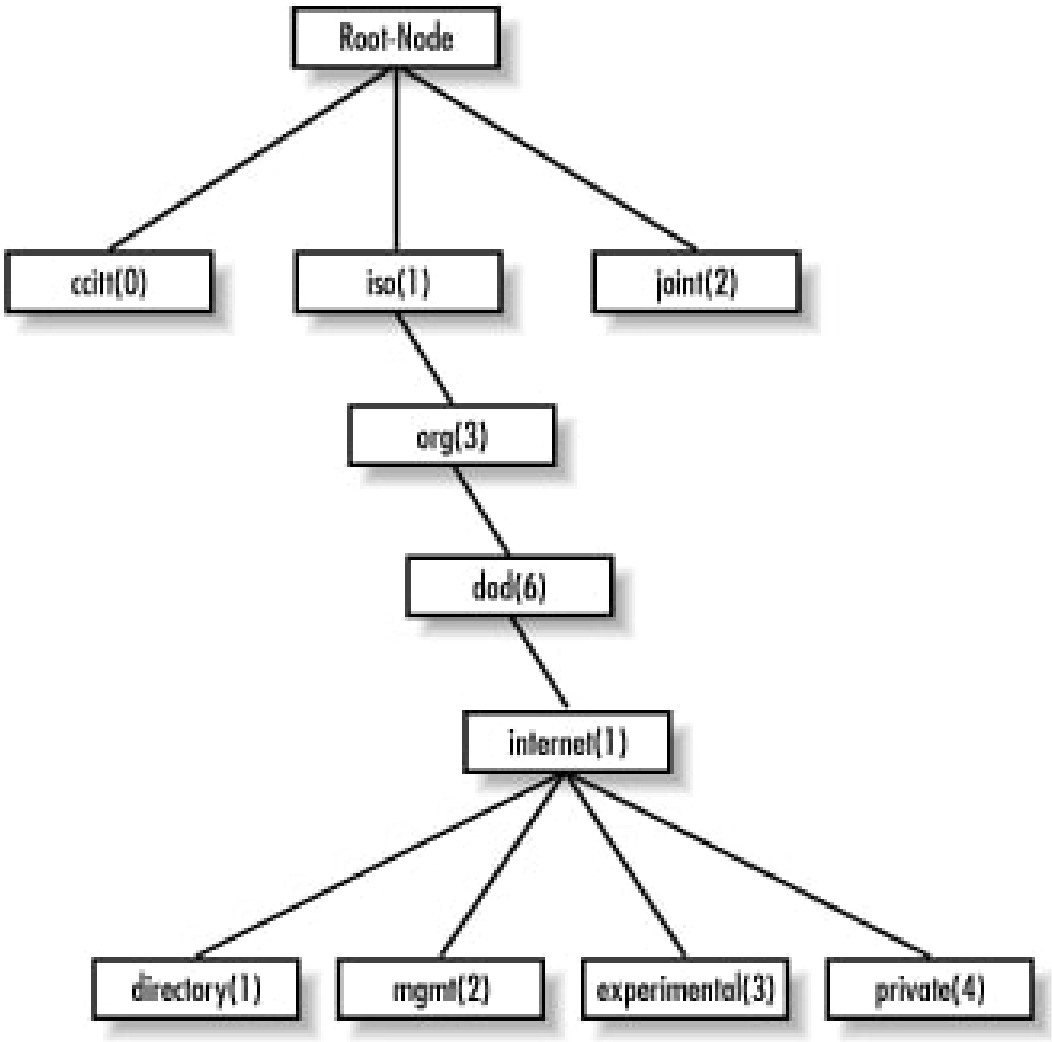

Figura 2.13: Topo da hierarquia de nomes da árvore de objetos SMI(O'Reilly and Associates,2002) [11].

será uma folha ou terá dois outros nós se originando dele). Em segundo lugar precisam ser razoavelmente equilibradas, ou seja, um dos ramos não pode se desenvolver de forma muito mais numerosa que o outro. Apenas por obedecer esses dois conceitos, dados organizados em árvores binárias equilibradas atingem performances invejáveis para buscas, inserções e remoções de dados em algoritmos computacionais. Portanto, ao gerenciar grandes massas de dados, se houver uma forma de organizá-las em árvores binárias de busca, é altamente encorajado que seja feito. Estudando esse conceito, uma das primeiras definições de estruturas de dados surgiu, a "árvore AVL" (Adelson-Velskii e Landis – 1962). De forma resumida, uma árvore AVL é uma árvore binária altamente balanceada, sendo perfeita para elevar ao extremo performances de operações com bases de dados. Definindo o balanceamento de forma mais ilustrativa, se o nó raiz de uma árvore dá origem a dois ramos, esquerdo e direito, uma árvore AVL é aquela na qual a altura (ou seja, a quantidade de níveis de hierarquia) em cada um dos dois ramos, direito e esquerdo, não difere em mais do que uma (1) unidade. Essa característica é garantida por uma série de operações de troca de posição dos nós quando da inserção e/ou remoção de um nó. Apesar de ser extremamente útil para modelagens de algoritmos, quando os dados possuem representações

complexas e/ou abstratas (tal qual o padrão Abstract Syntax Notation One, ou ASN.1), é muito difícil relacioná-los com base numa árvore AVL. Portanto, qual a relevância desse conceito para gerência de infraestrutura? Ocorre que a árvore AVL é aquela com a melhor performance possível em complexidade algorítmica, sendo que numa árvore com "N" elementos, a complexidade em buscas, inserções e remoções tende a $O(\log_2 N)$. Para efeito de comparação, uma árvore binária com sucessivas inserções desorganizadas pode comprometer a complexidade para até O(N), que seria o mesmo que realizar uma busca linear num vetor, não representando ganho de performance algum. Portanto, em uma base de dados organizada em árvore binária, caso as alturas dos ramos sejam constantemente checadas, pode-se calcular o fator de balanceamento (que seria a diferença de altura entre os dois ramos principais) e medir o quanto a árvore se distanciou da árvore AVL. Não apenas isso, mas o conceito formal de uma árvore AVL define que qualquer subárvore deve, também, ser equilibrada. Logo, é possível aplicar rotinas de verificação a grandes árvores binárias para remanejamento dos nós de forma a torná-la mais próxima da árvore AVL ideal, e portanto, manter o ganho de performance. Os ganhos com o uso da estrutura em árvore não se mostram tão relevantes para massas de dados simples (como números inteiros pequenos) da ordem de centenas ou milhares devido ao poder computacional disponível hoje, porém, para o caso de milhões de objetos complexos, ou ainda bilhões, essa é uma abordagem de projeto extremamente relevante. Observa-se, por fim, que o caso das *Smart grids* e das infraestruturas inteligentes recai num escopo extremamente massivo de dados, no qual pode existir um número indefinido de dispositivos sensores e cada qual conter, ainda, um número suficientemente grande de variáveis, portanto, o conhecimento e fundamentação das estruturas de dados e gerência em árvores e o uso de padrões como ASN.1 e a árvore de OID's da ISO podem ser de grande auxílio. Tendo abordado os conceitos técnicos importantes do campo de gerência de redes, o tópico a seguir irá detalhar os pontos interessantes do protocolo padrão que nomeia o framework atual de gerência de redes: o SNMP.

2.7 PROTOCOLO SNMP

Este tópico trará definições e detalhes adicionais acerca do protocolo SNMP, além de fundamentações sobre as vantagens no seu uso. Também percorrerá de forma breve a evolução do protocolo com a finalidade de mostrar a importância, simplicidade e robustez de sua aplicação em projetos de gerência.

Entre os elementos descritos no tópico "Gerência de Redes e as classes de softwares NMS, APM e DCIM", estava presente o "Protocolo de Gerência". Esse descreve os procedimentos formais para o funcionamento de sistemas de gerência, baseado não apenas no protocolo em si, mas também em todos os padrões e normas anteriormente definidos, como a árvore de nomes da ISO, a organização das OID's, o padrão ASN.1, a MIB-II e a arquitetura de sistemas de gerência. O nome do protocolo mais usado e famoso na área é SNMP (Simple Network Management Protocol - Protocolo de Gerência de Redes Simples), tendo sua primeira versão definida pela RFC 1157 [26], contendo apenas 36 páginas. A segunda versão (SNMPv2) está descrita pela RFC

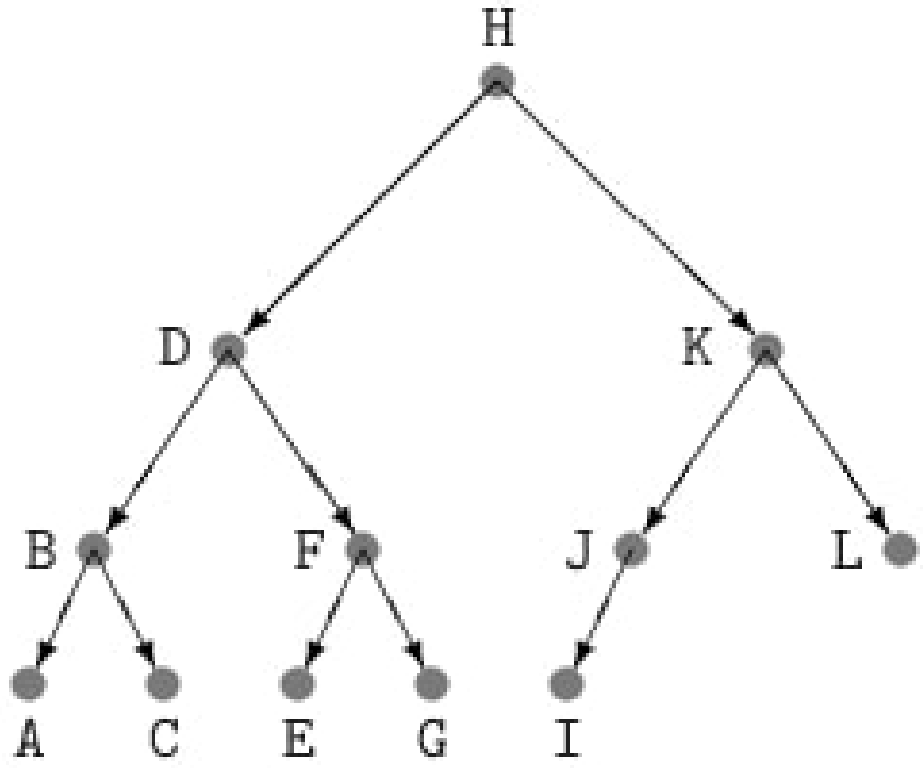

Figura 2.14: Exemplo de estrutura que satisfaz os critérios de uma árvore AVL (P. Feofiloff,2018) [12].

3416 [53] e a terceira versão (SNMPv3) está descrita pela RFC 3414 [54], contendo 88 páginas. É interessante notar não apenas a quantidade de páginas, mas também o número de RFC's suplementares: a primeira versão era baseada em 4 RFC's, a segunda, em 16 desses documentos técnicos, e a terceira, atualmente, em 20 RFC's. Somente destas observações e das menções ao nome do protocolo nos outros tópicos da seção "Fundamentação Teórica e Estado da Arte", é possível inferir a importância deste para as redes atuais. De fato, o próprio nome do modelo de trabalho, ou framework, de gerência padrão, vem do protocolo: "Simple Network Management Protocol (SNMP) Framework". A seguir, será abordada de forma breve a história por trás do protocolo, e posteriormente, as definições formais que compõem a base de funcionamento do protocolo.

Em 27 de Outubro de 1980, ocorreu um problema num dos gateways de dados (precursores dos roteadores) da rede ARPA, inutilizando o envio de mensagens. O caso todo está muito bem descrito na RFC 789 [55], que não tem valor normativo ou técnico, apenas histórico. Quando a falha aconteceu, a primeira atitude foi de investigação da rede, entretanto, é interessante notar que tal trabalho poderia se tornar inviável se, antes da falha, a rede já tivesse crescido para milhares localidades. Esse evento trouxe novas discussões para questões sobre como detectar falhas e gerenciar tais redes. Logo depois, o mundo viu um crescimento exponencial de organizações conectadas, e a gerência, que antes era apenas uma ideia promissora, de repente, virou necessidade urgente. Foi concebido, então, em novembro de 1987, o protocolo SGMP (Simple Gateway Monitoring

Protocol - Protocolo de Monitoramento de Gateway Simples), definido na RFC 1028 [56]. Pouco tempo após, em maio de 1990, foi publicada a RFC 1157, referente à primeira versão do SNMP, abrangendo de forma mais geral qualquer dispositivo de rede. Inicialmente, pretendia-se que este fosse usado apenas de forma provisória, enquanto outros protocolos mais completos fossem especificados. Um desses candidatos foi o CMIP (Common Management Information Protocol: Specification - Protocolo de Gerência de Informação Comum: Especificação), o qual entrou até mesmo para a indicação técnica X.711 da ITU-T [57] como padrão. Tinha muitas capacidades e era bem mais versátil que o próprio SNMP, contudo, as redes da Internet baseadas na pilha TCP/IP não o adotaram. O SNMP permaneceu como padrão, se espalhando rapidamente pelo mundo e universalizando as possibilidades e arquiteturas de gerência de redes, conforme descritas na seção ”Gerência de Redes e as classes de softwares NMS, APM e DCIM”. Muitos pesquisadores creditam o sucesso do protocolo à facilidade de implementação com uso baixíssimo de recursos e universalidade das estruturas básicas de dados. Dali em diante, surgiriam outras necessidades tais como automação e segurança, as quais convergiriam a gerência para o lançamento das RFC's das versões 2 e 3 do SNMP em 2002. No entanto, na prática, verifica-se ainda um uso muito mais expressivo do SNMPv1 pelo mundo, usos isolados e bem específicos de SNMPv3, principalmente pelas vantagens nas implementações de segurança, e o SNMPv2 atuando majoritariamente como coadjuvante das outras duas versões. Note-se que a coexistência entre as três versões é prevista na RFC 3584 [58].

Sobre o funcionamento técnico do protocolo, em primeiro lugar, é suficiente dizer que todos os conceitos, elementos e a arquitetura abordados no tópico ”Gerência de Redes e as classes de softwares NMS, APM e DCIM” são parte da especificação do SNMP, afinal, o framework de gerência se baseia no mesmo. Porém, de forma específica, seu funcionamento se dá sobre o protocolo da Camada de Transporte da pilha TCP/IP chamado UDP, descrito de forma oficial na RFC 768 [59]. Esse protocolo se caracteriza pela sua simplicidade implícita: não é prevista criação de conexão, nem armazenamento de estados, ou ainda controle de tráfego, e sequer confirmação de entrega. A única ”garantia” que esse protocolo provê é a taxa de envios, e mesmo nesse caso, essa taxa é dependente de outros fatores tais como as limitações de processamento do dispositivo e/ou programas da Camada de Aplicação da pilha TCP/IP. Também existe a necessidade de endereçamento fixo na Camada de Rede da pilha TCP/IP, ou o uso de outros serviços com resolução de nomes. O SNMP foi criado, inicialmente, para gerência de redes locais, portanto, mudanças de endereços de agentes ou gerentes sem quaisquer serviços de tradução de nomes (DNS - Domain Name Service - Serviço de Nomes de Domínio) podem inviabilizar a gerência. Serviços DNS são responsáveis por traduzir um endereço tal como ”agente1.organizacao.com” para o endereço IP do dispositivo alvo, no entanto, sem esses serviços, o gerente ficará impossibilitado de contatar agentes quando estes mudarem de IP. De forma complementar, se o gerente muda de endereço, e não existe DNS, os agentes que enviarem alertas de forma assíncrona também não conseguirão contatá-lo. Logo, se esse protocolo não provê nenhuma garantia ou qualidade de serviço, além de ser orientado a endereçamento IP puro da Camada de Rede (ao invés de dispor de códigos identificadores únicos e auto descobertas, por exemplo), por que basear algo tão importante como a

gerência da rede nele? A leitura atenta da RFC 1157 permite identificar quatro principais aspectos vantajosos do projeto:

1. O desenvolvimento de software necessário para suportar o protocolo SNMP é pouco oneroso para fabricantes;
2. O uso leve de recursos permite que todos os dispositivos e elementos necessários sejam monitorados com o menor impacto possível na performance da rede;
3. A simplicidade no funcionamento do protocolo impõe poucas regras para a forma e sofisticação dos sistemas de monitoramento;
4. A facilidade e simplicidade (principalmente pelo uso de OID's muito bem referenciadas) torna fácil a compreensão e aperfeiçoamento dos operadores no uso do protocolo.

Sobre a estrutura dos pacotes de dados, o protocolo UDP usa campos bastante simples devido sua especificação pouco restrita, como visto na figura 2.15. Formada na Camada de Aplicação da

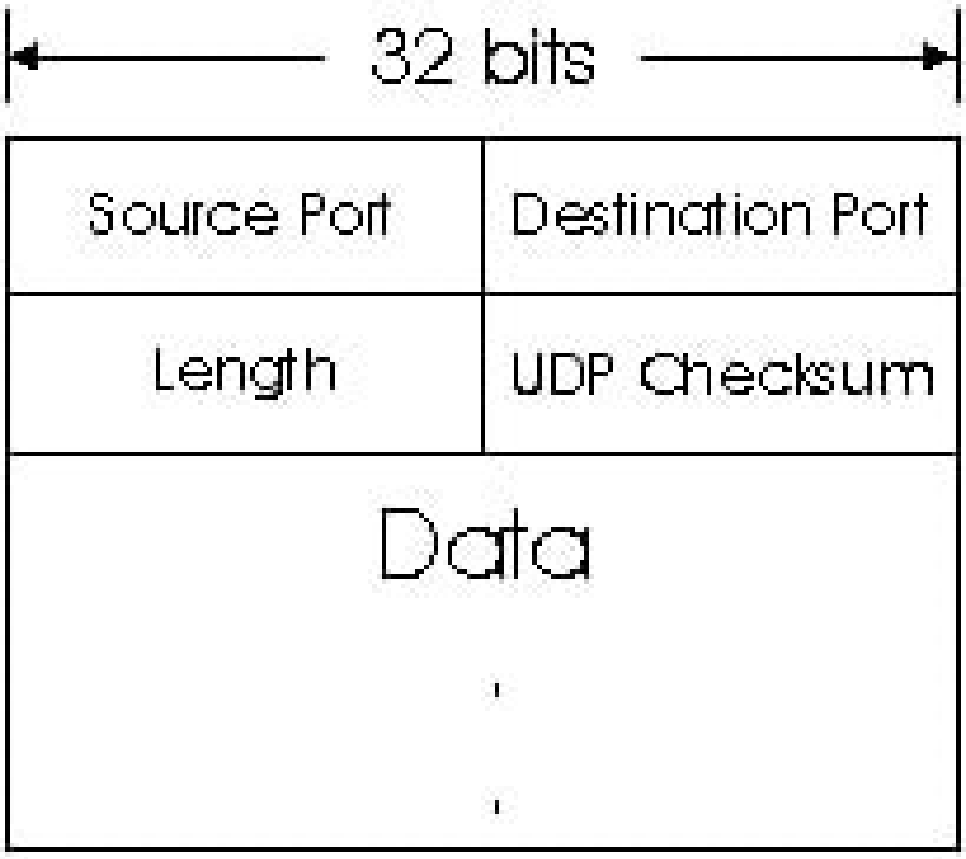

Figura 2.15: Estrutura básica de um segmento UDP (K. W. Ross e J. F. Kurose,2000) [13].

pilha TCP/IP, uma mensagem SNMP é composta por três partes principais:

Version: A versão do SNMP correspondente à PDU. Para o caso da primeira versão, é o número ”0”.

Community name: Uma palavra com até 255 caracteres que serve como ”chave” para identificar o grupo de acesso. Pode ser qualquer palavra, porém, é comum que os fabricantes atribuam apenas o termo ”public”, denotando livre acesso.

PDU: Protocol Data Unit - Unidade de Dados de Protocolo. Compreende a parte da mensagem SNMP na qual o protocolo envia as informações relevantes para os trabalhos de gerência do protocolo.

O protocolo SNMP, portanto, tem sua própria estrutura de informações com campos muito bem definidos. O nome dessas estruturas é PDU (Protocol Data Unit - Unidade de Dados de Protocolo) e elas são formadas na Camada de Aplicação da pilha TCP/IP. Uma vez formada uma PDU, ela é encapsulada pelo próprio protocolo SNMP acrescentando os campos ”Community” e ”Version”. Depois, a mensagem SNMP é tratada pelo protocolo UDP na Camada de Transporte e enviada às próximas camadas da pilha TCP/IP para transmissão. Aqui, fica clara a importância do uso do ASN.1: o UDP não realiza qualquer operação sobre os dados, logo, se plataformas com representações de dados diferentes tentassem se comunicar, os dados recebidos seriam mal interpretados. Contudo, como o SNMP sempre envia mensagens com o mesmo formato e tipos de dados padronizados independentemente da plataforma, essa dificuldade se torna transparente para o restante das camadas, de fato, se torna transparente para qualquer sistema operacional, hardware e meio de transmissão. Apesar de reiterar mais de uma vez que o projeto não pretende restringir as possibilidades exploradas em qualquer projeto de monitoramento, as PDU’s devem ser, obrigatoriamente, de um dos cinco tipos definidos na RFC 1157, sendo eles:

Get-request: É enviado de um dispositivo para outro para requisitar um ou mais dados de gerência.

Get-next-request: É enviado de um dispositivo para outro para requisitar dados sequenciais. Ou seja, o primeiro pedido é sempre do tipo ”get-request”, e do segundo em diante, são enviadas mensagens do tipo ”get-next-request”. Em geral, o resultado é a solicitação de uma tabela de dados da MIB.

Get-response: Esse tipo de mensagem é enviada como resposta do agente de um elemento gerenciado que recebeu um dos outros tipos de mensagens SNMP (”get-request”, ”get-next-request” e ”set-request”).

Set-request: Essa mensagem é a única que representa um comando, e não uma requisição. Ela é usada para atribuir/alterar dados de variáveis diretamente na MIB do elemento gerenciado.

Trap: Todos os outros tipos de mensagens necessariamente seguem um ritual sequencial de envio, baseado na ideia de ”pedido-resposta”. Esse tipo de mensagem, no entanto, é assíncrona, por isso o nome, que na língua Portuguesa significa ”armadilha”. O agente dentro do

elemento gerenciado, ao perceber alguma situação de alerta ou evento significativo, envia de imediato uma mensagem do tipo ”trap” para o gerente.

Agora, sobre a estrutura do campo PDU da mensagem SNMP para os tipos ”get-request”, ”get-next-request”, ”set-request” e ”get-response”, esse é composto pelos subcampos:

PDU Type: Esse campo é importantíssimo e determina qual o tipo da PDU, e portanto, o que ela significa. Respectivamente: ”get-request” recebe o valor ”0”, ”get-next-request” recebe ”1”, ”get-response” recebe ”2” e ”set-request” recebe ”3”.

Request ID: Campo contendo o número da requisição associada. Por exemplo, uma mensagem ”get-response” conterá um valor para o campo ”request-id”, e portanto, a subsequente mensagem ”get-response” conterá o mesmo número, identificando o fluxo de comunicação.

Error-status: A função básica desse campo é indicar se existe, ou não, uma falha associada ao fluxo de dados do SNMP para aquele número de solicitação (”request-id”) específico. Caso contrário, o valor do campo é zero.

Error-index: Para o caso de haver falhas (ou seja, se o campo ”error-status” for diferente de zero), esse campo pode enviar códigos de identificação de falhas. Caso contrário, o valor do campo é zero.

Variables: Esse campo é uma lista de argumentos armazenados na MIB. O preenchimento deste dependerá do tipo da PDU: se for uma mensagem de requisição de dados, como ”get-request” ou ”get-next-request”, ela apenas conterá a especificação das variáveis sendo requisitadas; por outro lado, se a mensagem for do tipo ”get-response” ou ”set-request”, o campo conterá a identificação da variável da MIB e seu valor.

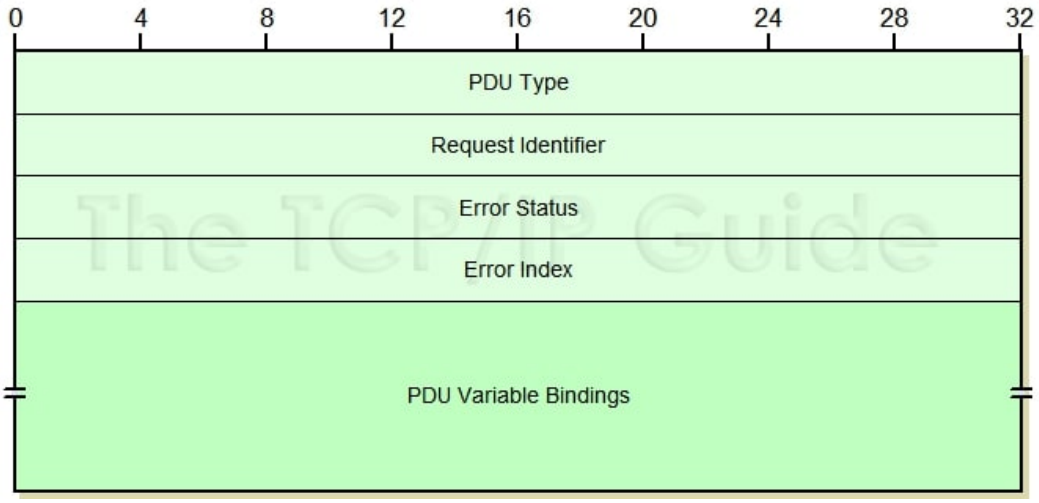

Figura 2.16: Campos e estrutura geral de uma PDU dos tipos ”get” ou ”set” do SNMPv1 (C. M. Kozierok,2005) [14].

De forma complementar, a estrutura do campo PDU da mensagem SNMP para o tipo ”trap” é composto pelos subcampos:

PDU Type: Tem a mesma função do campo dos outros tipos de mensagens SNMP, ou seja, especifica o tipo da PDU. No caso, para mensagens ”trap”, o valor será ”4”.

Enterprise: Esse campo carrega um identificador do elemento, em geral, o valor da variável ”sysObjectID”, que é o mesmo que uma OID que identifica o tipo/fabricante do dispositivo.

Agent-addr: Endereço IP do agente o qual está gerando a mensagem ”trap”.

Generic-trap: Por ser um tipo especial de mensagem SNMP, o tipo ”trap” tem subtipos, e esse campo identifica qual tipo de ”trap” está sendo enviada. A seguir, uma lista desses tipos baseando-se no SNMPv1:

1. ColdStart (valor ”0”), significa que o elemento que enviou a mensagem ”trap” está efetuando ”reset” de configurações, de forma que as definições de agente podem ser alteradas.
2. WarmStart (valor ”1”), significa que o elemento que enviou a mensagem ”trap” está reinicializando, de forma que as definições de agente não serão alteradas.
3. LinkDown (valor ”2”), significa que o elemento que enviou a mensagem ”trap” reconhece falha de comunicação em um dos links configurados para gerência.
4. LinkUp (valor ”3”), significa que o elemento que enviou a mensagem ”trap” reconhece que um dos links configurados para gerência voltou a apresentar conexão (ou seja, em algum momento no passado esteve em falha e voltou ao normal).
5. AuthenticationFailure (valor ”4”), significa que o elemento que enviou a mensagem ”trap” recebeu uma mensagem SNMP a qual não foi propriamente autenticada (por falha no campo ”community”, por exemplo).
6. EgpNeighborLoss (valor ”5”), servia para indicar que um nó vizinho usando o protocolo EGP (Exterior Gateway Protocol - Protocolo de Gateway Externo) o qual tinha relacionamento com o nó que enviou a mensagem ”trap” não está mais alcançável, e por isso, a associação não está ativa. Atualmente, o protocolo EGP está obsoleto, sendo o padrão da Internet baseado no BGP (Border Gateway Protocol - Protocolo de Gateway de Borda).
7. EnterpriseSpecific (valor ”6”), significa que o elemento que gerou a mensagem ”trap” reconhece o tipo dela como um evento específico do fabricante, o qual é especificado no campo ”specific-trap”.

Specific-trap: Para o caso de um tipo de mensagem ”trap” personalizada, definida pelo fabricante, a identificação dela deve ser posta neste campo.

Time-stamp: O tempo, em segundos, desde que o sistema que gerou a mensagem ”trap” foi inicializado pela última vez.

Variables: Mesmo uso dos outros tipos de PDU’s SNMP, ou seja, uma lista de variáveis. No caso, a lista contém os identificadores e os valores dos objetos. Porém, deve-se notar que a RFC

1157 esclarece que esse campo deve ser usado conforme a aplicação, ou seja, diferentemente dos outros tipos de PDU's, a do tipo "trap" foi pensada de forma mais flexível.

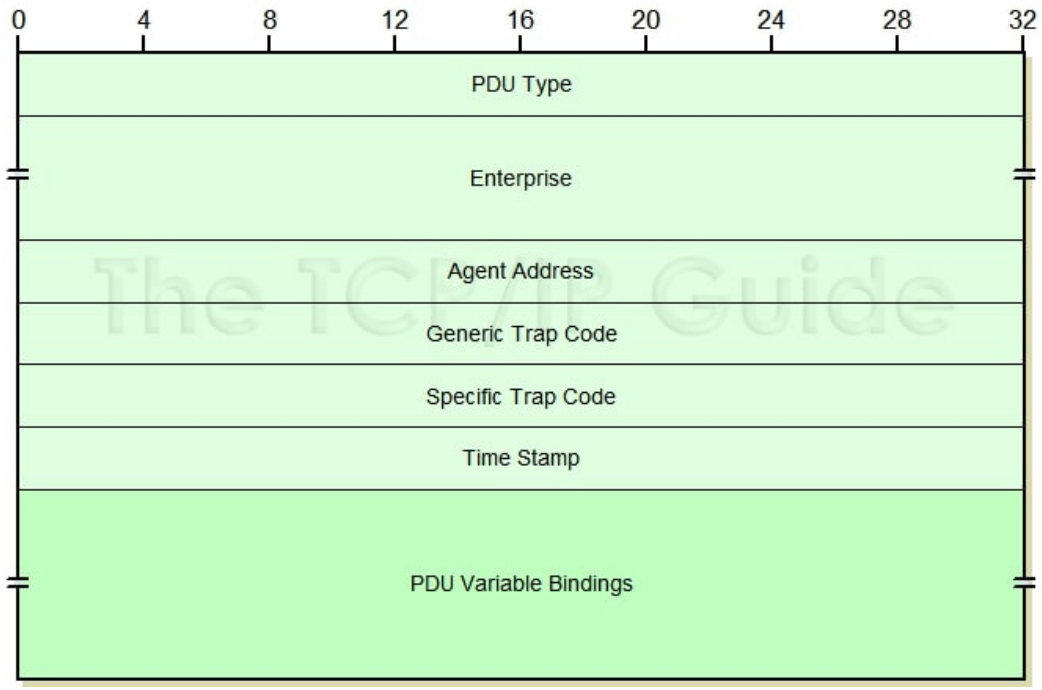

Figura 2.17: Campos e estrutura geral de uma PDU dos tipos 'trap" do SNMPv1 (C. M. Kozierok,2005) [15].

Após especificar os campos e formatos das mensagens SNMP, na figura 2.18, é possível ver um diagrama do funcionamento do protocolo SNMP. Note-se que, apesar de não ser orientado à conexão, o fluxo de conversação do protocolo é extremamente bem definido, bem como a hierarquia entre os elementos constituintes da estrutura da aplicação. Todavia, também é possível perceber, da análise diagrama e dos campos das PDU's especificados, uma limitação do SNMP: este foi concebido principalmente para funcionamento em redes locais, e não em redes distribuídas. Ocorre que a maioria dos dispositivos que acessam outras redes que não a que estão conectados passam por algum serviço de NAT (Network Address Translator - Tradutor de Endereços de Rede), e nesses casos, ficam "invisíveis" para as outras redes, já que seus endereços são traduzidos. Em situações como essa, um agente não consegue contatar diretamente seu gerente que esteja sendo traduzido por um NAT para envio de uma mensagem "trap", por exemplo, assim como um gerente não consegue contatar seus agentes que estejam sendo traduzidos por um NAT para fazer qualquer requisição de dados. De modo geral, quando um dos lados está sendo traduzido por um NAT, o outro não conseguirá iniciar a comunicação, apenas respondê-la (como mostra a figura 2.20), e se os dois lados estiverem sendo traduzidos por NAT's, então não é possível que qualquer um deles tome a iniciativa do processo de comunicação sem algum agente intermediador.

Apesar de o projeto do SNMPv1 parecer bastante completo e simples, a popularização das redes de comunicação acabou revelando que algumas das funções do protocolo logo estariam obsoletas e/ou seriam insuficientes para a gerência das infraestruturas. Em primeiro lugar, a quantidade de informações de interesse para monitoramento crescia exponencialmente, e em segundo, a

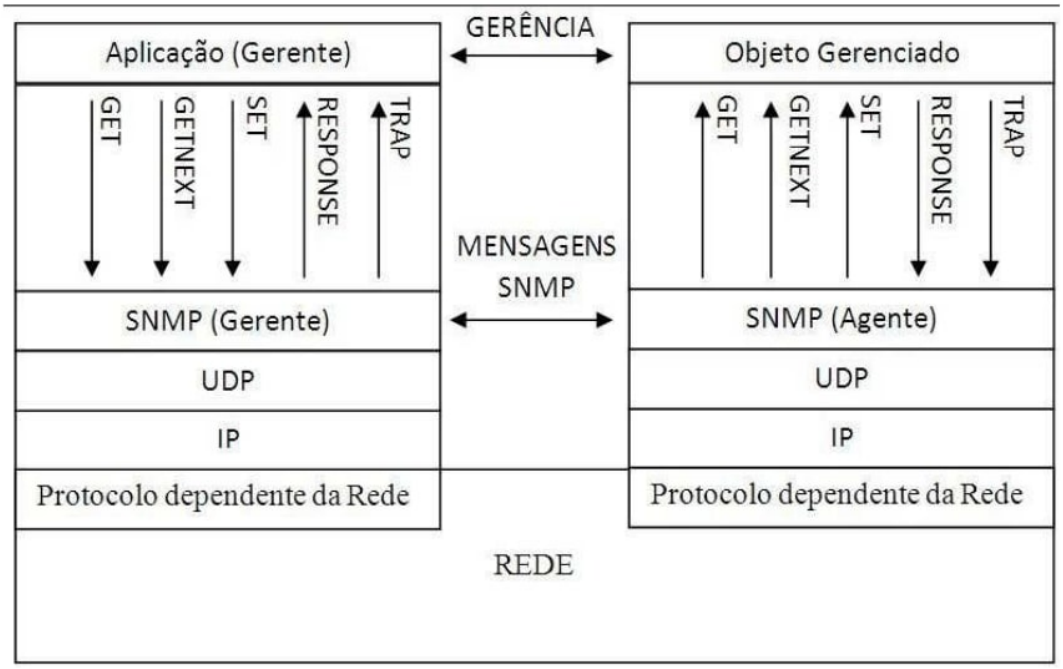

Figura 2.18: Esquema geral do funcionamento do protocolo SNMPv1 (CooperaTI,2019) [16].

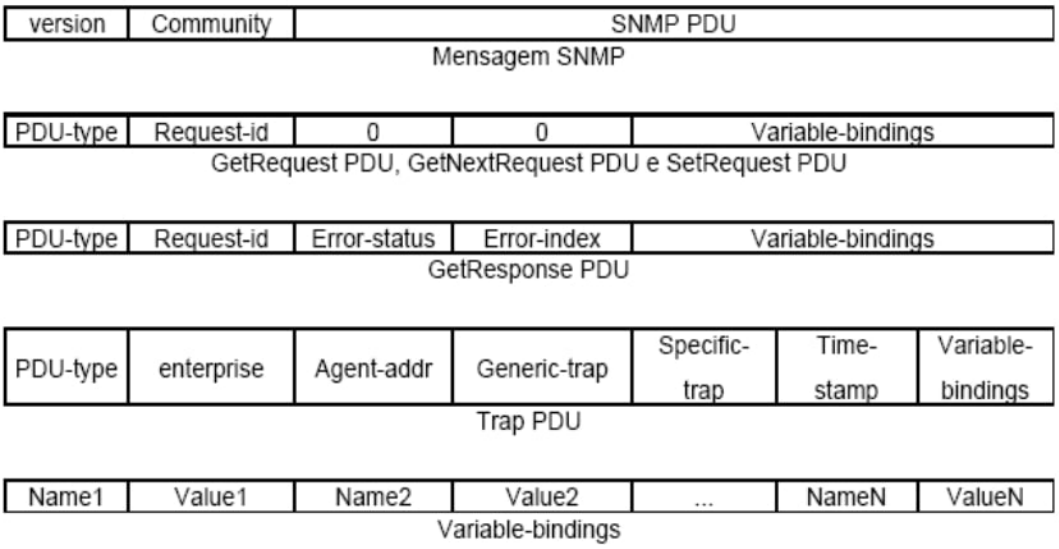

Figura 2.19: Resumo ilustrando todos os campos e tipos de mensagens do SNMPv1 (CooperaTI,2019) [16].

necessidade de gerências distribuídas e novos tipos de dados logo seria realidade. Portanto, a segunda versão do SNMP trouxe novidades para resolver esse problemas, e entre as mais relevantes, cita-se:

Bulk-requests: O SNMPv2 trouxe um tipo de mensagem específico para a recuperação de grandes quantidades de dados de MIB's, satisfazendo a necessidade de gerência de equipamentos e tecnologias cada vez mais complexas como os firewalls e roteadores de borda da Internet, aqueles com a maior quantidade de tráfego.

Inform-request: O SNMP sempre funcionou de forma centralizada em um gerente. Nunca

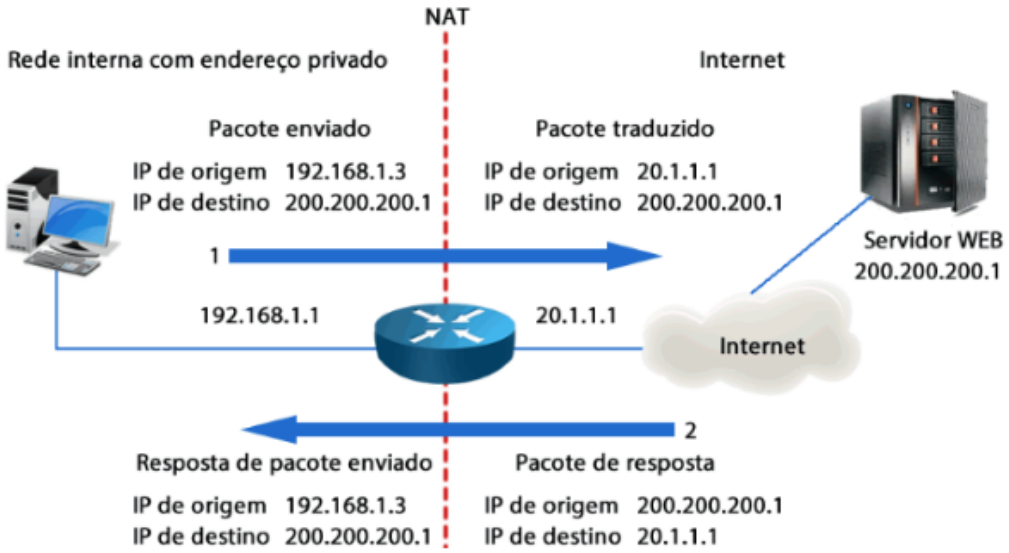

Figura 2.20: Ilustração do funcionamento de um NAT (D. A. Santos e L. Silva,2019) [17].

houve qualquer impeditivo para que dois ou mais gerentes trabalhassem simultaneamente, porém, não existia qualquer previsão de troca de dados entre eles. As novas mensagens do tipo ”inform-request” foram criadas justamente para possibilitar que gerentes conversassem, permitindo a criação de hierarquias e gerências distribuídas. Além disso, houve revisão das variáveis da MIB de dispositivos de redes.

As duas melhorias expostas não são as únicas: um novo tipo de dado (”Counter64”), novos códigos de erros, geração de códigos de exceção, modelos de notificações, novos tipos de PDU’s, novo tipo de mensagens ”trap” (comumente chamado ”Trapv2”), entre outros. Contudo, para a finalidade deste trabalho, é suficiente notar as duas principais mudanças expostas. Isso porque elas provam o quanto o escopo de atuação do protocolo evoluiu, passando de um ”simples” sistema de mensagens estruturadas para um grande padrão de indústria, devendo ser capaz de atender quaisquer tecnologias e interesses da gerência, não importando a quantidade de dados, a distribuição geográfica, o uso de tecnologias proprietárias ou mesmo a hierarquia de elementos gerenciados e gerentes que se queira/necessite projetar.

Um último passo ainda permanecia sem aderência: as implementações de segurança. Ainda que o SNMPv2 tenha tido algumas especificações e previsões, na prática, ele foi usado com o mesmo nível de segurança da primeira versão. Sendo, portanto, os critérios mínimos de segurança uma necessidade crescente, a terceira versão do protocolo foi concebida. O SNMPv3, em sua totalidade, consegue proporcionar controle de acesso às variáveis da MIB, proteção contra modificações de informação, contra uso falso de identidades, contra duplicação de mensagens, atraso destas, e ainda provê confidencialidade para os dados da MIB sendo enviados. É interessante notar que o protocolo consegue, com sucesso, implementar diversas abordagens de segurança sem que pra isso tenha que abandonar o uso do UDP e trabalhar orientado à conexão.

A especificação do SNMPv3 é bastante modular e apresenta uma visão de alto nível do projeto. Isso porque entendeu-se ser interessante a definição de módulos, assim, o desenvolvimento do protocolo poderia dar-se sem a necessidade de lançamento de novas versões. As imagens 2.21 e 2.22 mostram, respectivamente, um diagrama resumindo o funcionamento do SNMPv3 no gerente e no agente. Note-se que existem dois módulos que implementam funções de segurança e autenticação. É neles onde se verificam os conceitos de USM (User-based Security Model - Modelo de Segurança Baseado em Usuário) e VACM (View-based Access Control Model - Modelo de Controle de Acesso Baseado em Visão).

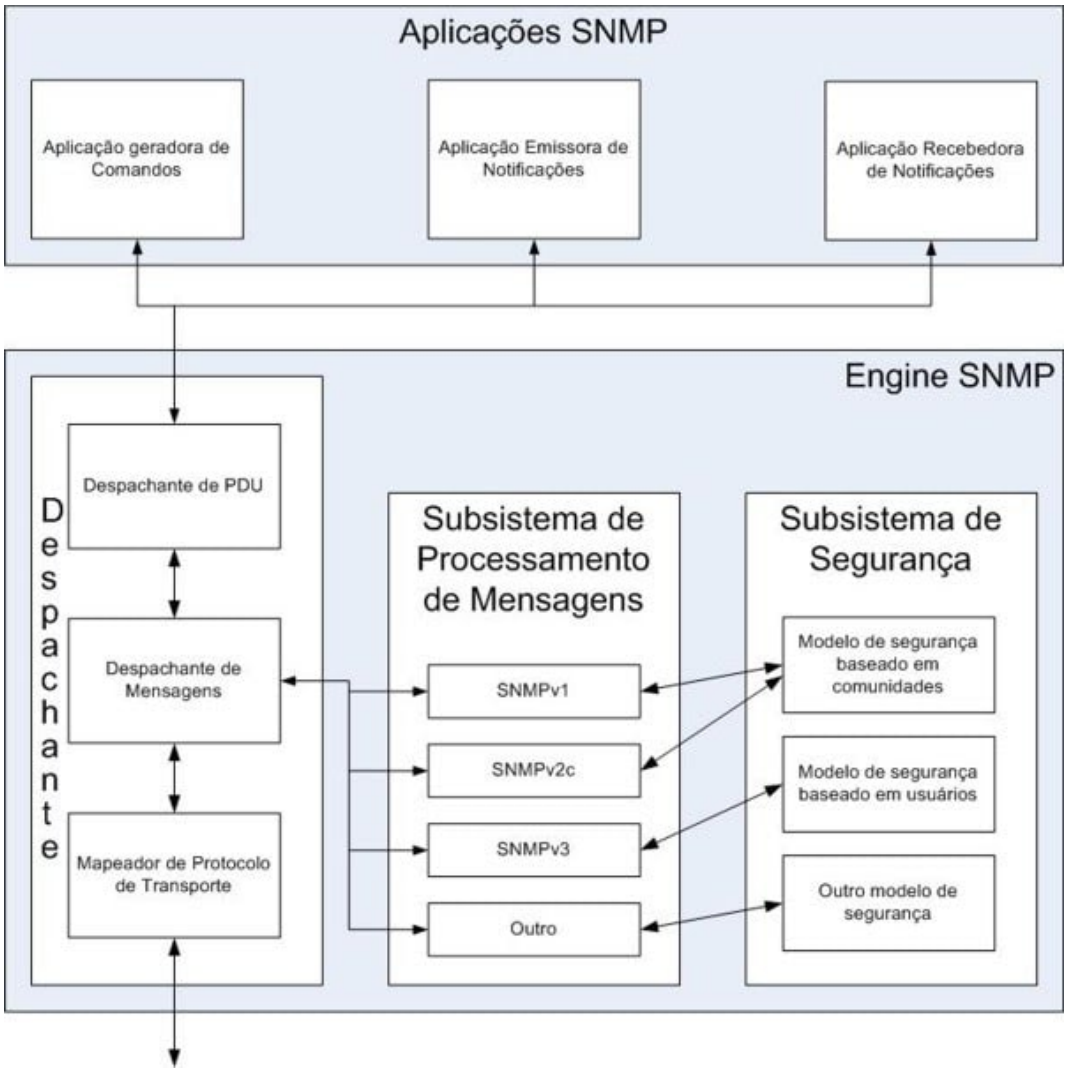

Figura 2.21: Resumo do funcionamento de um gerente segundo o SNMPv3 (H. Fassi,2008) [18].

O USM prevê que a MIB de um dispositivo é protegida, e que cada usuário precisa de chaves próprias de autenticação e privacidade. Essas chaves não estão armazenadas na MIB e não podem ser acessadas/modificadas usando mensagens do tipo ”get” ou ”set”, Na verdade, se tratam de usuários e senhas cadastrados no próprio dispositivo/elemento gerenciado. O USM também define um processo de descoberta entre gerente e elemento gerenciado, de forma que o gerente possa ter acesso autorizado às variáveis da MIB e conheça a chave simétrica secreta que o per-

mita descriptografar as PDU's. O SNMPv3 também trouxe campos novos para o cabeçalho, os quais lidam com informações de controle e segurança e não entram no processo de encriptação. Adicionalmente, no SNMPv3, a PDU é chamada de "scopedPDU", ou seja, ela tem um "escopo" definido. Esse escopo é assim chamado porque a PDU envia informações que fazem parte de um contexto, no qual determinadas informações gerenciais estão disponíveis para determinadas entidades.

O VACM, assim como o USM, provê serviços de autenticação. Contudo, diferente do USM, no qual o controle é definido a cada usuário, no VACM, usuários fazem parte de grupos e suas políticas. A RFC 2275 [60] especifica o esquema de políticas de segurança para grupos no SNMP. Em suma, os direitos de acesso e/ou modificação de variáveis são dados a diferentes grupos, os quais os exercem em contextos diferentes, que são agregações de objetos em coleções baseadas na política de acesso. Dessa forma, ao enviar uma requisição, o usuário será autenticado e poderá ter acesso de leitura/escrita somente na "visão da MIB" permitida para seu grupo, com uma quantidade de objetos diferente da MIB completa e com possibilidades de interação totalmente preestabelecidas. Por fim, a finalidade deste tópico não é comparar as versões do protocolo SNMP

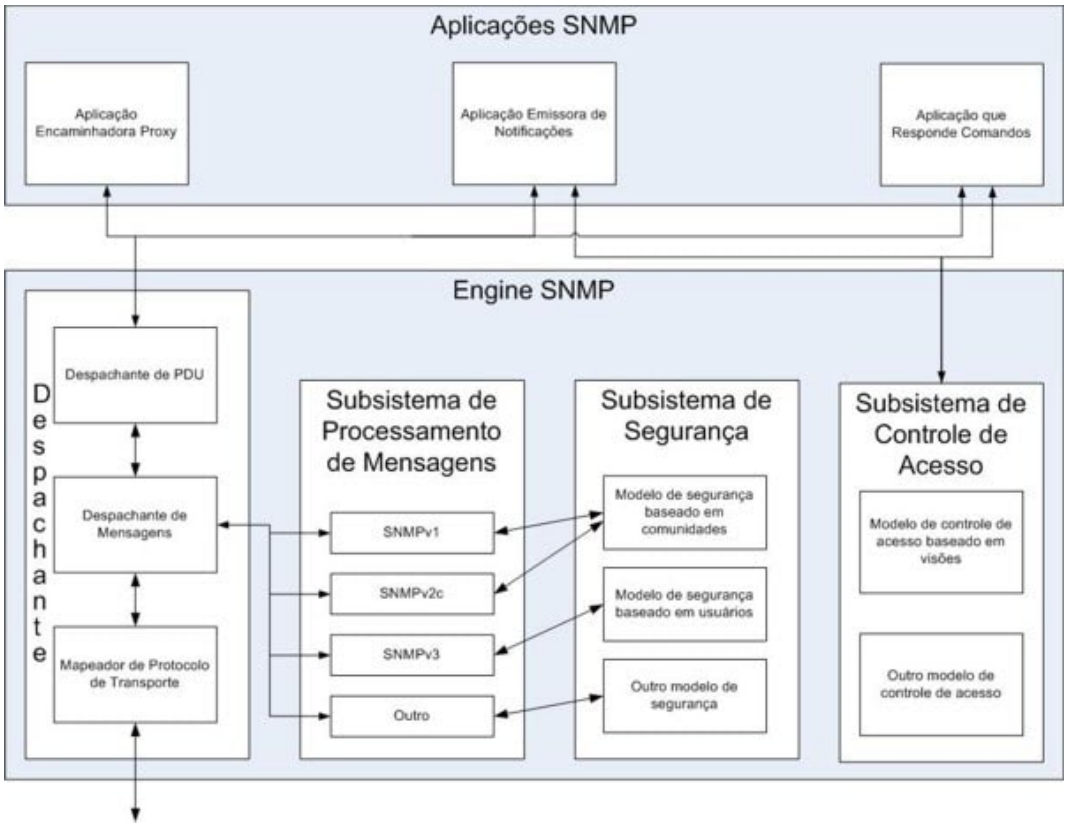

Figura 2.22: Resumo do funcionamento de um agente segundo o SNMPv3 (H. Fassi,2008) [18].

para eleger o melhor, afinal, nem as RFC's citadas indicam que determinada versão esteja obsoleta ou não deva ser mais usada. De forma totalmente contrária, são várias as citações sobre a coexistência das três versões e de suas diversas distribuições. O objetivo, portanto, era a apresentação das características fundamentais do protocolo de gerência padrão das redes TCP/IP e de

sua evolução, mostrando ser esse um projeto maduro e capaz de ser aplicado em diversos contextos de gerência de dispositivos e monitoramento, oferecendo de forma garantida performance, facilidade de implementação, integração de diferentes plataformas, gerência distribuída e padrões estabelecidos de segurança.

Tendo especificado o protocolo SNMP, o tópico a seguir introduzirá os conceitos gerais de microcontroladores e suas vantagens para uso em tarefas muito bem determinadas, como monitoramento e supervisão.

2.8 MICROCONTROLADORES

As proposições do projeto desse trabalho basear-se-ão no uso de microcontroladores. Dispositivos microprocessados estão presentes nas mais diversas aplicações, tais como fábricas, montadoras, aviação, indústria aeroespacial, sensoriamento, entre diversos outros. Contudo, antes de abordá-los mais detalhadamente, é interessante entender a história desses circuitos. Este tópico percorrerá a história dos microcontroladores e fundamentará as vantagens que tornam seu uso tão universal, mostrando, ao fim, serem ótimas ferramentas para as aplicações de gerência de infraestruturas.

As primeiras aplicações da Eletrônica baseavam-se em circuitos analógicos com componentes de respostas contínuas (não discretizadas), como resistores e capacitores. A necessidade, no entanto, de dispositivos que permitissem o ”controle” do fluxo de corrente elétrica fizeram a eletrônica convergir para o uso das válvulas termiônicas, ou simplesmente válvulas. Esses dispositivos continham três terminais, de forma que uma corrente elétrica seria percebida num deles se houvesse diferença de potencial (e, portanto, corrente) entre os outros dois terminais. Após a válvula, os

Figura 2.23: Vários exemplos de válvulas termiônicas, os dispositivos que faziam o papel dos transistores (S. Riepl,2008) [19].

transistores e diodos ganharam as cenas. Dispositivos baseados nas teorias de interação entre junções de metais condutores e materiais semicondutores, a ampla disponibilidade desses componentes possibilitaram a fabricação em massa de circuitos discretizados, emulando as operações básicas da Álgebra Booleana (AND, OR, XOR, e assim por diante). A associação dos circuitos lógicos provenientes dessas montagens permitia a criação de funções lógicas mais complexas, as quais poderiam mapear entradas do circuito (por exemplo, sequência de terminais com tensão positiva e negativa) para saídas predeterminadas. Logo depois, seria apenas questão de tempo até que fossem desenhados circuitos capazes de resolver operações matemáticas simples, como determinar somas, subtrações, multiplicações, divisões, identificação de números negativos, entre outros. A evolução dessas montagens convergiu para os conceitos de circuitos combinacionais e sequenciais. Os circuitos combinacionais seriam aqueles nos quais existem portas lógicas de entrada e saída, e uma determinada entrada gera uma saída preestabelecida, que pode ser descrita por uma equação booleana. Os circuitos sequenciais, no entanto, empregam, além das portas lógicas, o uso de elementos chamados latches e flip-flops para armazenamento de estados, logo, sua saída depende não apenas das entradas, mas dos estados armazenados nesses elementos, que podem mudar a cada interação do sistema.

A evolução exponencial desses tipos de circuitos deu origem a projetos bem complexos, como circuitos codificadores/decodificadores, ALU's (Arithmetic Logic Unit - Unidade Lógica Aritmética), multiplexadores/demultiplexadores, conversores Analógico/Digital, entre outros. Outro aspecto importante da historia da Eletrônica para este contexto recai sobre a concepção das memórias EEPROM (Eletrically Erasable Programmable Read-Only Memory - Memória Somente-Leitura Programável Apagável Eletricamente). Antes, era um procedimento extremamente oneroso (seja pelos requisitos, seja pela demora) lidar com memórias reprogramáveis não-voláteis (ou seja, que conseguem manter os dados armazenados mesmo com falta de alimentação), porém, com a invenção e ampla produção das memórias EEPROM, apagar e gravar novos dados nessas era extremamente rápido e fácil. Esse possibilidade era condição essencial para que fossem concebidos sistemas reprogramáveis, os quais teriam uma lista de capacidades e poderiam realizar sequências de ações de forma autônoma, lendo sequencialmente os comandos armazenados nas ditas memórias EEPROM. Com a associação das ALU's, das memórias de alta velocidade (como registradores), dos circuitos de multiplexação, codificação, entre outros, tornou-se viável o projeto de CPU's (Central Processing Unit - Unidade de Processamento Central). Esses seriam circuitos extremamente complexos os quais teriam uma lista de instruções de máquina, e cada instrução determinaria uma operação realizada pela CPU sobre a entrada fornecida. A CPU, portanto, seria um projeto sem escopo inicialmente definido, no qual o objetivo seria fornecer uma ferramenta extremamente flexível e com suporte a múltiplas funções para serem usadas nas mais diversas aplicações. O caminho, portanto, estaria completo para o nascimento de um novo tipo de componente: associando CPU's, conversores Analógicos/Digitais, memórias EEPROM e programas de software, surgiram os primeiros microcontroladores, amplamente distribuídos por empresas como Texas Instruments e Intel. Portanto, fica fácil definir um microcontrolador: um elemento de hardware sem contexto definido com suporte a diversas instruções de máquina pre-

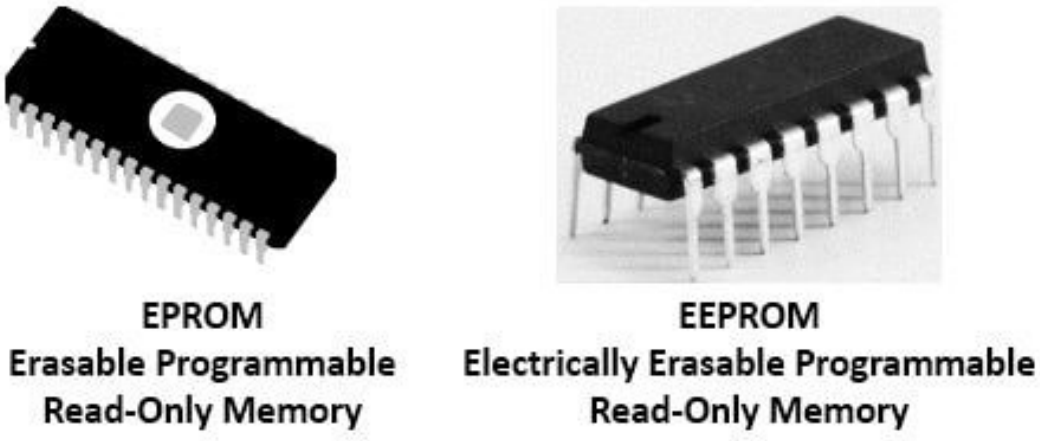

Figura 2.24: À esquerda, exemplo de EPROM, memória que só podia ser apagada com o uso de luz ultravioleta; à direita, exemplo de EEPROM, memória apagável eletricamente que revolucionou a Eletrônica (Tech Difference,2019) [20].

definidas e com um conjunto de portas analógicas e/ou digitais, o qual pode ser programado para executar tarefas sobre essas portas, possibilitando o controle de outros sistemas/componentes e/ou a integração deste com outros dispositivos. É importante lembrar que um microcontrolador não é um processador, já que o microcontrolador contém memórias programáveis e voláteis e vários outros componentes como portas e circuitos osciladores (geradores de clock), enquanto um processador é simplesmente uma unidade de processamento, necessitando de interface com outros componentes para formar um dispositivo completo, como uma placa mãe de um computador que liga um processador à memória, disco rígido, etc. Caracterizando, agora, sob um ponto de vista

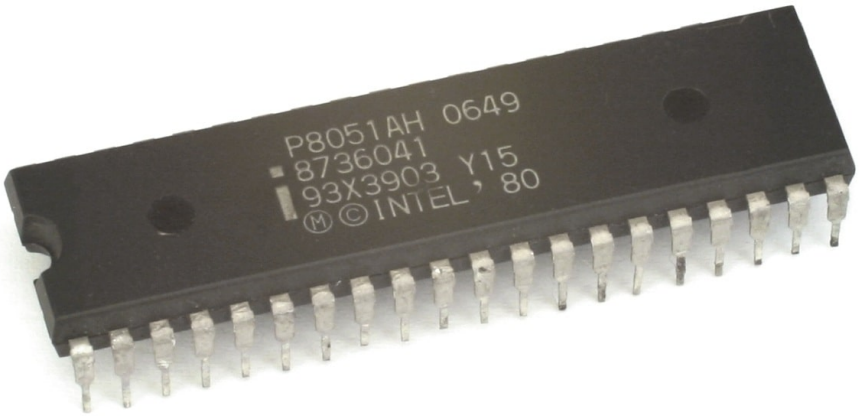

Figura 2.25: Foto de um dos primeiros microcontroladores amplamente distribuídos, o Intel P8051 (K. Lanzet,2008) [21].

de alto nível, o funcionamento dos microcontroladores, pode-se entender melhor o papel do software nestes. Ocorre que, como dito, microcontroladores dispõem de uma memória EEPROM, a qual pode ser apagada e reescrita através de comandos elétricos e que mantém dados mesmo após desligadas. Mas como separar o local onde estão gravadas as instruções de máquina (programa) e onde os dados de memória volátil estão armazenados? Esse conceito recai sobre a diferença das arquiteturas Von-Neumann e Harvard:

Von-Neumann: Nessa arquitetura, a memória deve ser a mesma para as instruções do programa e os dados deste, não devendo haver separação física. Porém, vale perceber que, se os dois estão na mesma memória, torna-se impossível acessar dados e instruções de forma simultânea, podendo haver a verificação de gargalos.

Harvard: Nesta arquitetura, propõe-se que existam pelo menos duas memórias: uma na qual estão as instruções do programa e outras na qual estão os dados. Assim, a CPU consegue acessar tanto as instruções quanto os dados de forma independente e simultânea.

A importância das arquiteturas descritas reside na forma como funcionam os microcontroladores: a maioria destes segue a arquitetura de Harvard. Diferentemente dos computadores pessoais, os quais têm grandes memórias e usam um misto das duas arquiteturas, os microcontroladores, em geral, dispõem de recursos limitados, portanto, é mais viável e flexível usar memórias diferentes para as instruções e os dados. O microcontrolador da imagem 2.25 funciona baseado na arquitetura de Harvard, ou seja, memória de dados e de instruções estão separadas. Mas e a velocidade? Por que os computadores pessoais são bem mais potentes e velozes que os microcontroladores? Em primeiro lugar, é importante entender que as CPU's atuais, seja dos computadores, seja dos microcontroladores, são máquinas síncronas, ou seja, cada operação ocorre após uma "batida de clock", que seria uma oscilação completa de um circuito com comportamento oscilatório bastante preciso. Isso não significa que o sistema necessariamente fica em espera entre cada batida, mas sim, que elas sincronizam as atividades da CPU. Portanto, a CPU mais veloz será aquela que consegue trabalhar em frequências maiores. Logo, sobre a diferença de velocidade citada entre computadores e microcontroladores, pode-se dizer que um computador pessoal é um sistema mais complexo no qual o objetivo é performance e agilidade em múltiplas tarefas, exigindo processamento de grandes massas de dados. Por esse motivo, atualmente, a maioria dos computadores funciona em frequências na ordem dos "GHz", ou seja, executando bilhões de operações por segundo. Diferentemente, os microcontroladores são dispositivos com recursos limitados concebidos para atuarem em escopos definidos de projeto. Logo, uma vez programados, espera-se que sempre executem a mesma tarefa para o qual o software foi planejado. Como esses elementos deveriam atuar no controle e supervisão de tarefas simples e repetitivas, não havia necessidade de disponibilização de recursos de processamento em demasia (o que os tornaria caros), portanto, a maioria dos microcontroladores disponíveis no mercado terão memórias para instruções limitadas na ordem dos "Kb", e quando muito, de alguns "Mb". Ainda, a maioria das aplicações nas quais os microcontroladores são usados envolve o acompanhamento e controle de processos e sinais físicos, os quais têm velocidades de ordem de grandeza relativamente baixa, por esse mo-

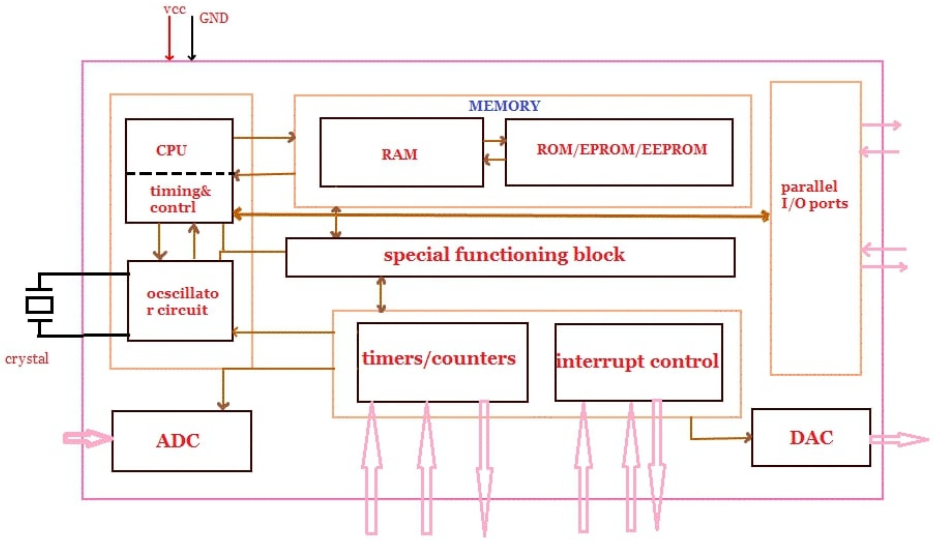

Figura 2.26: Estrutura básica que representa a maioria dos microcontroladores disponíveis (CircuitsToday,2018) [22].

tivo, a maioria dos dispositivos terá CPU's operando na ordem dos "MHz", ou seja, milhões de instruções por segundo, milhares de vezes menor que os computadores. Essa velocidade não é, porém, determinada simplesmente pela falta de necessidade de potência dos microcontroladores. De fato, velocidades da ordem de bilhões de operações demandam circuitos osciladores e componentes muito mais caros. Como dito anteriormente, uma CPU nada mais é do que um projeto extremamente complexo que associa um grande número de circuitos lógicos que trabalham no mundo digital, onde cada informação pode ser representada por números binários ("0" ou "1"), ou seja, pela presença/ausência de corrente ou não-nulidade/nulidade da tensão, por exemplo. Contudo, essa não é uma verdade universal para os circuitos: existem frequências a partir das quais os componentes passam a operar fora de sua normalidade, e o sistema deixa de funcionar. Para que um microcontrolador, portanto, funcione a frequências maiores, seria necessário substituir não apenas o circuito oscilador, porém todos os componentes e a própria CPU por outros de qualidade superior. Pode-se concluir, portanto, que os microcontroladores são mais simples e com menos recursos justamente para que possam ser implementados e projetados com custos baixos. Um fato adicional é que a maioria dos projetos com microcontroladores atuais seguem uma abordagem baseada em um funcionamento indefinido. Ou seja, o programa é projetado de forma que, tão logo o sistema seja ligado, este esteja sempre em um de dois estados possíveis: em espera ("idle") por algum fenômeno/entrada ou executando uma sequência de passos predefinida. Portanto, eles se tornam perfeitos para a realização de tarefas repetitivas. Ainda, existe o conceito de "interrupção", na qual o acontecimento de determinado evento pré-programado interrompe o

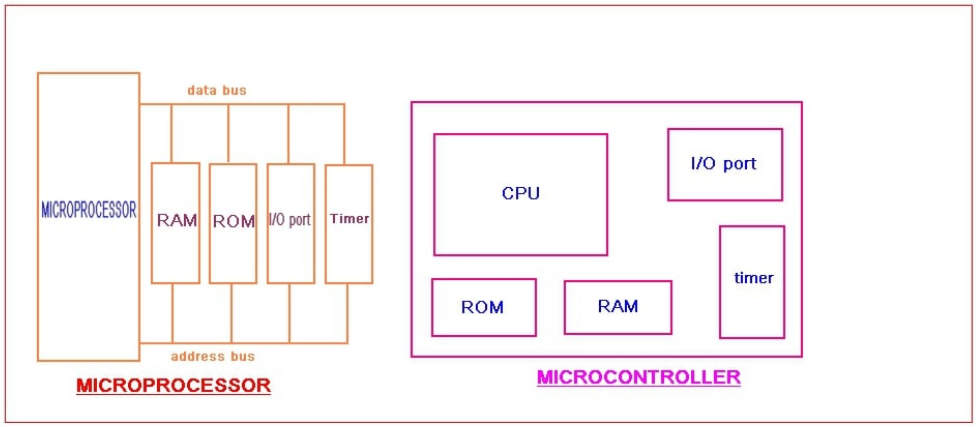

Figura 2.27: Diferença entre um processador e um microcontrolador (CircuitsToday,2018) [22].

microcontrolador e o leva e executar uma sequência de passos em resposta ao evento. Esse recurso é usado de forma larga nas aplicações de monitoramento e segurança.

O objetivo deste tópico era embasar brevemente os microcontroladores e seu funcionamento. Além disso, as diretrizes de projeto do SNMP, que exigem baixo consumo de memória, processamento e armazenamento, tornam o protocolo perfeito para implementação em microcontroladores. É uma conclusão desejada, portanto, a de que a associação de padrões robustos de gerência com tecnologias de baixo custo e fácil implementação, como microcontroladores, constitui o caminho para tornar viáveis tecnologias como IoT, *Smart grids*, prédios inteligentes, Indústria 4.0, Agricultura 4.0, entre vários outros.

A seguir, serão fundamentados os métodos de medição de variáveis de circuitos elétricos baseados nas teorias eletromagnéticas, concluindo as necessidades preliminares de fundamentação para este projeto.

2.9 O USO DE TRANSFORMADORES DE CORRENTE NA MEDIÇÃO NÃO-INVASIVA DE VARIÁVEIS EM CIRCUITOS ELÉTRICOS

Este tópico tratará a teoria eletromagnética por trás da medição indireta de variáveis de circuitos elétricos usando transformadores de corrente, aplicando, ao fim, seu uso na medição de potência e corrente em circuitos trifásicos, os mais comumente encontrados em instalações de infraestruturas e grandes motores, por exemplo.

De acordo com Sadiku (2010) [61], "Em 1831 [...], Michael Faraday, em Londres, e Joseph Henry, em Nova York, descobriram que um campo magnético variável no tempo poderia produzir uma corrente elétrica. De acordo com os experimentos de Faraday, um campo magnético estático não produz fluxo de corrente, mas um campo magnético variável no tempo produz uma tensão induzida (denominada força eletromotriz ou, simplesmente, fem) em um circuito fechado, o que causa um fluxo de corrente." Ainda segundo o texto, "Faraday descobriu que a fem induzida, Vfem (em volts), em qualquer circuito fechado, é igual à taxa de variação do fluxo magnético enlaçado pelo circuito." A citação faz menção à Lei de Faraday, definida por:

$$Vfem = -N\frac{d\Psi}{dt} \tag{2.1}$$

Nela, N é a quantidade de espiras no circuito e Ψ é o fluxo em cada espira. O sinal negativo indica que existe uma oposição entre a variação de fluxo e a tensão induzida, propriedade definida pela Lei de Lenz, porém não será impeditiva para o projeto, visto que a corrente medida será sempre convertida para valores positivos em software, para refletir em potências positivas. Na figura 2.28, uma imagem que demonstra o conceito geral da Lei de Faraday. É importante destacar, portanto, que um circuito pode ser visto como uma representação, mantidas as relações de proporcionalidade, do comportamento da corrente no outro circuito. Considerando, portanto, correntes em regime senoidal (correntes AC), como as que alimentam os sistemas num data center, conclui-se, por construção, que aplicando a Lei de Faraday, poder-se-ia medir indiretamente a corrente elétrica demandada por uma carga, e a partir daí, o cálculo aproximado da energia consumida se torna desimpedido, valendo-se da Primeira Lei de Ohm (Potência = Tensão $\times$ Corrente) e dos valores RMS, ou eficazes, das grandezas de corrente e tensão. Note-se que correntes e tensões típicas dos sistemas de fornecimento de energia têm regime senoidal e apresentam valores positivos e negativos no tempo, não sendo trivial, portanto, observar esses valores numa medição com circuitos simples. Na verdade, os valores a serem obtidos tratam-se de valores eficazes, ou seja, segundo Irwin (2003) [62], tomando-se por base uma corrente elétrica alternada periodicamente, o valor eficaz, ou RMS, é um valor constante de uma corrente elétrica contínua que forneceria a mesma potência no mesmo período de tempo. Logo, ao usar um sensor de corrente não invasivo (formado por um circuito adicionado de um transformador de corrente), a corrente medida (ou seja, aquilo que será tido por entrada para o sistema, a saída do circuito) será o valor eficaz dessa, não os valores diretos assumidos pelo sinal com natureza variável. Esse valor eficaz será referente à potência dissipada no circuito, potência essa que está correlacionada com a corrente

variável sendo gerada pelo sensor, o qual, por sua vez, será proporcional à corrente real do circuito alvo das medições. Logo, para se obter a corrente primária, apenas será necessário multiplicar a corrente secundária por um fator fixo, determinado pelo transformador do circuito, obedecendo à Lei de Faraday.

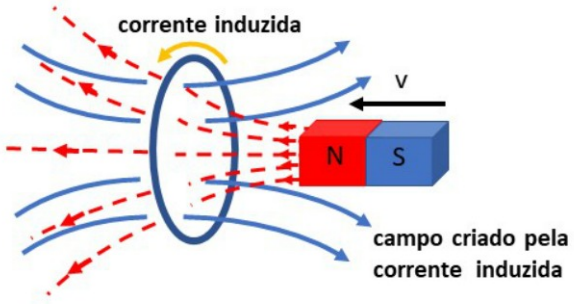

Figura 2.28: Ilustração da Lei de Faraday.

Tendo como base os conhecimentos descritos acima, Scherz-Monk (2016) [63], explana sobre transformadores de corrente. Segundo o texto, adaptado para português, transformadores de corrente são dispositivos especiais usados principalmente para medir grandes correntes, as quais seriam muito perigosas para se medir com um amperímetro. Eles são desenhados para prover uma corrente secundária que é proporcional à corrente primária fluindo pelo condutor alvo das medições. Esses transformadores são especificados pela relação entre a corrente primária, a medida, e a secundária, provida pelo dispositivo como saída (por exemplo, 400:5, ou 2000:1, como no caso do dispositivo que será usado nesse projeto). Na figura 2.29, um exemplo desse tipo de transformador e seu funcionamento. Finalmente, esses dados significam que, tomando como exemplo o sensor "SCT-013 100A:50mA" da marca YHDC [64], ao se medir 10mA na sua saída (corrente secundária), significará que a corrente primária é: $0.010 \times 2000 = 20$ Ampéres.

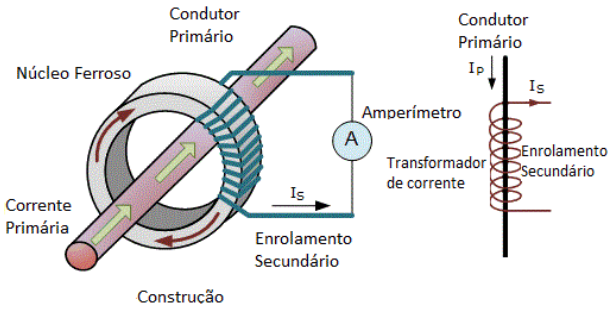

Figura 2.29: Exemplo de funcionamento de um transformador de corrente.

Um detalhe ainda necessita ser abordado: o cálculo e as medições em sistemas de uma (1) fase e três (3) fases. A escolha da medição do valor eficaz traz várias facilitações para o projeto sem

deixar de cumprir os objetivos. Segundo Irwin (2003) [62], sendo P a potência, Ief a corrente eficaz, ou RMS, e R, a resistência de um circuito simples com uma única fase, tem-se:

$$P = Ief^2 \times R \tag{2.2}$$

Também segundo Irwin (2003) [62], sendo "a", "b" e "c" as três (3) fases e P a potência, num circuito trifásico tem-se:

$$P(t) = Pa(t) + Pb(t) + Pc(t) \tag{2.3}$$

Logo, pode-se concluir que a potência num circuito trifásico pode ser calculada com as correntes eficazes medidas em cada fase:

$$P(t) = ((Ia)ef^2 \times Ra) + ((Ib)ef^2 \times Rb) + ((Ic)ef^2 \times Rc) \tag{2.4}$$

Portanto, basta apenas o uso de três (3) sensores de corrente não invasivos, um para cada fase, e poder-se-à realizar medições para sistemas trifásicos. Como a potência real e aparente também são componentes da potência dispendida no circuito, Irwin (2003) [62] também mostra que, sendo S a potência complexa, definida pela soma da parte real e imaginária desta, e sendo "a", "b" e "c" as três (3) fases:

$$S(t) = Sa(t) + Sb(t) + Sc(t) \tag{2.5}$$

Adicionalmente, circuitos trifásicos comumente contém um quarto condutor, denominado "neutro". Sobre a corrente de neutro (representada com letra "n"), tendo as três (3) fases "a", "b" e "c" a mesma intensidade de corrente fluindo (ou seja, num circuito perfeitamente balanceado), e considerando suas funções variantes no tempo e devidamente defasadas como num circuito trifásico, tem-se que, idealmente:

$$In = (Ia + Ib + Ic) = 0 \tag{2.6}$$

Por fim, é interessante notar que a medição de variáveis em circuitos elétricos é condição essencial para que uma correta gestão de infraestrutura seja realizada. Em primeiro lugar, em circuitos trifásicos, é possível verificar o balanceamento da carga nas três fases e na presença (e módulo) da corrente de neutro, que segundo Irwin (2003) [62], para um circuito balanceado, deveria ser nula. Assim, o sistema pode ser aplicado na medição da corrente de neutro, obtendo-se informações para gerenciar o balanceamento dos circuitos. Além disso, monitorar variáveis de instalações de energia permite inferir informações sobre eficiência de sistemas, taxa de utilização da infraestrutura, limite de corrente por circuito (devido a dispositivos de proteção como disjuntores e DR's - Diferential Residual - Residual Diferencial, o qual interrompe circuitos se detecta fuga de corrente), e até cálculos de indicadores de eficiência energética, bem como adoção de medidas e políticas de redução de consumo e comprovação da eficácia dessas.

Conclui-se, portanto, todo o conjunto de fundamentações teóricas necessárias para o completo entendimento deste trabalho. No próximo capítulo, a proposta de solução será especificada e a metodologia usada no projeto será percorrida.

3 PROPOSTA DE PROJETO

Este capítulo definirá os conceitos que perfazem a proposta de solução para o problema da gerência de infraestruturas físicas. A primeira seção aborda o projeto de uma solução de monitoramento de baixo custo que disponibiliza dados através do protocolo SNMP. A segunda seção irá explorar e propor formas de uso desse sistema em dois cenários diferentes: no primeiro, todos os endereços estão acessíveis via rede local; no outro, as instalações estão espalhadas, tendo em comum apenas o acesso à Internet. Nesse último caso, será proposto um uso diferente do sistema projetado para a gerência de infraestruturas massivas distribuídas geograficamente, nas quais não é possível o monitoramento clássico do SNMP, sendo o maior exemplo as *Smart grids*.

3.1 PROJETO DO SISTEMA

Esta seção percorre as etapas e considerações, bem como especificações e decisões de projeto pertinentes ao desenvolvimento de um sistema de monitoramento baseado em microcontroladores e o protocolo SNMP. O projeto foi dividido em três partes, começando pelo levantamento de requisitos e especificações (além da determinação de escopo), passando à metodologia aplicada na montagem e escolha do hardware, e concluindo com a metodologia aplicada ao desenvolvimento do software embarcado para a solução.

3.1.1 Requisitos e Especificações

Inicialmente, era necessário que os requisitos reais fossem levantados, de forma a guiar o projeto para a simplicidade e eficiência necessárias à aplicação, e por isso, escolheu-se o escopo de um data center genérico. Logo, se o projeto atendesse de forma satisfatória qualquer infraestrutura média de TIC, com base nos conceitos abordados no Capítulo ”Fundamentação Teórica e Estado da Arte”, esse mesmo sistema poderia ser usado em qualquer outro cenário proposto. Isso só é verdade pelo fato de que a grande maioria das empresas detentoras de data centers têm resistência a incluir ferramentas novas em seus fluxos de trabalho; na verdade, o próprio setor de infraestrutura física apresenta dificuldade na adoção de tecnologias novas de gerência, mesmo ciente, muitas vezes, de seus benefícios, o que acaba por retardar profundas mudanças, como a já citada mentalidade a respeito da necessidade urgente de esforços para a eficiência energética. Apesar de os motivos para esse comportamento serem variados, as causas mais comumente identificadas são:

1. *Falta de profissionais capacitados:* O investimento em melhorias no setor privado ocorre quase sempre alinhado com expectativas de lucro e/ou redução de gastos, ou seja, existe

sempre o questionamento sobre o ROI (Return of Investiment - Retorno de Investimento). O problema é que a maioria dos profissionais e das equipes técnicas ainda não é capaz de quantificar expectativas de lucros advindos de melhorias na gestão de ativos, bem como têm dificuldade em apontar e implementar as ações de gerência que resultariam em diminuição de gastos e paradas. A capacitação em eficiência energética e sustentabilidade, no entanto, é um tema extremamente atual, sendo possível encontrar diversos movimentos na Indústria que levam ao amadurecimento e incentivo desse conhecimento, contudo, esse ainda é um fator limitante para a ampla valorização dos sistemas de gerenciamento.

2. *Processos "engessados":* Empresas detentoras de data centers privados são, em geral, grandes e complexas hierarquicamente, de modo que todas as tarefas e entregáveis já estão definidos e são considerados satisfatórios. Logo, acrescentar mudanças de paradigmas nesses ambientes se torna oneroso e, algumas vezes, potencialmente conflitante, seja com o negócio, seja com os profissionais.

3. *Receios de acréscimo de falhas desconhecidas:* Existe um grande receio de que, ao implementar um novo sistema e/ou processo (principalmente de automação), sejam acrescidas à operação falhas não especificadas, o que resultaria num potencial risco para o suporte dos serviços de dados.

4. *Indisponibilidades de janelas de trabalho:* Data centers, em geral, devem funcionar de forma ininterrupta, e sua operação deve objetivar a disponibilidade máxima. Disso decorre que não podem ser criadas paradas momentâneas dos sistemas para instalação de novos subsistemas (desligar um circuito para instalação de medidor, por exemplo).

5. *Dependências de empresas privadas e licenças de software proprietário:* Existe um esforço constante para diminuir o uso de tecnologias proprietárias, de forma que as empresas tenham facilidade na reposição dos sistemas, liberdade na compra e também na personalização. Entretanto, a maior parte das soluções de monitoramento e gestão disponíveis no mercado atual se baseiam em soluções proprietárias de custo bastante elevado, contrariando as políticas internas de várias organizações e inviabilizando aquisições em infraestruturas de médio e pequeno porte, ou em setores com pouco orçamento.

Sabendo, portanto, que os requisitos do setor de infraestrutura física de TIC são extremamente rígidos, optou-se por investigar se seria possível desenvolver um sistema que cumprisse a tarefa de medir consumo de energia elétrica e que também se adequasse, de forma completa, a cada problema listado. O sistema, consequentemente, precisaria:

1. *Medir consumo de energia de forma não invasiva:* O sistema deve ser capaz de realizar as medições sem que seja necessário interromper o funcionamento de circuitos ativos, seja para a aferição, seja para a instalação.

2. *Não acrescentar pontos de falha:* As medições devem ser realizadas sem colocar em contato partes metálicas desse sistema de medição com quaisquer equipamentos e sem que o

sobreaquecimento e/ou qualquer tipo de falha no sistema de medição possa afetar os circuitos alvo. Essa limitação de escopo evita que sejam necessários conhecimento profundos sobre as normatizações de segurança para medidores em instalações elétricas, sendo necessário apenas um profissional capacitado pela norma NR-10 para as instalações (Segurança em Instalações E Serviços em Eletricidade [65]).

3. *Não acrescentar vulnerabilidades à rede:* O sistema deve evitar qualquer tipo de comunicação que possa servir como porta de entrada e/ou atrativo para atacantes, mas deve, ainda sim, usar métodos que sejam simples o bastante para não exigir processamento adicional do sistema de medição. Portanto, protocolos de Internet das Coisas e redes sem fio padrão IEEE 802.11 [66] estariam descartados para a maioria dos locais. Apesar de o padrão Wireless IEEE 802.11 conter várias implementações de segurança, redes sem fio criadas dentro de ambientes de data centers ainda têm certa dificuldade de penetração no setor, dada a impossibilidade de controle no acesso deste (controla-se a autenticação de usuários, mas não a difusão do sinal), além de as implementações de segurança consumirem muitos recursos de processamento. No caso dos protocolos de IoT (Internet of Things - Internet das Coisas), ainda existem problemas sérios sobre segurança, além de a maioria destes ser própria para comunicação sem fio, que como já mencionado, ainda encontra resistência no setor. Sobram, por fim, os padrões de comunicações cabeadas.

4. *Fácil integração:* O sistema deve usar um meio de comunicação facilmente aproveitável e se apoiar em protocolos e padrões de troca de dados universais, de forma que qualquer empresa com infraestrutura mínima possa implantar o sistema sem onerar os fluxos de trabalho e sem depender de licenças e/ou softwares adicionais. Portanto, padrões de comunicação serial não seriam interessantes, visto que dificilmente existem, nos data centers, dispositivos que consigam se comunicar usando esses protocolos para coletar dados e enviar essas informações para aplicações completas de monitoramento. Desenvolver um software local para monitoramento também tornaria o sistema complexo e pouco integrável com o restante da operação.

5. *Simplicidade:* O sistema deve ser simples para interação, rápido em operação e não gastar parcela relevante de energia.

6. *Hardware e Software "abertos":* O sistema deve ser desenvolvido baseado em hardware aberto e de fácil aquisição e os softwares usados devem ser todos abertos e globais, para garantir a oferta e suporte adequados.

Após extensa pesquisa e estudo das falhas e pontos positivos e negativos dos produtos existentes no mercado, concluiu-se que as seguintes especificações seriam suficientes para atender o propósito do sistema (a seguir, ao lado do requisito, a especificação escolhida):

1. *Medir consumo de energia de forma não invasiva:* Serão usados sensores de corrente não invasivos, baseados nos efeitos de indução de correntes em núcleos ferrosos por campos

magnéticos presentes em cabos condutores de corrente elétrica (ou seja, no conceito de transformadores de corrente, explorado melhor no Capítulo "Fundamentação Teórica e Estado da Arte"). Para a maioria dos circuito de corrente alternada internos às salas dos data centers, o sensor "SCT-013 100A:50mA" da marca YHDC [64], será suficiente (além de facilmente encontrado para compra). O valor principal a ser medido será corrente elétrica, porém, para circuitos com fator de potência elevado (como instalações com poucos motores e abundância de computadores) e presença de sistemas de no-break e estabilização de tensão, é possível assumir os fatores de potência e a tensão das fases como sendo fixos. Sendo assim, assume-se que, uma vez medidos esses valores e configurados no sistema, o mesmo poderá fornecer, para cada fase (e para o neutro):

(a) Corrente elétrica
(b) Potência Aparente
(c) Potência Reativa
(d) Potência Real
(e) Consumo de energia Aparente
(f) Consumo de energia Reativa
(g) Consumo de energia Real

Frise-se que o sistema proposto não pretende, num primeiro momento, entregar variáveis de qualidade de energia, apenas de consumo, por isso o escopo limitado e as considerações de valores como tensão e fator de potências como fixos nas medições. A ideia seria que a tensão fosse assumida constante e que o profissional responsável efetuasse medições do fator de potência a cada período de tempo (ou quando ocorresse alguma mudança) e atualizasse a configuração do sistema.

2. *Não acrescentar pontos de falha:* Como a tensão RMS, ou tensão eficaz, das redes que alimentam os equipamentos deveria permanecer o máximo constante, e lembrando que o objetivo do sistema é medir consumo, e não qualidade de energia, o sistema deverá ser configurado com a tensão eficaz nominal da rede elétrica do local e fazer o cálculo indireto do consumo baseado na corrente medida (ou seja, multiplicando a tensão eficaz nominal pela corrente eficaz medida). Assim, não existirá necessidade de contato elétrico para medição de diferença de potencial, não acrescentando, portanto, possíveis pontos de falha, além de delimitar o escopo do projeto para evitar a necessidade de aplicações de normas diversas de segurança. Porém, é importante notar que essa escolha reduzirá a qualidade e precisão das leituras, sendo um campo de aperfeiçoamento em potenciais trabalhos futuros.

3. *Não acrescentar vulnerabilidades à rede:* As comunicações deverão ser baseadas em protocolos e padrões de redes cabeadas como o IEEE 802.3 [34], o padrão Ethernet com conectores RJ45, compatíveis com a ampla maioria dos equipamentos de redes encontrados em instalações de TIC.

4. *Fácil integração:* O sistema deverá usar o protocolo SNMPv1 [26] para envio de dados, de forma que qualquer software de gerência de redes seja capaz de obter dados deste. Aliando, portanto, o protocolo SNMPv1 ao padrão cabeado IEEE 802.3 com conexão RJ45, ter-se-á um sistema integrável com qualquer ambiente de TIC atual.

5. *Simplicidade:* O sistema deverá ser desenvolvido usando microcontrolador de ampla disponibilidade e programado em Linguagem C/C++, de forma que dispense a necessidade de Sistema Operacional e/ou programas remotos, tendo todas as funcionalidades necessárias embarcadas em si (em alinhamento com os atuais estágios de entendimento das tecnologias de IoT).

6. *Hardware e Software "abertos":* O sistema será desenvolvido usando a plataforma de hardware Arduino [67], conjuntamente com a placa de arquitetura aberta ”Ethernet Shield W5100”, da empresa Wiznet [68], e sua respectiva IDE (Integrated Development Environment - Ambiente de Desenvolvimento Integrado), de mesmo nome (a citar-se, ”Arduino IDE” [69]). Mais especificamente, a placa ”Arduino Mega 2560 Rev3” [70] será a escolhida, baseada no microcontrolador Atmel2560 de 8 bits com arquitetura RISK avançada, da empresa Atmel. O sistema se comunicará com qualquer software de gerência de redes com suporte a SNMPv1 [26] (exemplos são o software Zabbix [25], e Nagios [46], ambos softwares livres e de código aberto).

Tendo, por fim, definido o escopo geral do sistema e especificado suas características, funcionalidades e tecnologias, a subseção a seguir trata da problemática do hardware no projeto.

3.1.2 Conceitos Aplicados e Montagem - Hardware

Esta subseção especifica o hardware usado, bem como os esquemas de ligação e montagem aplicados.

Tendo em mente que o objetivo deste trabalho é desenvolver um sistema de monitoramento utilizando ferramentas do mundo ”Open-Source” e que seja facilmente reproduzido, torna-se desinteressante a confecção de uma placa de circuito impresso e projeto eletrônico completo. De fato, a melhor abordagem seria usar como suporte uma plataforma pronta que disponibilizasse microcontrolador (o qual, como visto no Capítulo ”Fundamentação Teórica e Estado da Arte” já é, por natureza, um componente bastante completo) e todos os periféricos necessários como conectores de energia, de dados e de jumpers (evitando a necessidade de soldas) e que, por fim, fosse de fácil aquisição. A plataforma Arduino [67], e mais especificamente a placa ”Arduino Mega 2560 Rev3” [70], se mostrou a melhor escolha:

1. Com velocidade de processamento de até 16MHz, a leitura de sensores e envio de dados via rede a taxas satisfatórias é completamente possível, possibilitando gerências em tempo real;

2. Tendo disponíveis 4KB de espaço para memória permanente, é possível armazenar informações de conexão (como endereços IP, máscaras de rede e endereços MAC) que, em conjunto com programas que permitam a configuração de parâmetros via porta serial, por exemplo, tornam desnecessárias quaisquer recompilações de projeto para efetuar mudanças nas configurações;

3. Com 248KB de memória disponíveis para o programa (de fato, são 256KB, porém 8KB são usados por um programa nativo da placa que grava na memória o projeto enviado de um computador, programa esse chamado "bootloader"), é possível implementar todo o processamento necessário para o serviço do protocolo SNMPv1 [26] e ainda manter rotinas avançadas de cálculos com as leituras dos sensores e até mesmo a implementação de outros serviços, como páginas web e dashboards;

4. Com 16 portas analógicas e 54 digitais (todas de fácil acesso com uso de jumpers), ela facilmente vira a "placa-mãe" de um sistema completo, tornando desnecessários trabalhos adicionais de confecção de circuitos e até mesmo eliminando as chances, para o caso deste projeto, de faltarem portas;

5. Com a operação em 5V, é possível alimentar o sistema com fontes de energia facilmente encontradas no mercado, pois esta é a mesma tensão usada em diversos outros dispositivos como pontos de acesso, câmeras e carregadores de telefones celulares.

6. A presença de conexão USB e conector de energia P4 permite diversas configurações de alimentação e compilação rápida do projeto;

7. A placa "Arduino Mega 2560 Rev3" [70] é compatível com o layout da placa "Arduino UNO" [71], podendo se utilizar de todas as placas complementares que a segunda dispõe. Essas placas, as quais adicionam capacidades ao projeto segundo a organização Arduino [72], são chamadas de "Shields", e especificamente para o interesse deste projeto, existe uma placa "shield" que traz consigo conexão via padrão Ethernet (IEEE 802.3 [34]) com conector RJ45 e com suporte a taxas de 10Mbs a 100Mbps. Essa placa é conhecida popularmente por "shield de rede", sendo seu nome "Ethernet Shield", e sua fabricante é a empresa Wiznet [68] (contudo, a arquitetura da placa é aberta). Apesar de existirem vários modelos, o escolhido será aquele amplamente disponível no comércio de componentes eletrônicos, o modelo "W5100". Este é um dos periféricos mais famosos da plataforma, e implementa nativamente a pilha TCP/IP, tornando a programação de aplicações baseadas nos protocolos TCP e UDP menos dispendiosas. Portanto, lembrando que a placa "Arduino Mega 2560 Rev3" [70] é compatível com esse "shield", ao encaixar as duas, obtém-se uma plataforma bastante flexível, adicionando conexão de rede cabeada ao sistema.

Portanto, de posse de uma plataforma de rápida programação e que já disponibiliza conexão de rede padrão Ethernet (IEEE 802.33 [34]) via conector RJ45, conector de energia, porta USB para programação, além de portas de fácil acesso ao microcontrolador, era necessário definir como seriam conectados os sensores desse sistema, responsáveis por medir, efetivamente, o valor de

corrente elétrica passando por um condutor/cabo.

Sobre o sensor de corrente não-invasivo especificado (”SCT-013 100A:50mA”), este não traz, consigo, o circuito necessário para que uma porta de leituras analógicas simples de um microcontrolador possa realizar leituras corretas (ou seja, esse dispositivo é puramente um transformador). Primeiramente, porque a saída do sensor é em corrente, e portas analógicas simples como a da maioria dos microcontroladores (incluindo a placa ”Arduino Mega 2560 Rev3”) não medem saídas em corrente, somente em tensão. Em segundo lugar, a corrente de saída do sensor é variável no tempo e apresenta valores negativos, não sendo interessante para as medições. Para solucionar o problema, é necessária a confecção de um circuito auxiliar simples, composto de três (3) resistores e um (1) capacitor. A iniciativa ”Open Energy Monitor” [73], tem uma sessão inteiramente dedicada ao ensino da teoria por trás desses conceitos, bem como aborda bastante de uma implementação de sistema parecida, mas voltada para residências e prédios. De fato, esse projeto utiliza a mesma arquitetura de hardware proposta para o sistema em questão e serviu de inspiração para várias problemáticas neste trabalho. Como disposto na figura 3.1, obtida na sessão de ensino do site da organização citada, o circuito necessário constitui-se, basicamente, de: um resistor de carga para a saída em corrente do sensor; um divisor de tensão, para que as leituras de tensão feitas pelo microcontrolador sejam sempre positivas; e um capacitor com baixa reactância, o qual filtra as componentes alternadas de corrente, apresentando um caminho de menor resistência em comparação com o resistor ligado ao terra do divisor de tensão (o qual é preferido pelas componentes contínuas de corrente).

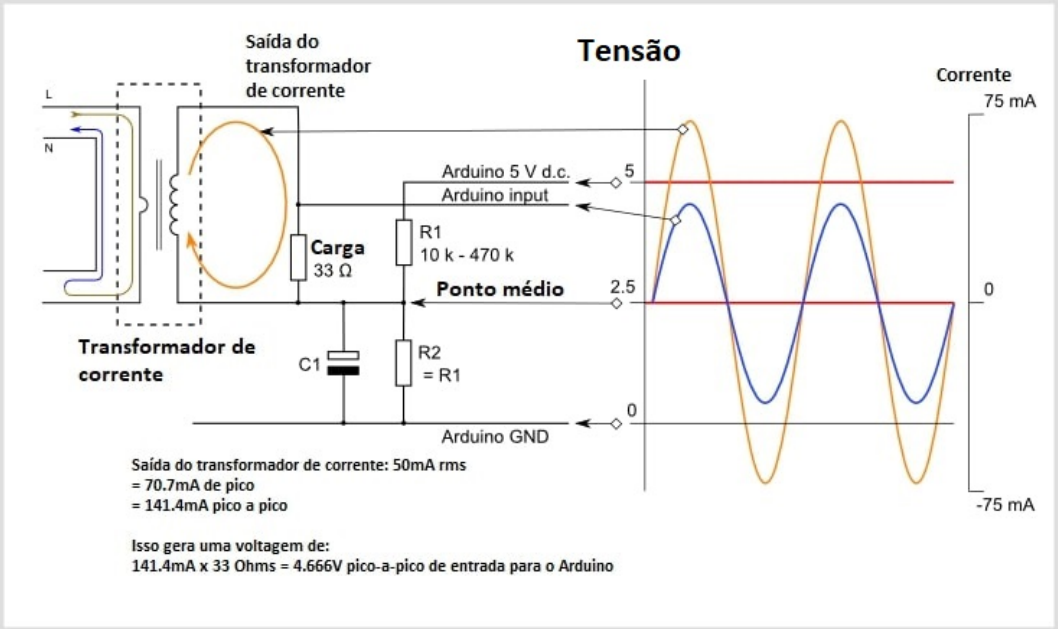

Figura 3.1: Esquemático e explicação do circuito auxiliar para a interface entre a placa Arduino Mega e o sensor ”SCT-013 100A:50mA”(Open Energy Monitor,2019) [23].

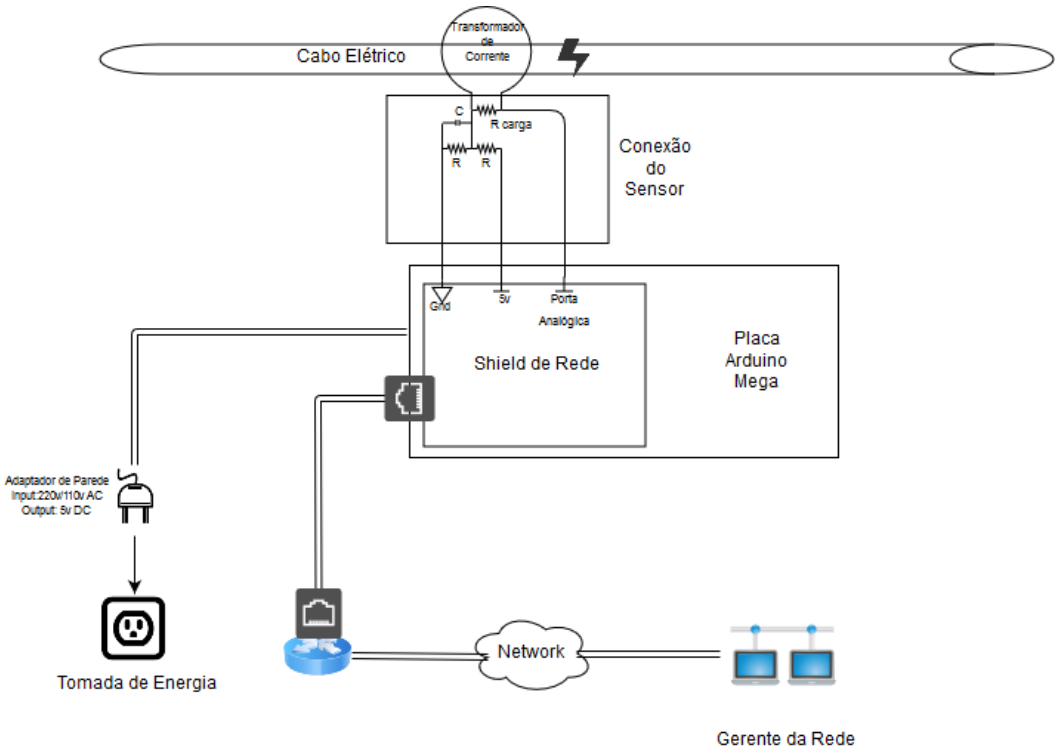

Figura 3.2: Diagrama do projeto de hardware completo.

Finalmente, associando a placa ”Arduino Mega 2560 Rev3” [70], a placa ”Ethernet Shield W5100” [68], um circuito elétrico simples e o sensor ”SCT-013 100A:50mA” [64], tem-se todo o aparato físico necessário para a montagem de um sistema capaz de realizar medições de corrente de forma não-invasiva e disponibilizar dados via redes TCP/IP.

Note-se que em circuitos os quais o fator de potência varia no tempo, o sistema fará cálculos imprecisos para as potências real e reativa. Porém, isso não afeta os valores da potência aparente, visto esse valor ser unicamente dependente da corrente e tensão; nesse caso, poderá existir imprecisão na potência aparente apenas pelo fato de a tensão ser assumida fixa, já que o sistema não efetua medidas dessa grandeza. O fator de potência é um valor que, se usado, deve ser configurado como fixo no sistema, entretanto, na prática, seu cálculo depende do valor da tensão, bem como da fase dessa, não estando no escopo deste projeto sua medição precisa. Foi escolhida a não inclusão de medição de tensão no sistema para que não fossem necessárias observações adicionais sobre normas de segurança para medidores de energia e nem fossem adicionados possíveis pontos de falha com adição de contatos metálicos em instalações elétricas operantes.

Tendo abordado todos os desafios da montagem de um hardware simples e de fácil instalação para a medição de consumo de energia, a seguir, a problemática do software é abordada.

3.1.3 Conceitos Aplicados e Desenvolvimento - Software Embarcado

Este tópico abordará os recursos de software, as referências de projetos que embasaram este trabalho e as metodologias e delimitações aplicadas, além de, por fim, definir os resultados esperados da implementação da solução embarcada em Linguagem C/C++ com uso de bibliotecas e funções próprias da já especificada plataforma Arduino. Inicia-se pela especificação de recursos para as leituras dos sensores, passando posteriormente à abordagem dos recursos de integração, que permitam ao sistema comunicar-se segundo os padrões e protocolos estabelecidos, e por fim, é feito um resumo da especificação completa de software necessária para o desenvolvimento completo.

Como já mencionado anteriormente, a montagem do hardware foi largamente inspirada nos conceitos descritos no projeto ”Open Energy Monitor” [73]. O mesmo trouxe consigo, também, o desenvolvimento de uma biblioteca para a plataforma Arduino, chamada ”EmonLib” [74], a qual será utilizada nas leituras dos sensores. Apesar de existirem vários recursos de aprendizado no guia do projeto citado, o foco deste não é ambientes técnicos e tampouco as tecnologias e padrões usados em locais de instalações de TIC, portanto, esse serviu de base apenas para a solução da problemática da montagem de circuito e método de medição (inclua-se em método o tipo de sensor escolhido e a classe de leitura). Visto que uma das premissas do sistema proposto neste trabalho é ter impacto zero na instalação e integração quase que automática com processos de gerência de redes já existentes, apenas a função de leitura de correntes RMS, ou eficazes, da biblioteca ”EmonLib” será usada nesse projeto, contudo, com mudanças nas chamadas. Isso porque, tratando-se de máquinas que gastam energia elétrica sem produzir trabalho (no sentido físico do termo), como servidores, roteadores e computadores, as variações de corrente estarão atreladas à demanda por processamento dessas unidades, e essa demanda pode variar bastante no tempo, logo, são necessárias leituras rápidas para uma melhor precisão, situação que não é atendida pela biblioteca ”EmonLib” nas implementações clássicas do projeto Open Energy Monitor.

Em primeiro lugar, a biblioteca tem a definição da classe ”EnergyMonitor”, a qual representa uma única interface de leitura para um único sensor. Ao criar um objeto genérico desta classe, ele deverá ser inicializado em uma etapa prévia do programa com a chamada do método de classe ”current”, devendo ser repassados dois parâmetros: a porta analógica de leitura do sensor e um valor de calibragem inicial. Este valor deve ser obtido através de testes, comparando-se as leituras dos sensores em diversos cenários com um medidor amperímetro do tipo alicate (neste caso, assume-se que o medidor é uma referência confiável e válida). Tal parâmetro se relaciona com os valores flutuantes (ou seja, a margem de erro) dos componentes eletrônicos passivos (resistores e capacitor) dispostos nos diagramas das figuras 3.1 e 3.2, por isso seu caráter empírico, e não analítico. Para os valores dos componentes especificados neste projeto, um valor aproximado para esse parâmetros é ”54.6”. Uma vez que um objeto ”EnergyMonitor” é inicializado, portanto, as leituras podem ser feitas através da invocação da função de classe ”calcIrms”, a qual recebe apenas um parâmetro inteiro e retorna, em ponto flutuante, a leitura do valor eficaz, ou RMS, da

corrente. O parâmetro a ser passado para a função de leitura representa o número de iterações que serão usadas. Ocorre que correntes em regime senoidal podem ser vistas como sinais variantes no tempo, e como tais, sofrem com interferência de ruído quanto menores forem as frequências de amostragem da onda. Portanto, nas implementações clássicas do Open Energy Monitor, valores da ordem de milhares de iterações são usados, para garantir leituras livres de ruído. Entretanto, para um projeto em linguagem estruturada o qual deverá, além de ler variáveis de vários sensores, suportar outro serviço de rede (como um agente SNMP, por exemplo), leituras demoradas podem inviabilizar o funcionamento do sistema. Para a resolução da problemática, a quantidade de iterações foi reduzida para a ordem de algumas dezenas, e ao invés de resolver o problema do ruído através de uma única leitura e variável, é possível realizar médias de várias leituras em várias variáveis. Isso significa que, no projeto proposto, variáveis auxiliares acumulam leituras enquanto a principal fica disponível para consultas via rede sem sofrer alterações, e após algumas dezenas de iterações (cada qual gerando leituras baseadas em dezenas de outras iterações), calcula-se a média dos valores das variáveis auxiliares e atualiza-se a variável principal. O resultado final é ganho de performance sem perda de resolução. Em resumo, aplica-se várias leituras em diferentes oportunidades cadenciadas, de forma que o resultado final assemelha-se bastante com o caso em que se realiza milhares de leituras, porém difere por economizar tempo de ocupação da CPU do microcontrolador.

Tendo-se à disposição recursos e metodologias de software para realizar as medições de correntes, e sabendo-se à priori os valores de tensão do circuito, o cálculo das potências é imediato: se a tensão conhecida for de um circuito trifásico, basta multiplicar a corrente em cada fase por essa tensão, e ter-se-á a potência em cada fase, e como mostrado no Capítulo ”Fundamentação Teórica e Estado da Arte”, a soma das potências é a potência total; caso seja um circuito monofásico, o mesmo procedimento é aplicado, ou seja, multiplica-se a corrente pela tensão, e obtém-se a potência instantânea. Basta, agora, resolver o cálculo do consumo de energia. Todavia, diferentemente do cálculo de potência instantânea, o consumo de energia remete à potência consumida num determinado período de tempo. Porém, se a especificação de hardware não contém qualquer módulo para medição de tempo, como esse problema será resolvido? Novamente, a decisão por um projeto de hardware e software simples delimita o cenário: dado que módulos RTC (Real Time Clock - Relógio de Tempo Real) não estão amplamente disponíveis para a plataforma Arduino e a exigência de serviços de rede que forneçam data e hora (ou mesmo de acesso à Internet para buscar esses dados) foge completamente aos requisitos observados anteriormente, uma decisão de projeto é a de que, caso o usuário queira monitorar consumo de energia, terá duas possíveis abordagens: ou irá obter os valores de potência instantânea e usar softwares terceiros para o cálculo e acumulação, hora após hora, ou ele irá configurar data e hora iniciais no sistema e este contará a passagem de tempo com base nas batidas de clock internas, relevando-se as possíveis margens de erro. Deverá ser implementado, portanto, um método de configuração serial de data e hora iniciais. O sistema, com base nessa contagem interna da passagem do tempo, calculará as médias das potências a cada hora, de forma cumulativa, e ao fim de um mês, essa acumulação será zerada, reiniciando-se o ciclo.

Após abordada a metodologia e as decisões de projeto para a medição e cálculo das variáveis, a integração com a rede cabeada e com a própria gerência de redes se torna o próximo alvo das discussões.

Como já descrito, o protocolo SNMPv1 [26] foi o escolhido para esse fim, tendo como vantagens, em resumo, a universalidade de suporte entre as soluções NMS (Network Management Solution - Solução de gerência de rede), amplamente usadas em ambientes de infraestrutura de TIC (Tecnologia da Informação e Comunicação), e a baixa demanda por processamento e recursos de armazenamento. Entretanto, mesmo se tratando de um protocolo maduro e bem divulgado, a implementação a nível de código de um serviço de SNMP pode se tornar um grande desafio. Em primeiro lugar, o protocolo funciona baseado no User Datagram Protocol, o UDP (RFC 768 [59]). Apesar de o funcionamento de um servidor UDP ser simples, pois em suma não existem estruturas de controle e nem mesmo é necessária a criação de conexões, boa parte da gerência de filas e escuta da chegada de mensagens, bem como do processamento dessas, fica a cargo do programador. Além disso, o protocolo SNMP está intimamente atrelado com a especificação de uma base de dados definida na MIB-II (RFC 1213 [48]), e suas mensagens, ou PDU's (Protocol Data Unit - Unidade de dados de protocolo), seguem o padrão ISO ASN.1, além de existir um criterioso rito no processo de envio de dados ditado na RFC3413 [75]. Felizmente, o projeto "Agentuino" [76] já trouxe uma solução para essa problemática através de uma biblioteca de mesmo nome, disponível em [77]. Com o uso da biblioteca, foi possível transformar um sistema com a plataforma Arduino num agente monitorado de um rede real e infraestruturada, e integrá-lo com softwares gerentes que suportem SNMPv1 [26]. O uso da biblioteca, todavia, não é trivial, afinal, o processamento das mensagens PDU's deve ser inteiramente feito pelo desenvolvedor, sendo a biblioteca unicamente responsável por suportar o serviço SNMP e realizar chamadas para a função a ela indicada, a qual deve processar as mensagens recebidas e enviar suas respostas (essa deve ser totalmente desenhada pelo programador). Portanto, é imprescindível o conhecimento aprofundado da estrutura de uma PDU SNMP [26], bem como da plataforma usada (Arduino), não sendo possível negligenciar as estruturas de mensagens dos padrões definidos nas RFC's citadas ao longo de todo este documento. Recapitulando alguns conceitos, na figura 3.3, uma parte da árvore da ISO é mostrada. Sua importância para a Internet é bem descrita pela IANA ao explanar sobre os SMI's (Structures of Management Information - Estruturas de Gerência de Informação) [78]. Um detalhe das especificações de tipos de dados da ISO ASN.1 [79] é mostrado na figura 3.4 (usados para o envio de dados padronizados no SNMP independentemente de plataforma e arquitetura de hardware), e a topologia SNMP (com a posição ocupada pelo sistema do projeto em destaque) é resumida na figura 3.5.

Sobre o funcionamento da biblioteca "Agentuino", esta não contém definições de classes e objetos. Ao invés disso, contém uma função chamada "begin", a qual não necessita de parâmetros e inicializa de forma autônoma o serviço de SNMP (bem como o servidor UDP necessário na porta

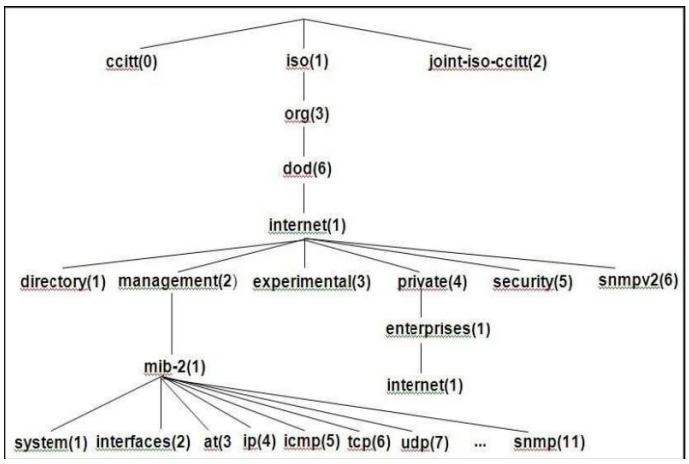

Figura 3.3: Árvore de nomes da ISO (no canto inferior direito, encontra-se o protocolo SNMP).

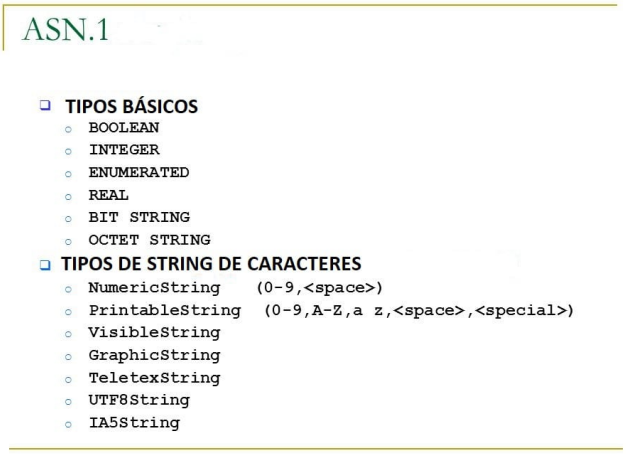

Figura 3.4: Detalhe das especificações de tipos definidos pela ISO ”ASN.1”.

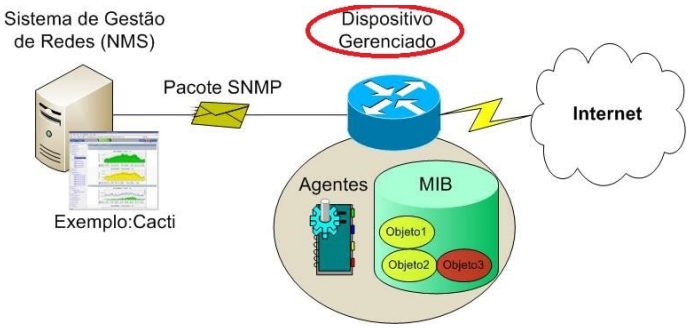

Figura 3.5: Detalhe da topologia típica do protocolo SNMP, e circulado em vermelho, o papel assumido pelo sistema proposto nessa estrutura.

161, padrão do protocolo). Também contém uma função denominada ”onPduReceive()”, a qual recebe como parâmetro de entrada o endereço de uma função criada pelo usuário para ser acionada toda vez que uma PDU nova for recebida (no caso, indica-se o uso do nome ”pduReceived” para manter o padrão da biblioteca). O recebimento de mensagens e consequente chamada da função ”pduReceived” se dá através da verificação do buffer de entrada, que ocorre toda vez que

a função da biblioteca denominada ”listen” é invocada. Uma vez chamada, de forma autônoma, a função ”pduReceived”, o design e processamento da PDU dentro da função é livre, sendo responsabilidade do programador. De forma complementar, para limitação do escopo do trabalho, a implementação de um dispositivo que enviasse mensagens do tipo ”trap” foi deixada de fora do projeto, porém, uma possível e interessante abordagem do uso de ”traps” está disposta nas sugestões de trabalhos futuros ao fim deste documento. Note-se, ao fim das explicações a respeito da biblioteca ”Agentuino”, que seu funcionamento depende da placa ”Shield de Rede”, a qual funciona baseada na biblioteca ”Ethernet” [80], portanto, é necessário que esta esteja incluída no projeto para que esse compile adequadamente. O último ponto a ser abordado sobre conexão se refere à configuração de endereços IP. Mais uma vez, por decisão de projeto, esse parâmetro deverá ser alterado via interface serial, tal qual a data e hora do sistema.

Ainda são necessárias especificações complementares que delimitem o escopo do projeto e guiem os entregáveis. Em primeiro lugar, note-se que uma decisão de projeto foi o não atendimento completo das especificações da MIB-II [48]. Não foram encontrados benefícios na implementação de tantas variáveis de rede num sistema que tem finalidades tão bem delimitadas como medir correntes elétricas e realizar cálculos de potência instantânea e consumida. Em segundo lugar, para uso em ambientes de infraestruturas de redes reais, ainda se fazia necessário que o sistema tivesse sua própria árvore de nomes (única no mundo) para que fosse possível separar os códigos identificadores, ou OID’s (Object Identification Number - Número de Identificação de Objeto), de cada variável produzida decorrente das medições. É através desses códigos que um software gerente consegue requisitar determinada variável e que um agente monitorado sabe qual valor deve enviar de sua base de dados. Logo, trabalhando pela padronização e facilidade de uso do sistema, realizou-se o pedido de cadastro de um PEN (Private Enterprise Number - número de empresa privada) junto à IANA (Internet Assigned Numbers Authority - Autoridade Designada de Números da Internet). Esse código requisitado cria um OID único sob as nomenclaturas definidas na árvore da ISO, ou seja, obtém um ”ramo” privado e único abaixo do ramo ”enterprise” da figura 3.3. O código recebido foi ”49191” (podendo ser consultado em [81]), e portanto, o ramo único e privado do sistema é ”1.3.6.1.4.1.49191”. Acrescentando mais pontos, ou ramos, definiu-se os OID’s para cada variável a qual o sistema deveria ser capaz de retornar algum valor, como mostrado na figura 3.6. A priori, todos os valores deveriam ser enviados no tipo ”INTEGER” do ASN.1, pois o SNMPv1 não previa envio de valores em ponto flutuante (ou seja, com casas decimais), contudo, algumas soluções de NMS são capazes de realizar o ”parse” de palavras, permitindo o envio de ponto flutuante na forma de ”string” de dados (do tipo ”OCTET STRING”). Esse é o caso do software Zabbix, o qual será usado para validação do sistema, portanto, indica-se a preferência pelo envio de strings em detrimento de números inteiros, os quais afetariam bastante a acurácia dos dados obtidos.

Com as duas principais necessidades do projeto (leitura e integração) atendidas com recursos de software através do protocolo SNMP [26], da biblioteca Open-Source ”Agentuino” [77], da

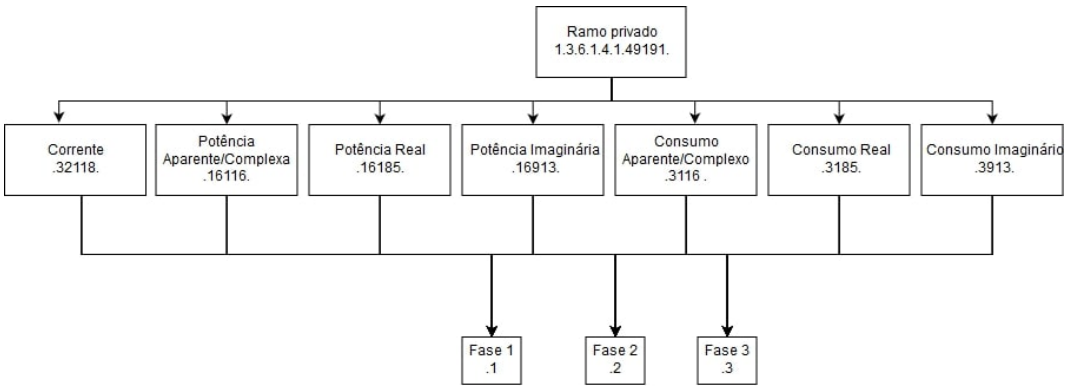

Figura 3.6: Árvore de nomes definidos e padronizados para o sistema proposto.

padronização das estruturas de nomes dos parâmetros a serem requisitados (os OID's de cada variável) e da biblioteca Open-Source "Emonlib" [74], todo o suporte estava pronto para o desenvolvimento do software embarcado. O próximo passo seria a definição do esquema de funcionamento do sistema. A figura 3.7 mostra o fluxograma esperado de funcionamento do sistema, que traduz de forma amigável como funcionará o software a ser desenvolvido. Relembrando, o consumo de energia é a soma acumulativa das leituras de potência no tempo, e para o caso das concessionárias, a cobrança se dá por valores mensais. Portanto, o sistema proposto, ao ser ligado, deverá ser configurado com o horário e data atual e ficará acumulando as médias de potência a cada hora até que se passe um (1) mês, quando esse valor será zerado e reinicia-se o acompanhamento do consumo no próximo mês, e assim por diante. Esse valor será oferecido, também, via SNMP. Com isso, será possível conseguir dados interessantes, como a evolução da curva de carga das instalações, e observar o rompimento de metas de consumo, ou mesmo usar os dados para averiguar possíveis cobranças indevidas, situação bastante comum.
As rotinas descritas no fluxograma, se implementadas sem cuidado, podem tornar o sistema inutilizável. Isso porque, se as leituras demorarem muito, a chance de perder uma PDU SNMP que chegou à interface de rede do sistema será grande, e no caso contrário, se o processamento do serviço SNMP demandar muito tempo, as leituras de corrente se tornarão demasiadamente desviadas dos valores reais, lembrando se tratarem de ondas em regime senoidal, e portanto, variantes no tempo. Contudo, deve-se atentar para alguns fatos importantes e que, se explorados de forma planejada, podem contribuir para a simplicidade no projeto:

1. A frequência de funcionamento do microcontrolador é de até 16MHz, logo, considerando que os softwares gerentes requisitem dados a cada segundo (uma consideração exagerada), e sabendo que o SNMP não exige muito processamento da unidade, ainda existirá boa carga de ociosidade do microcontrolador, a qual pode ser usada para concentrar suporte nos cálculos e leituras de sensores;

2. Apesar de dito anteriormente que a leitura dos sensores deveria ser rápida o suficiente para ter precisão, isso não significava que estas devessem ser realizadas continuamente. Se as medições forem entendidas como um fluxo de dados, a taxa que essas medições forem repetidas definirá a granularidade da informação, logo, se taxas de leituras muito altas fo-

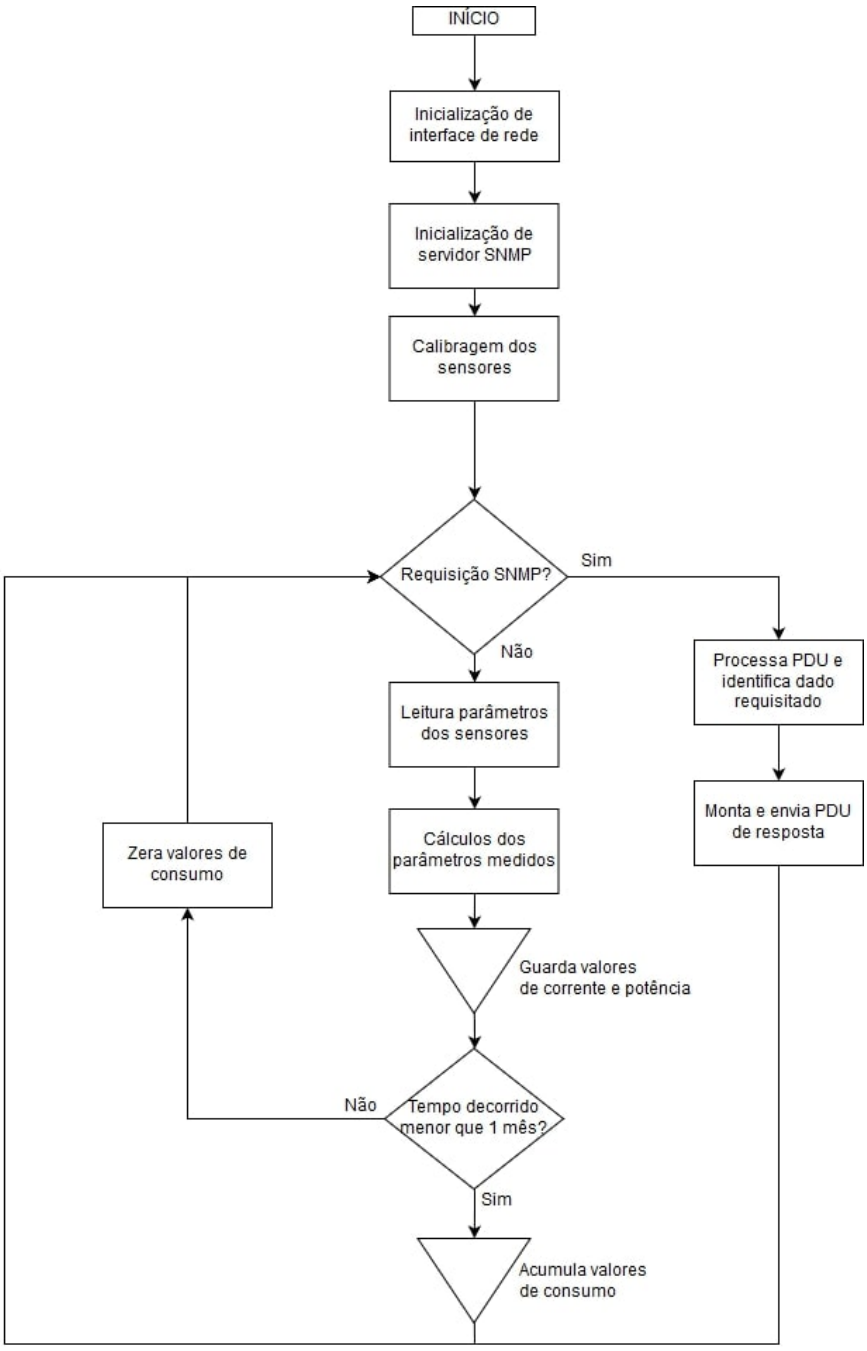

Figura 3.7: Fluxograma proposto para o funcionamento do software embarcado do projeto.

rem usadas, as mínimas variações de corrente serão percebidas, entretanto, sabendo que a frequência habitual das redes elétricas gira em torno de 50Hz a 60Hz, taxas muito maiores que isso poderiam ser bastante influenciadas por ruídos. Logo, taxas de leituras da mesma ordem dessas, como valores entre 10Hz e 30Hz, são mais que suficientes para a aplicação;

3. O SNMP é baseado no protocolo UDP, o qual não garante entrega das mensagens. Cientes disso, os desenvolvedores dos softwares gerentes de redes já programam esses para executar uma determinada quantidade de tentativas de requisições SNMP antes de desistir, ou permanecer tentando a obtenção dos dados a cada certo período de tempo. Portanto, sabendo

que o software gerente irá requisitar várias vezes a informação, o sistema a ser desenvolvido não precisa estar disponível em todos os momentos, só precisa estar disponível com uma frequência tal que dificilmente perca todas as tentativas de contato do software gerente. Logo, se as rotinas internas do software forem otimizadas, não existirá problemas em parar de suportar o serviço SNMP por pequenos períodos de tempo e atualizar os valores medidos rodando as rotinas de leitura e cálculo.

Unindo, portanto, os recursos, as bibliotecas e os paradigmas de desenvolvimento discutidos, será possível a criação de um software aberto, padronizado, com interação simples, necessidade de configuração quase inexistente e taxa de medição comparável à taxa de vídeos (10Hz a 30Hz), culminando num agente monitorado que transformará parâmetros físicos, como a corrente elétrica e o consumo de energia, em ”ativos”, sendo integrados dentro das soluções de NMS e passando a fazer parte do negócio, constituindo ferramenta valiosíssima de tomada de decisão para a gestão de data centers interessada em aplicar os conceitos de eficiência energética.

Portanto, a seguir, enumera-se as especificações básicas necessárias para o desenvolvimento do software:

1. Inclusão das bibliotecas ”EmonLib”, ”Ethernet” e ”Agentuino”;
2. Criação de pelo menos quatro (4) objetos ”EnergyMonitor”, sendo três (3) para as fases de um circuito trifásico e uma (1) para a corrente de neutro. Essa quantidade também atende circuitos monofásicos. Não pretende-se que um módulo monitore mais do que um circuito trifásico cada (porém seria possível monitorar 4 circuitos monofásicos). Também indica-se a criação de variável que armazene o valor da tensão nominal da instalação, a qual deve ser fixa, e outra variável que armazene os fatores de potência para cada fase (no caso de não haver interesse em uso desse parâmetro, a atribuição do valor ”1” a ele deve indicar ao software que ele não será usado nos cálculos).
3. O software deverá ter variáveis auxiliares, para acúmulo de leituras e cálculos de médias, e variáveis principais, as quais ficam disponíveis via rede e seus valores são alterados apenas em função de um novo valor de média das leituras, e não a cada rotina de leitura. Também deverá ter variáveis armazenadas em memória não volátil as quais irão armazenar data, hora e endereço IP.
4. O software deverá ter uma função de inicialização (a qual é chamada apenas uma vez pelo sistema, quando este é ligado), na qual invoca a função ”Agentuino.begin()” para iniciar o serviço SNMP, e a função ”Agentuino.onPduReceive()”, passando o endereço de uma função que processe as PDU’s SNMP recebidas (indica-se a denominação ”pduReceived”). Também deverá invocar as funções ”current” de cada objeto ”EnergyMonitor”, de forma a inicializá-los, passando as respectivas portas analógicas de leitura e o valor de calibragem (indicado em ”54.6” para os valores de resistores e capacitor especificados) e realizar alguma rotina de leitura prévia de variáveis para evitar comportamentos do tipo ”degrau” nas

leituras. Adicionalmente, essa função deve garantir o início da contagem de data e hora através das batidas de clock do dispositivo. Por fim, essa função deverá ter uma rotina de configuração via interface serial, a qual, sempre que o dispositivo for ligado, apresentará mensagem perguntando se o usuário se interessa em iniciar o modo de configuração ou não. A CPU deverá esperar por pelo menos 5 segundos antes de assumir reposta negativa e seguir com o funcionamento normal. Caso seja selecionado o modo de configuração, não deve haver tempo limite para inserção de dados, e uma vez que uma mudança seja completada, o sistema deverá apresentar pedido de ”reset” e manter-se em laço eterno no estado de”idle”, ou espera.

5. O software deverá ter uma função em laço eterno, na qual são realizadas as seguintes tarefas (ou invocadas funções que as realizem): acumulação de leituras dos sensores, cálculos de parâmetros indiretos (como consumo e potência instantânea), e invocação da função ”Agentuino.listen().

6. Deverá ser desenhada função que processa as PDU's recebidas, na qual uma estrutura do tipo ”switch/case” determina se a OID requisitada existe ou não e responde a requisição.

Completas as especificações e delimitações do projeto do software embarcado, a seção a seguir tratá da metodologia de aplicação e teste da solução.

3.2 METODOLOGIA DE APLICAÇÃO DO PROJETO

Esta seção tratará dos procedimentos de teste e validação do sistema proposto. A primeira subseção abordará a aplicação do sistema em infraestruturas nas quais uma única rede abrange todos os locais. A segunda seção proporá a aplicação do sistema em infraestruturas distribuídas, sendo os principais exemplos as *Smart grids*.

3.2.1 Infraestruturas Cobertas por Redes Locais

Mesmo infraestruturas grandes podem ter todos os seus pontos completamente atendidos e disponíveis por uma única rede. Nesses casos, todos os nós de interesse estão na mesma rede, não existindo impedimento para o gerente requisitar dados. Esse é o cenário ideal para o sistema proposto. O software NMS gerente a ser usado para a validação da solução será o Zabbix, visto ser esta a ferramenta aberta mais amplamente difundida no setor, (contudo, o sistema deveria integrar-se com qualquer outra solução de gerência atual). Os passos da aplicação do sistema (após montagem e desenvolvimento) e expectativas de resultados seguem para esse tipo de cenário:

1. Identificação de circuito de interesse no monitoramento (indica-se quadros de distribuição ou quadros de salas de médio e pequeno porte). Também indica-se que a validação seja feita

num circuito no qual se conhece o perfil de carga e, portanto, sabe-se a priori os valores e comportamentos esperados das medições.

2. Conexão dos sensores de corrente não invasivos nos condutores de fase e no condutor neutro, quando aplicável.

3. Disponibilização e habilitação de interface de acesso em switch ou equipamento da rede privada.

4. Disponibilização de IP fixo para o sistema.

5. Configuração de IP fixo, data e hora via interface serial no sistema.

6. Conexão dos sensores ao sistema, conexão das interfaces RJ45 e conexão do sistema à alimentação através de tomada e adaptador, conforme imagem 3.2.

7. Configuração de ”host” do tipo SNMPv1 agente e demais itens de monitoramento, usando as OID's resultantes da imagem 3.6.

8. Aquisição de dados por um período de aproximadamente 2 horas, para visualizar perfil de carga, periodicidade (se houver), acumulação de consumo pelo sistema (feito a cada hora) e aferição de resolução das medições. Indica-se comparar as leituras com um alicate amperímetro de referência.

A subseção a seguir propõe a forma de implementação do sistema em infraestruturas físicas distribuídas, a exemplo de grandes organizações multinacionais, órgãos governamentais e as famosas redes elétricas inteligentes.

3.2.2 Infraestruturas Massivas Distribuídas Geograficamente

Nesta seção, discute-se a aplicação de um sistema como o proposto em infraestruturas massivas e/ou distribuídas.

É interessante perceber que o alinhamento entre as tecnologias de gerências mais atuais e a simplicidade e eficiência do SNMP podem ajudar a atender quaisquer cenários possíveis. Um conceito bastante difundido entre os softwares NMS atuais também foi abordado no SNMPv2, como visto no Capítulo ”Fundamentação Teórica e Estado da Arte”, e trata-se da gerência distribuída. Nesses casos, existem gerentes os quais interagem localmente com agentes e enviam resumos dos dados coletados para um ou mais gerentes centrais. No caso do software Zabbix, esse conceito se materializa de forma extremamente descomplicada com o uso dos chamados ”Zabbix Proxies”. Estes conseguem se comunicar de forma segura, através da Internet, com o gerente central, permitindo a distribuição do monitoramento e gestão em diversas abordagens. Segundo o próprio site da ferramenta, traduzido para o português (Zabbix SIA,2019) [82]:

”O Zabbix Proxy é um processo que pode receber dados de um ou mais dispositivos monitorados e enviar ao Zabbix Server, basicamente ele funciona em nome do Zabbix Server (na visão do agente monitorado o Proxy passa a ser o Zabbix Server). Todo os dados recebidos são armazenados temporariamente (buferizados), transferidos ao Zabbix Server que o Zabbix Proxy pertencer, sendo excluídos na sequência do armazenamento temporário do Proxy.”

A figura 3.8 mostra um exemplo de funcionamento dessa solução. Com esse tipo de implementação em mente, o método de aplicação em cada cenário se torna descomplicado:

Organizações espalhadas geograficamente: Em casos de várias filiais, muito provavelmente, cada um terá pelo menos um método de conexão à Internet. Portanto, instalar um Zabbix Proxy em outro dispositivo que não o projetado, como um pequeno computador, permitirá gerenciar toda a filial à distância. Ainda, nos casos em que as instalações não necessariamente são locais de trabalho, e sim, salas de redes e/ou equipamentos, associar um sistema de Zabbix Proxy com alguma conexão de Internet via redes móveis (como, por exemplo, usando redes 3G ou 4G), compreende uma solução extremamente viável. Note-se, porém, que será necessário que o Zabbix Server tenha um IP público, para que os Zabbix Proxies consigam contatá-lo. Note-se também que nesta categoria também entram as fases de geração e transmissão de energia nas redes elétricas, e dado o baixo custo e flexibilidade do sistema, a contribuição nesses dois estágios pode ser enorme, principalmente para redução das perdas e avisos de falhas. No caso da geração, sempre existem grandes estruturas locais, logo, os desafios de implantação são facilmente superados, pois quase sempre existem meios de comunicação e redes locais. Na fase de transmissão, porém, apesar de ser desafiador instalar sistemas de monitoramento em regiões longínquas, é necessário lembrar as transmissões de energia elétrica se dão em alta tensão, e portanto, sempre existem subestações nas quais a tensão é reduzida e se inicia a distribuição local de energia, portanto, são nesses ambientes onde a aplicação de sistemas de monitoramento em conjunto com aplicações como o Zabbix-Proxy podem trazer benefícios inestimáveis.

Infraestruturas massivas espalhadas geograficamente: Este é o caso das *Smart grids*. Como proposto no item anterior, as fases de distribuição e transmissão, bem como as subestações no fim da fase de transmissão e início da de distribuição, têm muito a ganhar com implantações de sistema de gerência via SNMP. Mas já foi discutido que as *Smart grids* compreendem não apenas esses pontos, mas também as unidades consumidoras e os sistemas de microgeração. Como, então, seria possível a aplicação de um sistema com agente SNMPv1 sem suporte a mensagens ”trap” nesses cenários? Em casos de quantidades massivas de agentes, como esse, os quais envolvem milhões de dispositivos e diversas regulações entre prestadores e consumidores de serviços, as melhores abordagens parecem se apoiar na criação de redes de gerência específicas para essa finalidade. É fato que as infraestruturas de comunicações se apoiam nos postes, dutos e passagens subterrâneas para distribuição de seus serviços, e esses mesmos suportes são usados pelas redes elétricas, logo, os dois setores já estão intimamente ligados. Portanto, implementações de redes simples especí-

ficas para gerência de *Smart grids*, com baixa taxa de dados e uso de equipamentos com baixos requisitos de processamento, poderiam abrir espaço para o projeto de hierarquias de ”medidores-gerentes”, podendo-se, por exemplo, ter dispositivos gerentes de quadras, bairros, ruas, conjuntos de prédios, condomínios, entre outros. Por fim, por se tratar de um sistema de monitoramento robusto, de baixo custo, aberto e escalável, além de alinhado com os padrões mais universais de conexão, basta uma mínima disponibilidade de rede e haverá uma forma rápida, confiável e pouco onerosa de implantação do sistema. Como adendo, observa-se que nas propostas de trabalhos futuros ao fim deste documento, estão sugestões ainda mais escaláveis e fáceis de implantar, e todas as propostas continuam baseadas nos mesmos conceitos deste projeto, provando o nível de amadurecimento do framework SNMP padrão de gerência de redes.

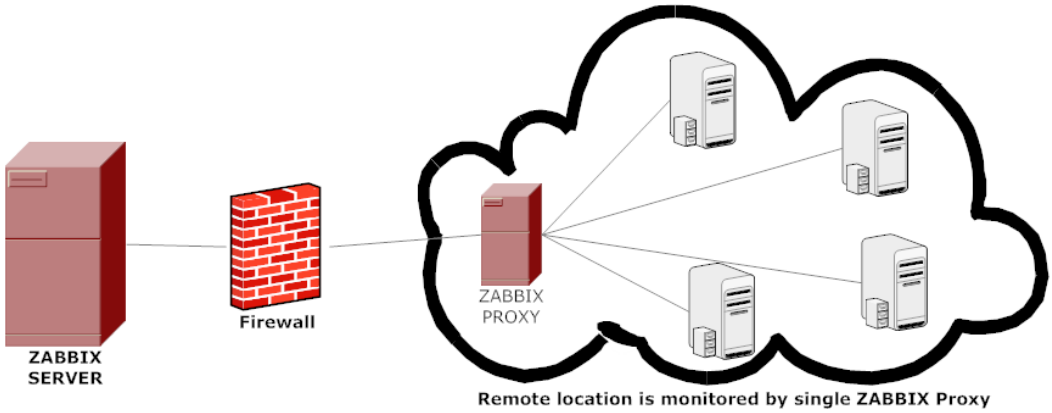

Figura 3.8: Exemplo de aplicações do Zabbix Proxy para resolver o já citado problema do NAT (Zabbix SIA,2019) [24].

Com o fim das propostas, proposições e especificações, o capítulo a seguir trará os resultados obtidos da instalação do sistema num ambiente real de um data center.

4 RESULTADOS OBTIDOS E DISCUSSÕES

A seguir, serão mostrados os resultados da implementação do sistema para um circuito trifásico. Note-se que, por se tratar de uma implementação (e não uma prototipação) foi necessário a confecção de enclausuramento do sistema e conectorização do mesmo. Os valores dos resistores foram escolhidos de acordo com a imagem 3.1. O valor do capacitor foi escolhido com base na ampla disponibilidade, visto que este não tem um valor exato no projeto (seu propósito no circuito é puramente absorver transientes). Adicionalmente, durante a implementação do sistema, optou-se pelo acréscimo de uma página web como painel (”dashboard”) para acompanhamento das leituras dos sensores e interface serial para configuração de data/hora e endereçamento IPv4, bem como envio contínuo das leituras dos sensores via interface serial. Ainda que nenhuma destas funções faça parte do projeto inicial ou sejam necessárias para atingir os objetivos finais, são interessantes para complementá-lo, torná-lo uma ferramenta mais completa e integrável.

4.1 MONTAGEM DO SISTEMA

A lista de componentes usados na montagem do sistema segue:

1. 1 (uma) placa ”Arduino Mega 2560 Rev3” [70];
2. 1 (uma) placa ”Ethernet Shield W5100”, da empresa Wiznet [68];
3. 5 (cinco) conectores XLR3 fêmeas;
4. 4 (quatro) conectores XLR3 machos;
5. 4 (quatro) sensores de corrente não-invasivos ”SCT-013 100A:50mA” da marca YHDC [64];
6. 4 (quatro) capacitores de 10uF;
7. 8 (oito) resistores de filme de carbono de 10kOhm;
8. 4 (quatro) resistores de filme de carbono de 33Ohm;
9. 15 fios jumpers.

As imagens 4.1 a 4.9 fornecem detalhes da montagem física do sistema. É importante observar que a configuração das portas e do funcionamento do sistema é livre, sendo limitado apenas às características do microcontrolador escolhido, portanto, optou-se pela montagem de um sistema com 5 portas para abrigar, futuramente, outros sensores (como temperatura ou abertura de porta).

Além disso, foram escolhidos 4 sensores de corrente para que o condutor neutro de uma instalação trifásica pudesse ser monitorado, e portanto, permitir verificações sobre o balanceamento geral do circuito.

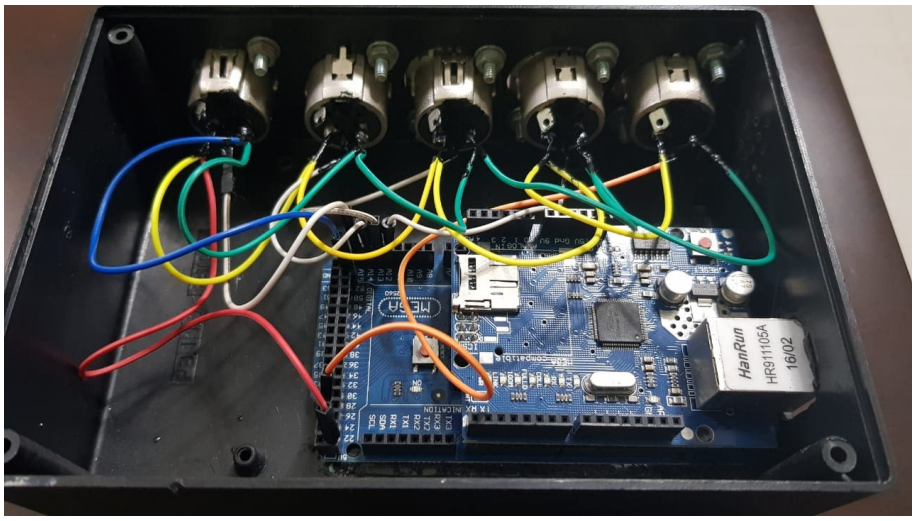

Figura 4.1: Visão em perspectiva da montagem.

Figura 4.2: Visão em perspectiva dos conectores e as ligações internas ao enclausuramento.

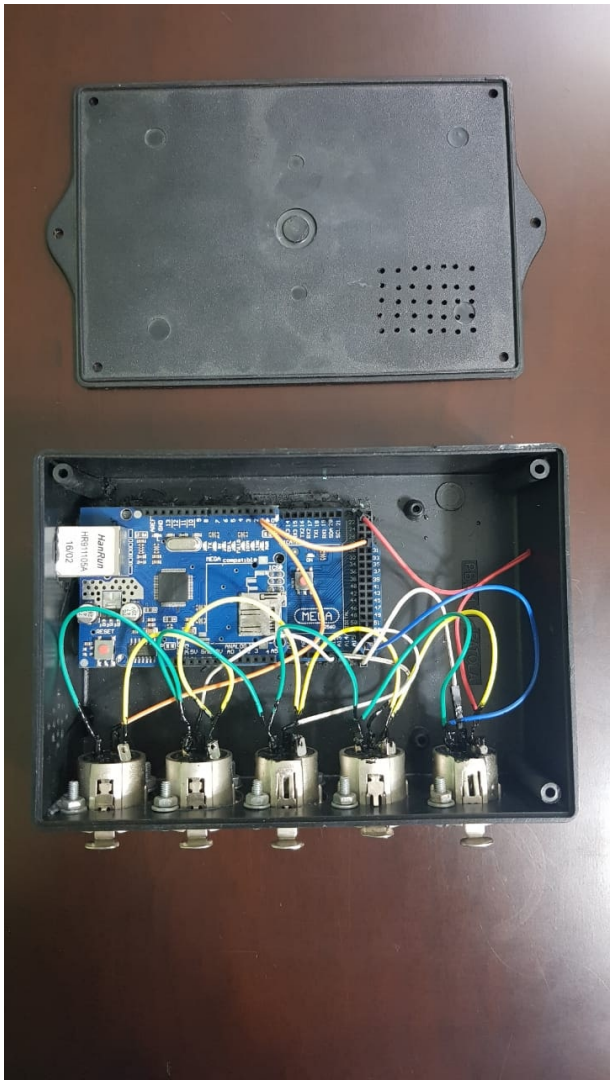

Figura 4.3: Visão aérea da montagem.

Figura 4.4: Visão frontal dos conectores de comunicação e alimentação do sistema.

Figura 4.5: Detalhe do sistema encapsulado e fechado.

Figura 4.6: Detalhe do transdutor do sensor de corrente não invasivo.

Figura 4.7: Detalhe da montagem do circuito da figura 5.3 dentro do conector XLR3 macho do sensor.

Figura 4.8: Visão do sensor conectorizado e pronto para uso.

Figura 4.9: Visão do sistema montado e pronto para uso.

4.2 APLICAÇÃO DO SISTEMA

As figuras 4.10, 4.11 e 4.12 mostram a ligação dos sensores e do sistema num quadro elétrico de baixa tensão exposto. É importante observar que essas conexões foram feitas com uso de equipamentos de proteção individual como luvas e calçados isolantes, em conformidade com instruções de um profissional certificado para tais trabalhos (segundo Norma Regulamentadora NR10 - ”Segurança em Instalações e Serviços em Eletricidade”). Note-se também que a organização na qual as fotos foram tiradas segue rígida política de segurança da informação e sigilo, por esse motivo, não serão divulgados dados e/ou referências do local.

Figura 4.10: Visão geral do quadro elétrico no qual se encontra o circuito a ser medido.

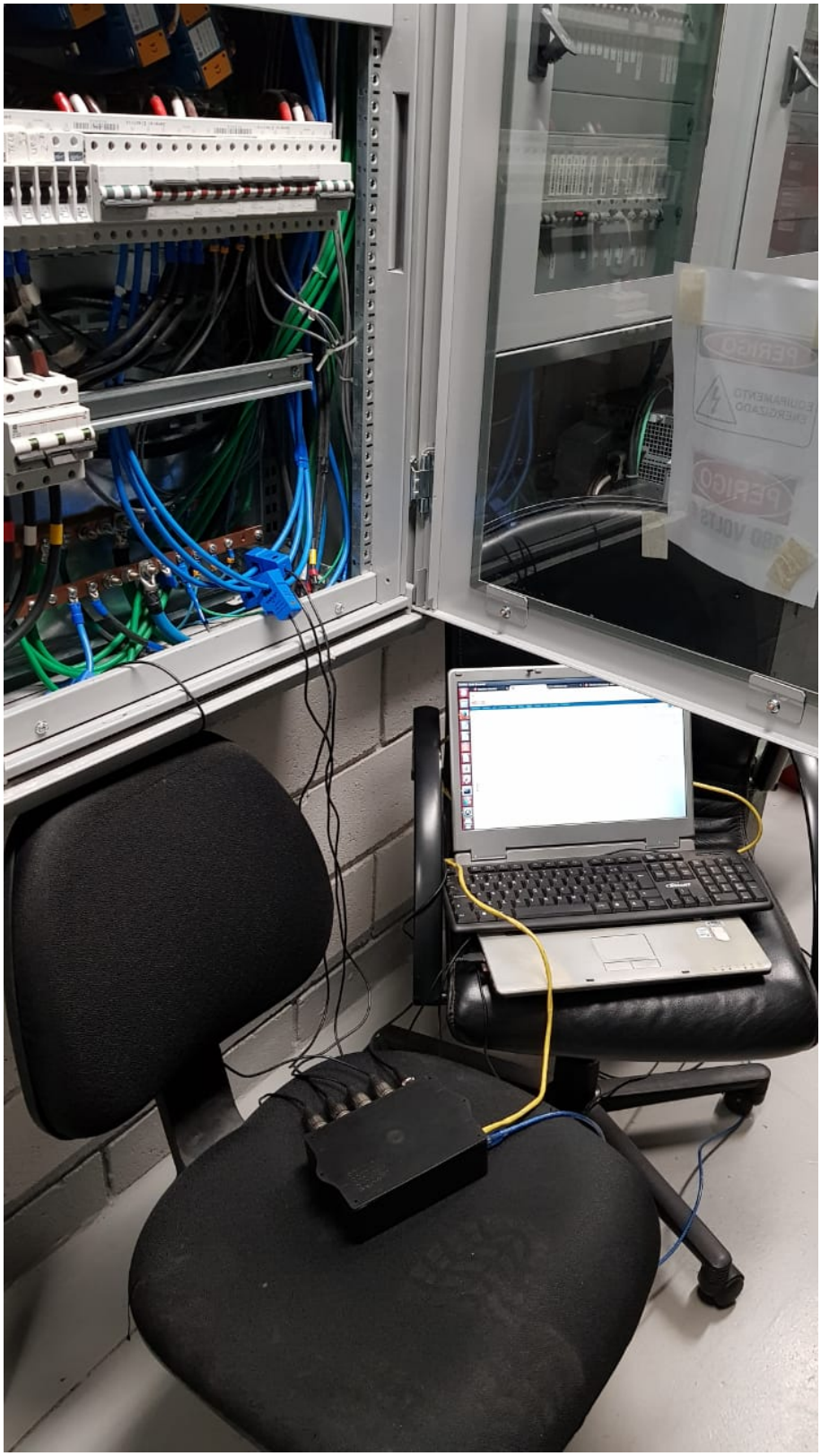

Figura 4.11: Visão do sistema instalado e pronto para testes (ao lado, notebook com o software gerente Zabbix em funcionamento).

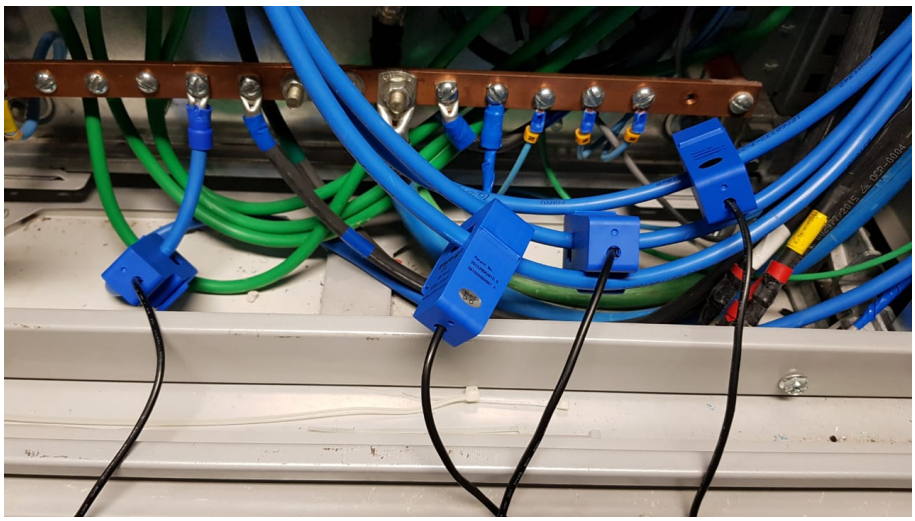

Figura 4.12: Visão dos sensores conectados aos condutores das fases e neutro do circuito trifásico de um sistema de refrigeração.

Na figura 4.13, o sistema foi configurado com um endereço IP fixo via interface serial e conectado via rede Ethernet a um computador com o software servidor Zabbix [25] instalado e configurado na mesma rede e com a mesma máscara de subrede. A imagem 4.14 mostra a criação de um ”host” no software para o sistema de monitoramento e a imagem 4.15 mostra a configuração de um item de monitoramento usando o protocolo SNMPv1 [26] e a OID correspondente para obter a corrente da fase 1 (sensor 0) sendo medida pela sistema. A figura 4.16 mostra o gráfico da obtenção dos valores de corrente total do sistema. A figura 4.17 mostra a página web para acompanhamento das leituras do sistema. As figuras 4.18, 4.19 e 4.20 mostram, respectivamente, a plotagem das correntes por fase (e neutro) e a corrente total (em vermelho), uma parte da lista de variáveis sendo requisitadas (chegando a mais de 25), e, por fim, o gráfico de consumo aparente, o qual acumulou dados de duas horas de funcionamento. Observe-se que a carga a qual estava sendo medida era um sistema de refrigeração predial de média potência, o qual tem comportamento cíclico. Chame-se atenção também para o fato de que os picos medidos foram reduzindo com o passar do tempo. Essas medições iniciaram-se no meio da tarde (quando há o pico de concentração de funcionários na empresa) e terminaram ao fim desta (quando o prédio já estava bem menos ocupado), ficando claro que o consumo do sistema reduziu seus picos de 40A para cerca de 30A, ou seja, aproximadamente 25% de queda. Sabendo que a maioria dos funcionários não tem acesso aos controles dos sistemas de refrigeração, poderia-se inferir que existe relação entre o calor decorrente dessa população de funcionários que deixou o local (calor esse que deixou de ser gerado) e a redução verificada na potência total da carga monitorada, pois seria necessário menos trabalho por parte dos motores para refrigerar o prédio.

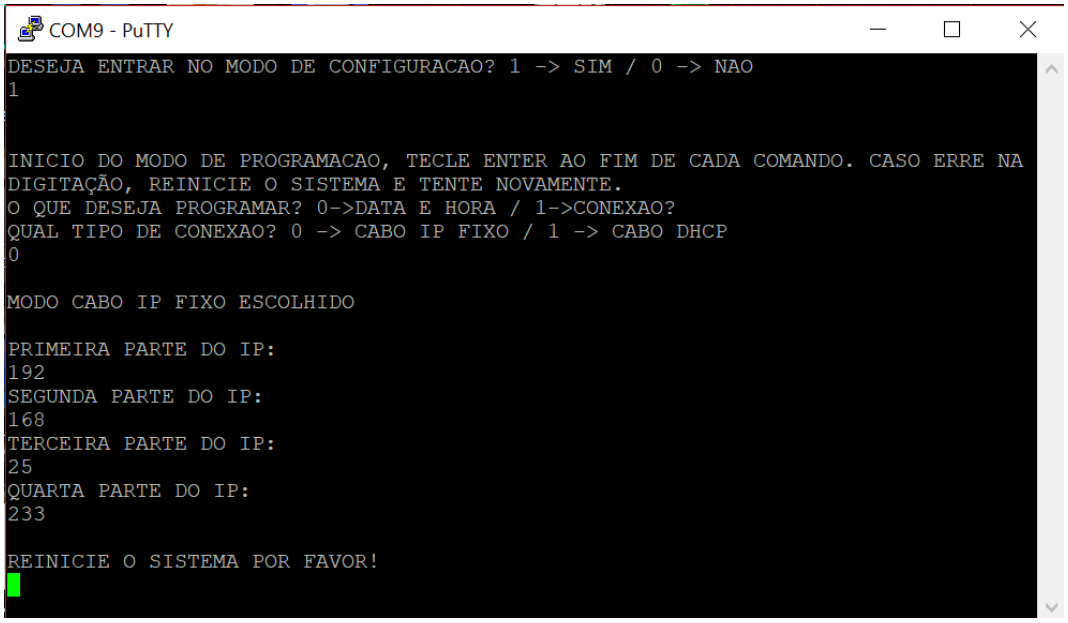

Figura 4.13: Detalhe da configuração do sistema com um endereço IPv4 fixo via interface serial.

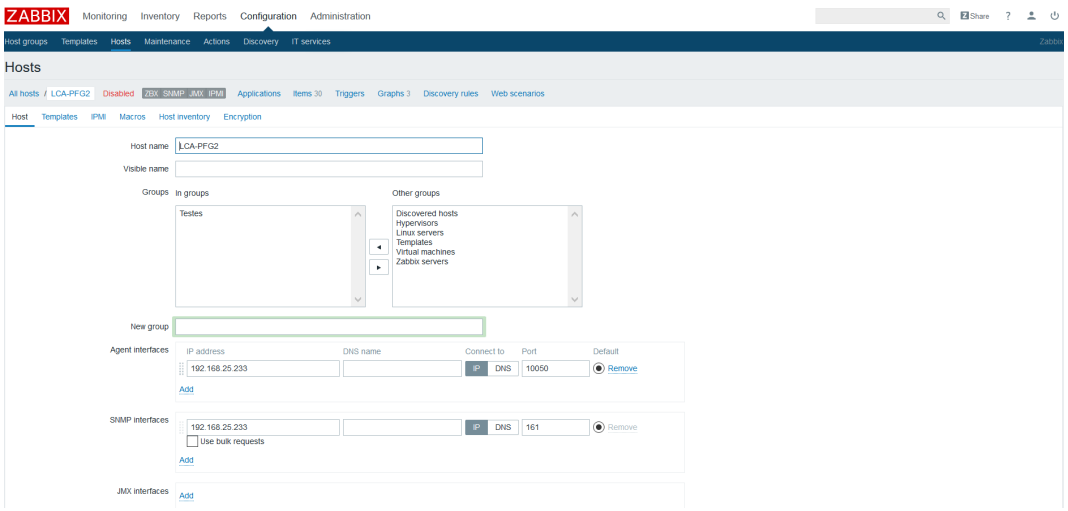

Figura 4.14: Detalhe da criação de ”host” no software Zabbix [25] para monitoramento do sistema.

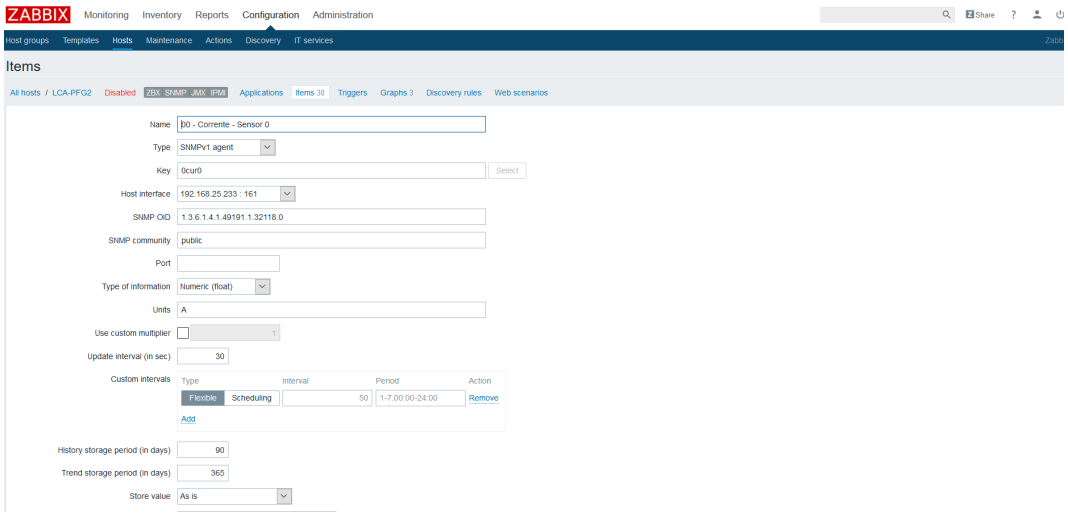

Figura 4.15: Detalhe da criação de item de monitoramento usando o protocolo SNMPv1 [26] e a OID correspondente para obter a corrente da fase 1 sendo medida pela sistema através do sensor 0.

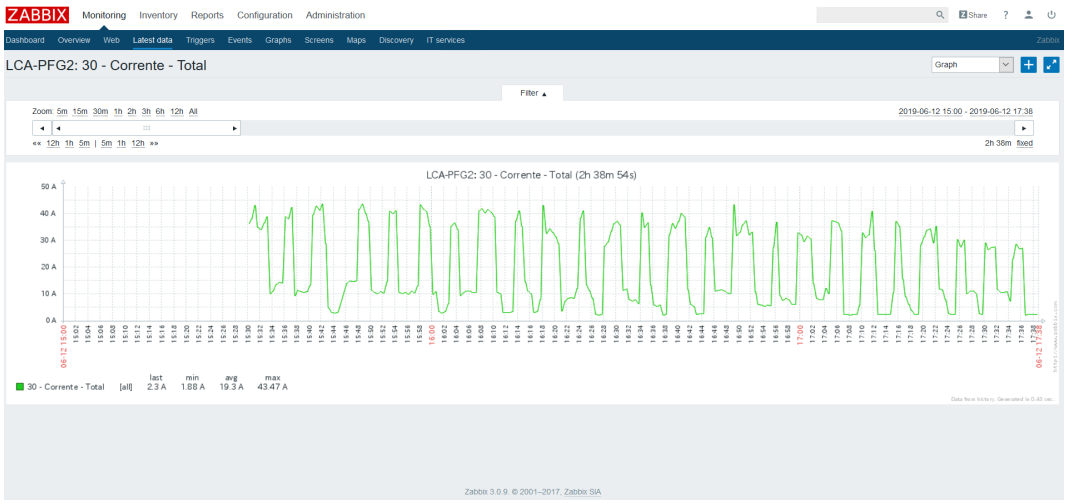

Figura 4.16: Gráfico sendo plotado com os valores de corrente total medida pelo sistema.

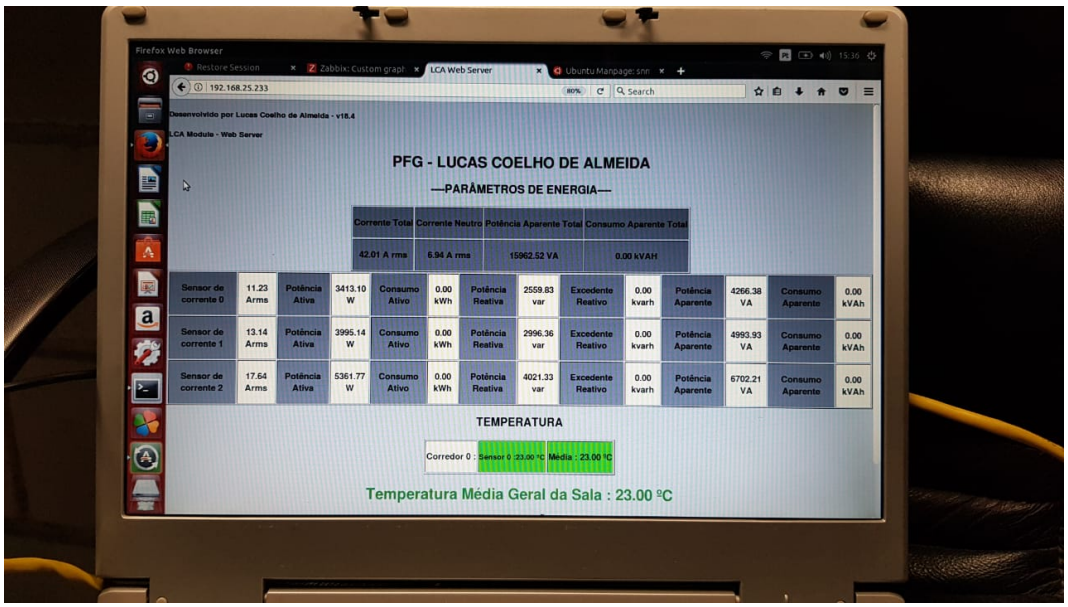

Figura 4.17: Página web com painel (”dashboard”) para acompanhamento das leituras dos sensores.

Figura 4.18: Gráfico conjunto das correntes de todos as três fases, terra e corrente total.

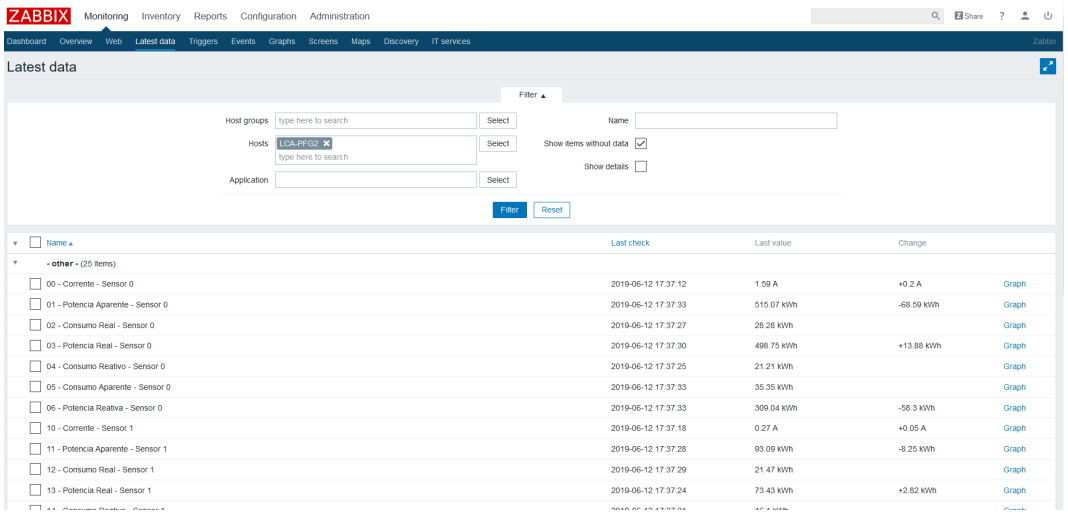

Figura 4.19: Detalhe da lista das últimas variáveis a serem requisitadas pelo gerente ao sistema.

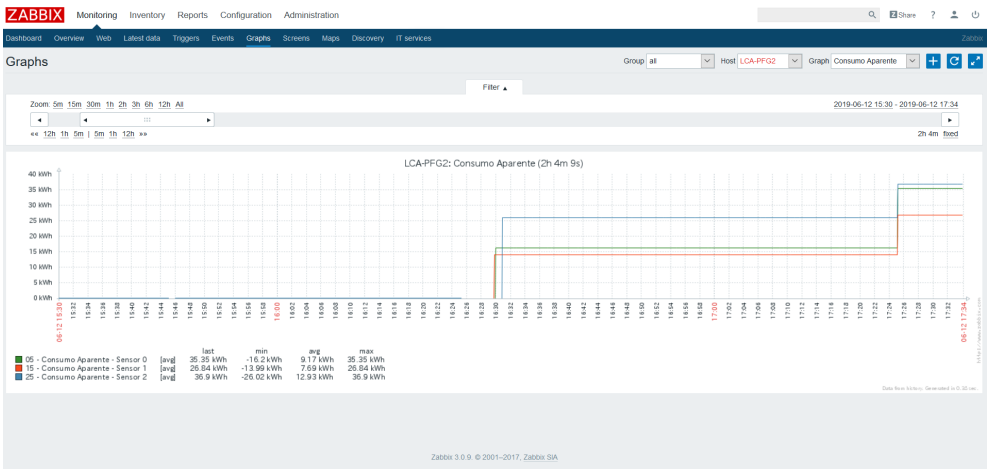

Figura 4.20: Gráfico do consumo aparente de energia por fase e total. Observa-se que esse valor é atualizado apenas a cada passagem completa de uma (1) hora.

Figura 4.21: Comparação entre a leitura do alicate amperímetro e do sistema para a fase 2. O alicate media 3.76A, enquanto o sistema, 3.56A, uma diferença de apenas 5%.

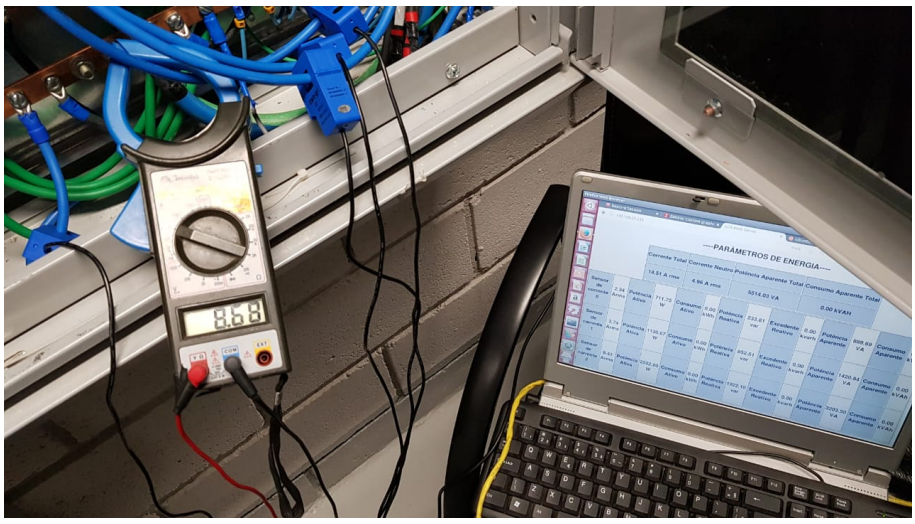

Figura 4.22: Outra comparação entre a leitura do alicate amperímetro e do sistema, agora para a fase 3. O alicate media 8.68A, enquanto o sistema, 8.43A, uma diferença de menos de 3%.

Ainda que o projeto tenha atingido seus objetivos, não se deve supor que este esteja completo e atenda de forma perfeita ao campo que se propôs (ainda mais quando se trata de um assunto tão novo quanto a eficiência energética na gestão de infraestruturas físicas). A seguir, os pontos principais nos quais se observam as limitações do projeto:

1. Em primeiro lugar, o sistema desenhado é bastante flexível e pode ser alterado com facilidade para aumentar a quantidade de sensores (e/ou seus tipos), operar de forma distribuída, enviar alertas de forma independente, entre outros. Contudo, sem o acréscimo da medição de tensão e fase de variáveis, é impossível evoluí-lo para o monitoramento da qualidade da energia, além de existir uma margem de erro considerável para fins de cálculos tarifários ao fixar o valor da tensão. Em outras palavras, o projeto do sistema é extremamente integrável com a operação usual de ambientes de TIC, porém, o caso ideal só se materializa quando a medição consegue trazer informações valiosas tais como: detecção de surtos, afundamentos, e até fator de potência em tempo real. Para a inclusão da medição de tensão e fase, entretanto, seria necessário observar normas e procedimentos mais rígidos de segurança para não acrescentar pontos de falha nas infraestruturas. Afinal, um pequeno surto para uma pequena fábrica poderia ser o suficiente para queimar o sistema e/ou iniciar um incêndio. Para ilustrar a dificuldade, a ANEEL - Agência Nacional de Energia Elétrica, é a responsável por divulgar vários documentos sobre os Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional, programa chamado PRODIST [83]. No módulo 5 desses procedimentos [84], são definidos os critérios para sistemas medidores de qualidade e consumo de energia elétrica. As exigências de precisão, armazenamento, métodos de medição, segurança de invólucro, garantia de inviolabilidade, entre outros, fogem completamente ao escopo deste projeto, mostrando o quão oneroso pode ser desenvolver (e implantar) um sistema licenciado e em conformidade com a agência reguladora. Portanto, o sistema proposto serve apenas como auxílio à gestão, e não como substituição aos equipamentos licenciados.

2. Outro fator complicador para a medição de correntes é a dificuldade de confecção e/ou compra de transdutores para grandes barramentos. A maioria dos condutores de cabos não apresentam correntes muito superiores a 150A, pois o efeito Joule começa a se apresentar de forma mais proeminente partir desses valores, logo, ainda é fácil encontrar transformadores do tipo alicate para a medição. No entanto, com a difusão dos equipamentos eletroeletrônicos, mesmo um prédio pequeno pode ter uma planta que demanda barramentos de metal para a distribuição de energia nos quadros principais. Quando esses barramentos são de plantas projetadas para cargas na ordem dos mega Watts, as correntes elétricas chegam a mais de 500A, e os transformadores de corrente próprios para esses casos atingem preços bastante elevados, além de atenderem a diversas normas adicionais de segurança e precisão. Por esse motivo, o sistema apresentado neste projeto é indicado para os quadros gerais de instalações de pequeno porte ou quadros intermediários para instalações de grande porte.

3. Um ponto importante a ser abordado é a qualidade do multímetro usado nas medições e a relação com o método de leitura do sistema proposto. O termo comercial ”true RMS” designa equipamentos que conseguem medir valores eficazes de quaisquer sinais, não apenas senoidais, logo, instrumentos desse tipo conseguem ter maior confiabilidade no uso, já que mesmo que a onda da tensão/corrente esteja distorcida, suas leituras serão bastante precisas. O multímetro usado nas figuras não dispõe desse tipo de leitura, logo, os valores apresentados são apenas uma resposta média a um sinal considerado perfeitamente senoidal (situação que não ocorre na realidade). O método de medição da biblioteca ”emonLib” usada no projeto, por outro lado, funciona de forma similar à citada função ”true RMS”, portanto, num ensaio de testes mais criterioso e com foco em precisão, dever-se-ia usar instrumentos que dispusessem desse método para aferições e conclusões mais acertadas.

4. O cálculo do consumo, conforme [84], deve resultar em valores de unidade em kWh. Adicionalmente, os cálculos tarifários são realizados mês a mês, logo, fica clara a necessidade de inclusão das variáveis de tempo. Inicialmente, o sistema foi desenhado com um módulo RTC, ou Real Time Clock (Relógio de Tempo Real), tal qual um computador de uso pessoal, o qual, mesmo desligado, continua acompanhando o tempo. Contudo, verificou-se que os módulos RTC para plataformas abertas não são de ampla disponibilidade, logo, o uso desses iria contra as premissas do projeto. De outra forma, pensou-se em obter a data e hora através de um servidor NTP (Network Time Protocol - Protocolo de Tempo da Internet [85]), contudo, fugiria ao escopo deste projeto a exigência desse tipo de serviço no ambiente a ser instalado, e o consumo de um servidor NTP aberto, na Internet, iria contra as diretrizes de segurança da maior parte das organizações. A solução, por fim, foi encontrada ao se analisar os casos de uso do sistema. Para os interessados puramente na obtenção das leituras, para cálculos posteriores via software próprio, não seria necessário nem ao menos a configuração de data e hora. Contudo, para os interessados em medir consumo, bastaria que esses, ao instalar o sistema, configurassem, via interface serial, o dia, mês e a hora. De posse desses dados, e sabendo a velocidade do microcontrolador, seria possível medir a passagem do tempo, com uma margem de erro de 1 (uma) hora. Contudo, existem limitações nessa abordagem: após um longo período de tempo, é possível que a margem de erro aumente cada vez mais, principalmente ao se considerar os anos bissextos. Além disso, se o sistema for desligado por longos períodos de tempo, ao ser religado, este continua com a última hora e data contabilizados, logo, a cada nova instalação, seria necessário reconfigurar tais parâmetros. Apesar de, à primeira vista parecer dispendioso, verificou-se o atendimento pleno dos objetivos do projeto, sendo este o método de contagem de tempo escolhido (a cada hora decorrida, contabiliza-se o consumo em kWh, e a cada mês decorrido, o consumo é zerado). A melhoria, portanto, seria alcançada com o uso do protocolo NTP [85] ou com a interface com outros módulos com circuitos RTC.

5. Ainda que as justificativas sobre o uso de sistemas cabeados sejam verdadeiras, a dependência de cabos é uma característica onerosa e dispendiosa para o sistema. Na configuração ideal, os transformadores de corrente se comunicariam sem fios com uma central ligada

numa rede padrão Ethernet [34]. O melhor candidato para protocolo sem fios seria o Zigbee, o qual já está bastante maduro no mercado (tendo até sua própria aliança [86]) e logo deverá ter implementações mais seguras. Com o uso de tecnologias sem fios mais modernas, seria possível reduzir ainda mais o custo e aumentar a granularidade das medições (por exemplo, medindo cada equipamento/motor/circuito de forma individual), bem como facilitar a implantação e a futura evolução do sistema para o campo da qualidade de energia. O maior problema, porém, é que não existem muitas plataformas abertas com suporte a esses protocolos, e quando existem, não são de ampla disponibilidade. A plataforma Arduino [67], por outro lado, ainda é a mais difundida no mundo, por isso foi a escolhida.

6. Um último detalhe é sobre a utilização do sistema. Ainda não são todos os gestores que se interessam em acompanhar de perto suas infraestruturas e projetar as mudanças necessárias, ou mesmo documentar as características de seus ambientes. De fato, um sistema de medição apenas permite que grandezas antes ignoradas possam, agora, ser observadas continuamente, porém, não são de forma alguma capazes de trazer retorno de forma autônoma. A medição é uma ferramenta poderosa para tomada de decisão, logo, é necessário que os gestores que se propõem a participar dos movimentos disruptivos na gestão de eficiência energética tomem decisões sobre redução de consumo, balanceamento de cargas, escalabilidade de infraestrutura, controle do ciclo de vida de ativos, comissionamento e descomissionamento de sistemas, entre outros. O primeiro passo, no entanto, sempre será o monitoramento. Um profissional qualificado e disposto não pode tomar decisões sobre sua infraestrutura sem medir, sem conhecer o estado atual da mesma, no entanto, mesmo o gestor com pouca experiência consegue extrair informações valiosas daquilo que é constantemente mensurado e apresentado de forma fácil e intuitivamente integrada à operação.

5 CONCLUSÃO

O objetivo deste trabalho foi inspirar novos projetos e mostrar o quão fácil e descomplicado pode ser a implantação de sistemas de medição de consumo em infraestruturas físicas de TIC. Apesar de a eficiência energética ser um tema que engloba o mundo todo, são várias as fontes de pesquisa apontando para o fato de que os data centers e as infraestruturas críticas de comunicação estão aumentando seu consumo de energia de forma muito mais rápida que o restante dos setores. Logo, se existe uma classe de profissionais que tem, no dia a dia, o dever de pensar e projetar de forma inovadora, com certeza os gestores de data centers estão entre os principais candidatos. Além disso, a gestão de eficiência energética não é mais apenas um trabalho adicional para salvar o meio-ambiente, tão importante quanto, essas atitudes economizam custos operacionais e reduzem falhas, logo, aplicar todos esses conceitos significa, de forma quase que instantânea, melhorar a receita das companhias e a sustentabilidade da Indústria como um todo. Porém, existe um longo caminho em direção à redução e consumo consciente e controlado: hardwares precisam ser redesenhados, softwares precisam ser melhorados, os motores devem ser mais eficientes, a gestão precisa ter mais dados e ser mais proativa e qualificada... O primeiro passo, contudo, é medir, de forma simples, eficiente, rápida e precisa o bastante para se conhecer a infraestrutura. Dessas mesmas ideias têm surgidos movimentos disruptivos de gerência em outros setores, e um deles é o das redes elétricas inteligentes. Foi possível analisar, por fim, que o framework SNMP de gerência constitui um dos melhores candidatos possíveis para a rápida e descomplicada implantação da gerência em todas as fases do setor elétrico, sendo esse um modelo robusto e globalmente aceito por pelo menos 2 décadas.

5.1 TRABALHOS FUTUROS

Os assuntos apresentados constituem campo inesgotável de discussão tanto no âmbito acadêmico quanto na Indústria. Ainda que o projeto resolva problemas de um escopo amplo, ainda existem diversos trabalhos que decorrem do alinhamentos dos conceitos de Gerência de Redes e infraestruturas físicas, e dentre eles, cita-se alguns dos mais relevantes:

1. *Aplicações em Smart grids:* O projeto proposto indica que as infraestruturas de comunicação e de energia já estão intimamente relacionadas, bastante lembrar que os postes públicos são usados como suporte de difusão de ambos setores, logo, a implantação de redes de gerência para a rede elétrica seria fácil e menos onerosa que outras tecnologias. No entanto, na seção ”Protocolo SNMP” do Capítulo ”Fundamentação Teórica e Estado da Arte” é possível contemplar mais uma dica de que o SNMP consegue tornar essa empreitada ainda menos custosa e mais interessante: a PDU do tipo ”trap” do SNMPv1 tem um campo chamado ”Agent-addr”, o qual carrega o endereço do agente que gerou a mensagem SNMP. Logo,

Independentemente de o agente estar sendo traduzido por um NAT (o qual atua apenas na Camada de Rede da pilha TCP/IP), se existe um gerente com endereço IP público, este consegue receber mensagens ”trap” SNMPv1 e identificar suas fontes sem impedimentos. Portanto, para a fase da distribuição de energia observada na seção ”*Smart grids*” do mesmo capítulo, seria interessante analisar um cenário no qual existem portais públicos de gerência de *Smart grids* na internet e todas as unidades consumidoras de energia (como casas e prédios) são livres para ativar dispositivos em sua conexão de Internet local, os quais enviariam ”traps” para esses portais e se cadastrariam de forma automática, talvez até mesmo implementando aspectos do SNMPv3. Características como o baixo uso de recursos, o baixo consumo de banda (quando as taxas de envio são controladas), a escalabilidade do modelo e a qualidade dos meios de comunicação atuais (nos quais a perda de mensagens vem se tornando cada vez mais rara), além da possibilidade de recebimento de dados de forma assíncrona pelos gerentes, fazem dessa sugestão uma ótima consideração para padrão de gerência do setor.

2. *Otimização do sistema:* O sistema proposto tem limitações e carece de um modelo padronizado e amplamente aceito de MIB. Além disso, não implementa outras versões do protocolo SNMP e nem o tipo ”get-next” do SNMPv1. Atender ao restante das especificações dos protocolos e das MIB’s existentes possibilitaria o uso de aplicações de auto descoberta e até de programas de navegação como os famosos ” browsers para MIB’s”. Além disso, existem diversos ganhos (os quais não foram abordados) envolvendo a medição sistemáticas de parâmetros de qualidade de energia. O aprimoramento do sistema para atender a novas variáveis seria uma adição de grande valor para os propósitos do projeto. Adicionalmente, ainda existem outras aplicações para o sistema tais como controle de acesso, monitoramento de temperaturas, automação (usando as mensagens ”set” do SNMP), entre diversos outros, bastando a implementação em hardware e adição das OID’s pertinentes à MIB já definida para o sistema, criando novos ramos.

3. *Implementações de Segurança:* Como o framework padrão SNMP de gerência é baseado no protocolo UDP, existem alguns problemas de segurança que nem a versão 3 do SNMP resolve, como os ataques DOS (Denial of Service - Negação de Serviço), os quais poderiam ser problemáticos em cenários de endereços públicos de gerentes. Entretanto, por se tratar de um protocolo leve, é extremamente bem vinda a investigação sobre a possibilidade de aplicação de filtros inteligentes de mensagens, analisando a origem, periodicidade e outras variáveis através de técnicas de aprendizado de máquina ou Inteligência Artificial. Some-se o fato de constituir campo de excelente estudo da aplicação de assinaturas digitais, visto que cada unidade consumidora seria autenticada através de sua chave, que poderia ser uma assinatura digital gerada por uma entidade reguladora, como as agências reguladoras (ANATEL e ANEEL, por exemplo).

4. *Investigação de limitações do modelo:* Novamente, dado o fato de o SNMP ser baseado no protocolo UDP, e pelo fato de a Internet ser uma rede pública heterogênea, num cenário em

que milhões/bilhões de dispositivos enviam dados pela Internet, mesmo que cada dispositivo envie mensagens a cada período de tempo determinado (300 segundos, por exemplo), pode ser que exista uma quantidade de dispositivos a partir da qual a chance de muitos enviarem ao mesmo tempo e colapsar a rede seja grande, tal qual os protocolos de acesso ao meio da Camada de Enlace da pilha TCP/IP, os quais todos têm limitações sobre seu desempenho em relação à quantidade de dispositivos compartilhando o meio. Um estudo como esse poderia avaliar, simultaneamente, o impacto do crescimento desordenado de dispositivos de IoT ligados diretamente à Internet.

5. *Proposição de novos protocolos e padrões:* A reunião de todos os conceitos e lógicas de projeto leva à identificação de um campo extremamente promissor: a especificação de novos padrões de estruturas de bases de dados gerenciáveis (MIB's) e de protocolos de gerência sob o ponto de vista do gerente. Isso porque, ao elevar a quantidade de dispositivos à casa de milhões/bilhões, a gerência e os serviços de recebimento e envio de dados precisam todos de revisão, logo, propor uma nova MIB com rotinas de normalização e/ou reorganização dos dados em árvores AVL, conforme visto na seção "Árvores de Nomes" do Capítulo "Fundamentação Teórica e Estado da Arte", poderia trazer saltos enormes de performance. Adicionalmente, poderia-se propor novas versões do protocolo SNMP específicas para a gerência de grandes infraestruturas físicas, abrangendo usinas de geração, redes elétricas, malhas metroviárias, entre vários outros.

REFERÊNCIAS BIBLIOGRÁFICAS

1 COMPUTER HISTORY MUSEUM. *Professor Kenneth N. Stevens, Gordon Bell and the TX-0 computer at MIT*. Disponível em: <https://www.computerhistory.org/pdp-1/e16344596cdd060839c6e72ae9c26379/>. Acesso em: 27 jun. 2019.

2 DATACENTER DYNAMICS. *Huge Networks utiliza data center da Equinix para serviços de segurança cibernética*. Disponível em: <http://www.datacenterdynamics.com.br/focus/archive/2019/02/huge-networks-utiliza-data-center-da-equinix-para-servi\%C3\%A7os-de-seguran\%C3\%A7a-cibern>. Acesso em: 27 jun. 2019.

3 TELECOMUNICAçõES BRASILEIRAS - S.A. *Carta de Serviços ao Usuário*. Disponível em: <https://www.telebras.com.br/documentos/CARTA_SERVICO_USUARIO.pdf>. Acesso em: 27 jun. 2019.

4 FOLHA DE SãO PAULO. *Veja os efeitos do apagão em todo o Brasil*. Disponível em: <https://www1.folha.uol.com.br/folha/dinheiro/ult91u40078.shtml>. Acesso em: 27 jun. 2019.

5 ANEEL - AGêNCIA NACIONAL DE ENERGIA ELéTRICA DO BRASIL. *Perdas de Energia*. Disponível em: <http://www2.aneel.gov.br/area.cfm?idArea=801&idPerfil=4>. Acesso em: 27 jun. 2019.

6 CERNE - CENTRO DE ESTRATéGIAS EM RECURSOS NATURAIS E ENERGIA. *Energia solar avança no Brasil e atrai empresas*. Disponível em: <http://cerne.org.br/energia-solar-avanca-no-brasil-e-atrai-empresas/>. Acesso em: 27 jun. 2019.

7 3D PRINTING INDUSTRY. *The factory of the future with Elysium's Industry 4.0 solution*. Disponível em: <https://3dprintingindustry.com/news/factory-future-elysiums-industry-4-0-solution-101815/>. Acesso em: 27 jun. 2019.

8 DATA CENTER BASICS. *SNMP basic components and their functionalities*. Disponível em: <http://dcbasics.blogspot.com/2015/08/simple-network-management-protocol.html>. Acesso em: 27 jun. 2019.

9 UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. *A Composição do SNMP*. Disponível em: <https://www.gta.ufrj.br/grad/00_1/joao/comp.htm>. Acesso em: 27 jun. 2019.

10 WIKIPéDIA. *Árvore filogenética*. Disponível em: <https://pt.wikipedia.org/wiki/\%C3\%81rvore_filogen\%C3\%A9tica>. Acesso em: 27 jun. 2019.

11 O'REILLY AND ASSOCIATES. *The Structure of Management Information*. Disponível em: <https://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_03.htm>. Acesso em: 27 jun. 2019.

12 IME/USP - INSTITUTO DE MATEMáTICA E ESTATíSTICA/UNIVERSIDADE DE SãO PAULO. *Árvores binárias - Paulo Feofiloff*. Disponível em: <https://www.ime.usp.br/~pf/algoritmos/aulas/bint.html>. Acesso em: 27 jun. 2019.

13 KEITH W. ROSS AND JAMES F. KUROSE. *Connectionless Transport: UDP*. Disponível em: <https://www.net.t-labs.tu-berlin.de/teaching/computer_networking/03.03.htm>. Acesso em: 27 jun. 2019.

14 CHARLES M. KOZIEROK. *SNMPv1 Common PDU Format*. Disponível em: <http://www.tcpipguide.com/free/t_SNMPVersion1SNMPv1MessageFormat-2.htm>. Acesso em: 27 jun. 2019.

15 CHARLES M. KOZIEROK. *SNMPv1 Trap-PDU Format*. Disponível em: <http://www.tcpipguide.com/free/t_SNMPVersion1SNMPv1MessageFormat-3.htm>. Acesso em: 27 jun. 2019.

16 COOPERATI. *O Protocolo SNMP*. Disponível em: <http://cooperati.com.br/2011/09/20/o-protocolo-snmp/>. Acesso em: 27 jun. 2019.

17 INSTITUTO FEDERAL SANTA CATARINA - SãO JOSé. *NAT*. Disponível em: <https://wiki.sj.ifsc.edu.br/wiki/index.php/NATf>. Acesso em: 27 jun. 2019.

18 HENRIQUE FASSI. *Comparativo entre as versões do SNMP*. Disponível em: <http://www.fassi.eti.br/artigos/gerencia-de-redes/comparativo-entre-as-versoes-do-snmp>. Acesso em: 27 jun. 2019.

19 WIKIPéDIA. *Válvula termiônica*. Disponível em: <https://pt.wikipedia.org/wiki/V\%C3\%A1lvula_termi\%C3\%B4nica>. Acesso em: 27 jun. 2019.

20 TECH DIFFERENCES. *Difference Between EPROM and EEPROM*. Disponível em: <https://techdifferences.com/difference-between-eprom-and-eeprom.html>. Acesso em: 27 jun. 2019.

21 WIKIPéDIA. *Intel 8051*. Disponível em: <https://pt.wikipedia.org/wiki/Intel_8051>. Acesso em: 27 jun. 2019.

22 CIRCUITSTODAY. *Basics of Microcontrollers*. Disponível em: <http://www.circuitstoday.com/basics-of-microcontrollers>. Acesso em: 27 jun. 2019.

23 OPEN ENERGY MONITOR. *CT Sensors - Interfacing with an Arduino*. Disponível em: <https://learn.openenergymonitor.org/electricity-monitoring/ct-sensors/interface-with-arduino>. Acesso em: 27 jun. 2019.

24 ZABBIX Documentation 3.0 - Proxies. Disponível em: <https://www.zabbix.com/documentation/3.0/manual/distributed_monitoring/proxies>. Acesso em: 27 jun. 2019.

25 ZABBIX ORGANIZATION. *Zabbix*. Disponível em: <https://zabbix.org/wiki/Main_Page>. Acesso em: 08 dec. 2018.

26 NETWORK WORKING GROUP. *SNMP - RFC 1157*. Disponível em: <https://www.ietf.org/rfc/rfc1157.txt>. Acesso em: 08 dec. 2018.

27 PONEMON, I. *Cost to Support Compute Capacity - Data Center Performance Benchmark Series*. 2016. 1–14 p.

28 DATACENTER DYNAMICS. *80% dos custos anuais do data center vêm de despesas com energia e operacionais, diz relatório da Emerson Network Power*. Disponível em: <http://www.datacenterdynamics.com.br/focus/archive/2016/11/80-dos-custos-anuais-do-data-center-v\%C3\%AAm-de-despesas-com-energia-e-operacionais>. Acesso em: 08 dec. 2018.

29 KOOMEY, J. G. Worldwide electricity used in data centers. *Environmental Research Letters - IOPscience*, v. 3, p. 1–1, 2008.

30 KOOMEY, J. G. Growth in data center electricity use 2005 to 2010. *Analytics Press and at the request of The New York Times*, v. 1, p. 1–24, 2011.

31 HINTEMANN, R. Energy consumption of data centers continues to increase – 2015 update. *Borderstep Institute analysis based on a study for the Federal Ministry of Economic Affairs of Germany*, v. 1, p. 1–3, 2015.

32 US DEPARTMENT OF ENERGY. *Center of Expertise for Energy Efficiency in Data Centers of the United States*. Disponível em: <https://datacenters.lbl.gov/>. Acesso em: 08 dec. 2018.

33 SHEHABI-SMITH-SARTOR, A. S. D. *United States Data Center Energy Usage Report*. 2016. 1–65 p.

34 ETHERNET WORKING GROUP. *IEEE 802.3 ETHERNET WORKING GROUP*. Disponível em: <http://www.ieee802.org/3/>. Acesso em: 08 dec. 2018.

35 BRASIL, M. de Minas e Energia do. *Grupo de Trabalho de Redes Elétricas Inteligentes do Ministério de Minas e Energia do Brasil*. 2010. 1–225 p.

36 BRASIL, A. A. N. de Energia Elétrica do. *RESOLUÇÃO NORMATIVA Nº 482, DE 17 DE ABRIL DE 2012*. 2012. 1–12 p.

37 PRESIDêNCIA DA REPúBLICA DO BRASIL. *Artigo 14º do Decreto Lei nº 5.163/2004*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5163.htm>. Acesso em: 31 may 2019.

38 INTERNET STANDARD. *DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION - RFC 791*. Disponível em: <https://tools.ietf.org/html/rfc791>. Acesso em: 31 may 2019.

39 NETWORK WORKING GROUP. *Internet Protocol, Version 6 (IPv6) Specification - RFC 2460*. Disponível em: <https://www.ietf.org/rfc/rfc2460.txt>. Acesso em: 31 may 2019.

40 TELECOM ITALIA S.P.A. *Towards a definition of the Internet of Things (IoT)*. Disponível em: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf>. Acesso em: 31 may 2019.

41 GARTNER GROUP. *Definition of the Internet of Things (IoT)*. Disponível em: <https://www.gartner.com/it-glossary/internet-of-things/>. Acesso em: 31 may 2019.

42 MINISTERIO DA INDUSTRIA, COMERCIO E SERVICOS DO GOVERNO FEDERAL DO BRASIL. *Agenda brasileira para a Indústria 4.0*. Disponível em: <http://www.industria40.gov.br/>. Acesso em: 02 jun. 2019.

43 KUROSE, K. W. R. J. F. *Redes de Computadores e a Internet - 5a Edição*. [S.l.]: Pearson Education do Brasil, 2010.

44 NETWORK WORKING GROUP. *Introduction and Applicability Statements for Internet Standard Management Framework - RFC 3410*. Disponível em: <https://tools.ietf.org/html/rfc3410>. Acesso em: 02 jun. 2019.

45 NETWORK WORKING GROUP. *Introduction to Version 3 of the Internet-standard Network Management Framework - RFC 2570*. Disponível em: <https://tools.ietf.org/html/rfc2570>. Acesso em: 02 jun. 2019.

46 NAGIOS ORGANIZATION. *Nagios*. Disponível em: <https://www.nagios.org/>. Acesso em: 08 dec. 2018.

47 ZABBIX ORGANIZATION. *Zabbix Agent*. Disponível em: <https://www.zabbix.com/zabbix_agent>. Acesso em: 31 may 2019.

48 NETWORK WORKING GROUP. *MIB-II - RFC1213*. Disponível em: <https://tools.ietf.org/html/rfc1213>. Acesso em: 08 dec. 2018.

49 NETWORK WORKING GROUP. *Management Information Base for Network Management of TCP/IP-based internets - RFC 1156*. Disponível em: <https://tools.ietf.org/html/rfc1156>. Acesso em: 02 jun. 2019.

50 NETWORK WORKING GROUP. *Structure of Management Information Version 2 (SMIv2) - RFC 2578*. Disponível em: <https://tools.ietf.org/html/rfc2578>. Acesso em: 02 jun. 2019.

51 TELECOMMUNICATIONS STANDARDIZATION SECTOR. *OID project*. Disponível em: <https://www.itu.int/en/ITU-T/asn1/Pages/OID-project.aspx>. Acesso em: 02 jun. 2019.

52 ORANGE S.A. *Open Object Identifier (OID) Repository*. Disponível em: <http://www.oid-info.com/>. Acesso em: 02 jun. 2019.

53 NETWORK WORKING GROUP. *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) - RFC 3416*. Disponível em: <https://www.ietf.org/rfc/rfc3416.txt?number=3416>. Acesso em: 02 jun. 2019.

54 NETWORK WORKING GROUP. *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) - RFC 3414*. Disponível em: <https://tools.ietf.org/html/rfc3414>. Acesso em: 02 jun. 2019.

55 ERIC C. ROSEN AND BOLT BERANEK AND NEWMAN INC. *Vulnerabilities of Network Control Protocols: An Example - RFC 789*. Disponível em: <https://tools.ietf.org/html/rfc789.html>. Acesso em: 02 jun. 2019.

56 NETWORK WORKING GROUP. *A Simple Gateway Monitoring Protocol - RFC 1028*. Disponível em: <https://tools.ietf.org/rfc/rfc1028.txt>. Acesso em: 02 jun. 2019.

57 TELECOMMUNICATION STANDARDIZATION SECTOR. *X.711 : Information technology - Open Systems Interconnection - Common Management Information Protocol: Specification*. Disponível em: <https://www.itu.int/rec/T-REC-X.711/en/>. Acesso em: 02 jun. 2019.

58 NETWORK WORKING GROUP. *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework - RFC 3584*. Disponível em: <https://tools.ietf.org/html/rfc3584>. Acesso em: 02 jun. 2019.

59 INTERNET STANDARD. *User Datagram Protocol - RFC768*. Disponível em: <https://tools.ietf.org/html/rfc768>. Acesso em: 08 dec. 2018.

60 NETWORK WORKING GROUP. *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) - RFC 2275*. Disponível em: <https://tools.ietf.org/html/rfc2275>. Acesso em: 02 jun. 2019.

61 SADIKU, M. N. O. *Elementos de Eletromagnetismo*. [S.l.]: Bookman Companhia Editora LTDA., 2010.

62 IRWIN, J. D. *Análise Básica de Circuitos para Engenharia*. [S.l.]: LTC - Livros Técnicos e Científicos Editora S.A., 2003.

63 SCHUERZ, P.; MONK, S. *Practical Electronics for Inventors*. [S.l.]: McGraw-Hill Education, 2016.

64 BEIJING YAOHUADECHANG ELECTRONIC CO. AND OPENENERGYMONITOR ORGANIZATION. *Yhdc SCT-013-000 Current Transformer*. Disponível em: <https://learn.openenergymonitor.org/electricity-monitoring/ct-sensors/files/YhdcCTReportIss6.pdf>. Acesso em: 08 dec. 2018.

65 MINISTéRIO DA ECONOMIA DO BRASIL. *NR 10–SEGURANÇA EM INSTALAÇÕES E SERVIÇOS EM ELETRICIDADE*. Disponível em: <http://trabalho.gov.br/images/Documentos/SST/NR/NR10.pdf>. Acesso em: 27 jun. 2019.

66 THE WORKING GROUP FOR WLAN STANDARDS. *IEEE 802.11 Wireless Local Area Networks*. Disponível em: <http://www.ieee802.org/11/>. Acesso em: 08 dec. 2018.

67 ARDUINO ORGANIZATION. *Arduino*. Disponível em: <https://www.arduino.cc/>. Acesso em: 08 dec. 2018.

68 WIZNET AND MOUSER. *WIZnet Ethernet Shield W5100 Datasheet*. Disponível em: <https://www.mouser.com/catalog/specsheets/A000056_DATASHEET.pdf>. Acesso em: 08 dec. 2018.

69 ARDUINO ORGANIZATION. *Arduino IDE*. Disponível em: <https://www.arduino.cc/en/Main/Software>. Acesso em: 08 dec. 2018.

70 ARDUINO ORGANIZATION. *Placa Arduino MEGA*. Disponível em: <https://www.arduino.cc/en/Main/ArduinoBoardMega2560?setlang=en>. Acesso em: 08 dec. 2018.

71 ARDUINO ORGANIZATION. *Arduino UNO Rev3*. Disponível em: <https://store.arduino.cc/usa/arduino-uno-rev3>. Acesso em: 08 dec. 2018.

72 ARDUINO ORGANIZATION. *Arduino Shields*. Disponível em: <https://www.arduino.cc/en/Main/arduinoShields>. Acesso em: 08 dec. 2018.

73 OPEN ENERGY MONITOR. *Open Energy Monitor Project*. Disponível em: <https://learn.openenergymonitor.org/>. Acesso em: 08 dec. 2018.

74 OPEN ENERGY MONITOR AND GITHUB. *Biblioteca Emonlib*. Disponível em: <https://github.com/openenergymonitor/EmonLib>. Acesso em: 08 dec. 2018.

75 NETWORK WORKING GROUP. *Simple Network Management Protocol (SNMP) Applications*. Disponível em: <https://tools.ietf.org/html/rfc3413>. Acesso em: 08 dec. 2018.

76 AGENTUINO COMMUNITY. *Agentuino Project*. Disponível em: <https://code.google.com/archive/p/agentuino/>. Acesso em: 08 dec. 2018.

77 GITHUB AGENTUINO COMMUNITY. *Agentuino Library*. Disponível em: <https://github.com/1sw/Agentuino>. Acesso em: 08 dec. 2018.

78 IANA - INTERNET ASSIGNED NUMBERS AUTHORITY. *Structure of Management Information (SMI) Numbers (MIB Module Registrations)*. Disponível em: <https://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml>. Acesso em: 08 dec. 2018.

79 ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Introduction to ASN.1*. Disponível em: <https://www.itu.int/en/ITU-T/asn1/Pages/introduction.aspx>. Acesso em: 08 dec. 2018.

80 ARDUINO FOUNDATION. *Ethernet library*. Disponível em: <https://www.arduino.cc/en/Reference/Ethernet>. Acesso em: 27 jun. 2019.

81 IANA - INTERNET ASSIGNED NUMBERS AUTHORITY. *IANA Enterprise Numbers*. Disponível em: <https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>. Acesso em: 08 dec. 2018.

82 ZABBIX SIA. *Zabbix Documentation 4.0 - Proxy*. Disponível em: <https://www.zabbix.com/documentation/4.0/manual/concepts/proxy>. Acesso em: 27 jun. 2019.

83 AGêNCIA NACIONAL DE ENERGIA ELéTRICA - ANEEL. *ANEEL - Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional – PRODIST*. Disponível em: <http://www.aneel.gov.br/prodist>. Acesso em: 27 jun. 2019.

84 AGêNCIA NACIONAL DE ENERGIA ELéTRICA - ANEEL. *ANEEL - Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional – PRODIST, Módulo 5 – Sistemas de Medição*. Disponível em: <http://www.aneel.gov.br/modulo-5>. Acesso em: 27 jun. 2019.

85 NETWORK WORKING GROUP. *Network Time Protocol (NTP) - RFC 958*. Disponível em: <https://tools.ietf.org/html/rfc958>. Acesso em: 27 jun. 2019.

86 ZIGBEE ALLIANCE. *Zigbee Alliance*. Disponível em: <https://www.zigbee.org/>. Acesso em: 27 jun. 2019.