Desenvolvimento de um agente SNMP para monitoramento de ambientes empresariais

Gerson Dalcin

Universidade de Caxias do Sul
95700-000 – Bento Gonçalves – RS – Brasil

gdalcin2@ucs.br

Resumo. *Conforme tendência da indústria 4.0, o monitoramento e busca de dados sobre máquinas está cada vez mais insurgente. As tecnologias IoT buscam auxiliar nas soluções em coleta de dados e facilitar a comunicação entre dispositivos de rede. O protocolo SNMP se caracteriza por ser robusto e de simples manuseio para a coleta de dados e controle dos ativos. Este artigo apresenta a proposta de desenvolvimento de um agente SNMP modular para monitoramento a nível empresarial e/ou industrial.*

1. Introdução

A tecnologia sempre foi um dos pilares dos avanços na produtividade e competitividade no âmbito industrial. Com a mesma, foi possível alcançar os desenvolvimentos necessários para dar o início às revoluções industriais. Hoje, nos encontramos em meio à quarta revolução que se dá pelo avanço da Internet das Coisas (IoT – *Internet of Things*) em ambientes de fabricação. Sistemas de coletas, armazenagem e processamento de dados em máquinas são fundamentais para o desenvolvimento fabril, de modo a deixar as instalações ainda mais inteligentes e rentáveis [Schneider 2018].

Para obter uma rede IoT, é necessário possuir suporte para aplicações e serviços heterogêneos, isto envolve qualquer objeto que pode ser conectado tanto em redes locais, como globais. Nos dias atuais, há uma perspectiva de 50 bilhões de dispositivos conectados na internet e com um valor estimado de U$7,1 trilhões [Silva *et al.* 2018].

O protocolo *Simple Network Management Protocol* (SNMP) é um protocolo não orientado a conexão, o próprio, é um protocolo simples e robusto e ao mesmo tempo, poderoso o suficiente para resolver problemas em gerenciamento de redes [Silva 2018]. O protocolo SNMP foi utilizado basicamente para controlar a disponibilidade e desempenho de dispositivos como roteadores, switches, servidores e outras interfaces que disponibilizavam o agente SNMP [Poloni *et al.* 2017].

O objetivo de desenvolvimento deste artigo é proposto através da criação de um agente SNMP microcontrolado, o sistema será modular e de fácil implementação em conjunto com o monitoramento ativo existente. Ele será ajustado para os vários aspectos industriais e empresariais encontrados. A prova de conceito, se dará em uma aplicação de monitoramento de ambientes de centro de processamento de dados (Data Center).

Este artigo consiste em cinco seções, incluindo a introdução. Para a seção 2 é apresentado uma contextualização da indústria 4.0 na atualidade, enquanto na seção 3, possui uma base teórica sobre o protocolo SNMP e suas principais operações. Na seção 4 é apresentado a proposta e metodologia a ser aplicada e por fim, é demonstrado os resultados esperados após a finalização da prática na seção 5.

2. Indústria 4.0 e Internet das Coisas (IoT)

O termo Indústria 4.0 ficou conhecido em 2011, quando uma junção público/privada alemã promoveu uma abordagem a fim de aprimorar a competitividade industrial nacional. Este movimento criou o que chamamos de fábricas inteligentes, onde possuem estruturas modulares em que sistemas ciber físicos monitoram processos e tomam decisões descentralizadas. Essa transformação se dá pela interconexão de sensores, máquinas, peças e sistemas de informação em uma cadeia de valores multi empresas. Esses sistemas denominados ciber físicos, podem interagir uns com os outros usando protocolos padrões e análise de dados para prever falhas e prover monitoramento nos ativos. Através desta análise, é possível organizar processos com mais rapidez, flexibilidade e eficiência, mantendo sempre a alta qualidade e diminuindo custos operacionais com o aumento da produtividade de manufatura [Schneider 2018]. A Figura 1, demonstra as etapas de cada evolução industrial até os dias atuais [Kagermann *et al.* 2013].

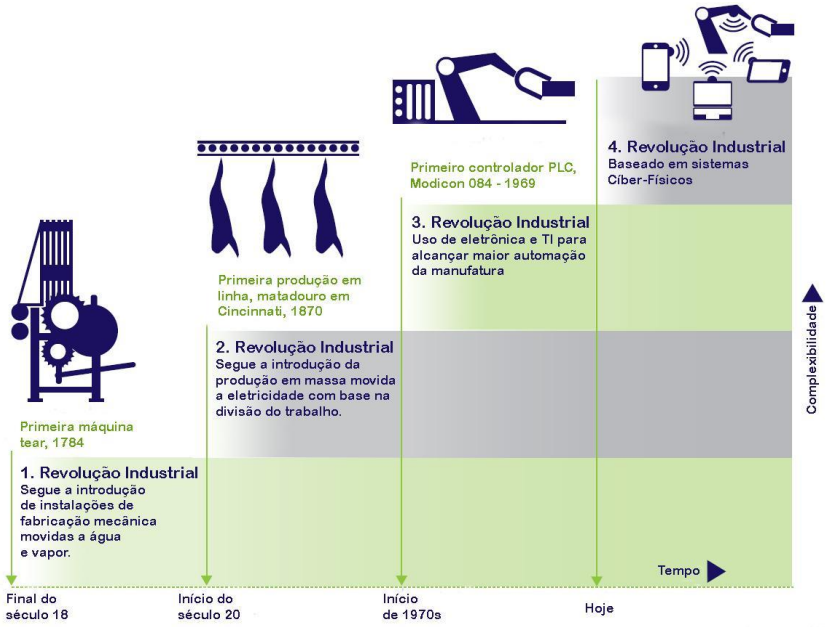

Figura 1. Revoluções Industriais [Kagermann et al. 2013] (Adaptado pelo Autor).

Um dos pilares da Indústria 4.0 é a Internet das Coisas. O conceito foi introduzido primeiramente em 1999, onde foi utilizado para nomear um sistema de comunicação entre sensores e computadores. Este conceito envolve a combinação de dispositivos identificáveis através de uma rede, esses objetos possuem a possibilidade de coleta, processamento ou troca de dados de forma direta ou indireta. A capacidade da IoT de integrar com as redes clássicas e objetos de rede, vem ao encontro com a construção de um ambiente inteligente que nos circula nos dias atuais [Schneider 2018].

Esses dispositivos são apresentados de forma direta e/ou indireta para a população, através de telefones, *tags* RFID (*Radio Frequency Identification*), entre outros. Para o objeto ser reconhecido como um dispositivo de IoT, o mesmo deve possuir um baixo consumo e poder computacional. Em estudos direcionados a saúde, é buscado a possibilidade de as pessoas possuírem um chip que efetue o monitoramento da saúde

através de sensores na residência, e ser possível acionar uma ajuda médica caso necessário de forma autônoma [Poloni *et al.* 2017].

Desta forma, um dos desafios mais críticos para o gerenciamento IoT, é a interoperabilidade e heterogeneidade de comunicação dos protocolos com os dispositivos, onde se faz necessária uma rede de dispositivos que é capaz de extrair dados individualmente de cada objeto e intercomunicando-se entre si [Silva *et al.* 2018].

3. Protocolo SNMP

O SNMP apresenta-se como um protocolo da camada de aplicação que compõe a pilha do TCP/IP (*Transmission Control Protocol / Internet Protocol*), o mesmo é amplamente utilizado na gerência de redes e ativos. O SNMP foi aprovado pela *Internet Architecture Board* (IAB) em 1988, como o protocolo padrão para gerenciamento de redes IP, hoje o protocolo é o mais utilizado em gerenciamento de redes. O SNMP utiliza um protocolo de simples solicitação/resposta, que executa sobre o *User Datagram Protocol* (UDP), que está na camada de transporte da pilha TCP/IP. Com isso, minimizando a complexidade dos procedimentos de comunicação e implementação [Machado 2015][Sinche *et al.* 2020]. O SNMP baseia-se em arquitetura cliente/servidor e consiste nos seguintes componentes (Figura 2) [Sinche *et al.* 2020]:

a. Dispositivo gerenciado: um nó de rede onde um agente está localizado.

b. Agente: Software de gerenciamento de rede modular, responsável pela manutenção das informações dos dispositivos. O mesmo, recebe requisições provenientes do gerente e envia as informações relativas a requisição. Também é responsável por enviar alterações sobre condições anormais previamente cadastradas.

c. Gerente: Software de gerenciamento SNMP, normalmente instalado em servidores. O mesmo envia solicitações e recebe respostas / notificações dos agentes, sobre informações de dispositivos gerenciados, a fim de realizar tarefas. Possui comunicação com todos os agentes disponíveis na rede. É responsável pelo monitoramento, geração de relatórios e controles de falhas.

d. Sistema de gerenciamento de rede (NMS): monitora e controla dispositivos gerenciados usando aplicativos de gerenciamento.

e. *Management Information Base* (MIB): Os objetos MIB são representados com uma linguagem de dados chamada Estrutura de Gestão Informações (SMI). A estruturação é em formato de árvore que contém os objetos gerenciados, cada objeto possui uma identificação única denominada *Object Identification* (OID), composta por uma sequência de números que identifica a posição do objeto na árvore do MIB.

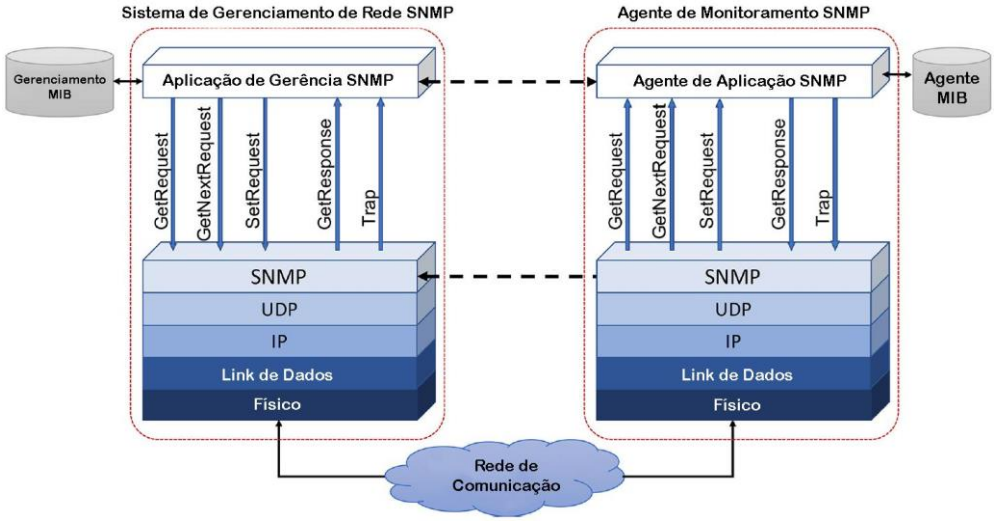

Figura 2. Arquitetura de gerenciamento de redes SNMP [Sinche *et al.* 2020] (Adaptado pelo Autor).

O protocolo SNMP possui quatro operações comuns entre todas as versões, são elas [Boyko *et al.* 2019]:

a. *Get*: Usado pelo gerente para buscar o valor de um objeto em um agente.

b. *GetNext*: Busca o próximo objeto instanciado pelo Get.

c. *Set*: Inicia ou reinicia os valores dos objetos instanciados no agente.

d. *Trap*: É uma mensagem não solicitada pelo gerente, normalmente sobre um evento significante ou falha no sistema monitorado.

4. Proposta de Desenvolvimento

Conforme abordado anteriormente, o objetivo deste trabalho é o desenvolvimento de um agente SNMP para ambientes industriais e com o primeiro desenvolvimento voltado a monitoramento de data center. Os data centers são peças chaves no desempenho de uma empresa, idealmente os ativos são mantidos com uma alimentação de energia e resfriamento estável. Como os equipamentos que fazem parte da infraestrutura central da rede são sensíveis, é necessária uma infraestrutura dedicada ao monitoramento de energia, temperatura, umidade e entre outros pontos críticos ao ambiente e sua ininterrupção.

Em empresas que trabalham em 24/7 e não possuem gerência de infraestrutura disponível em todos os horários, a necessidade de monitoramento constante é um fator crucial para o desempenho adequado do data center. Pois em casos de alterações bruscas, como por exemplo, na temperatura do ambiente, pode levar a uma reação em cadeia de danos em equipamentos e paralisação parcial ou total dos serviços e servidores. Estas paralisações podem acarretar em prejuízos enormes e/ou irreversíveis para a empresa, dependendo da magnitude do sinistro ocorrido. Desta forma, proporcionando um sistema de monitoramento adequado, é possível prevenir paradas e mitigar os riscos de perdas mais agressivas.

O experimento será efetuado em um ambiente de data center corporativo, na Figura 3 é demonstrado o layout da disposição dos componentes presentes. Nestes ambientes, é desejável que se mantenha o monitoramento das variáveis de temperatura,

umidade e de gás/incêndio. Para o desenvolvimento, será instalado o sensoriamento no corredor frio em frente ao rack de servidores, pois os mesmos são equipamentos mais sensíveis em comparação com equipamentos de telecomunicações e rede.

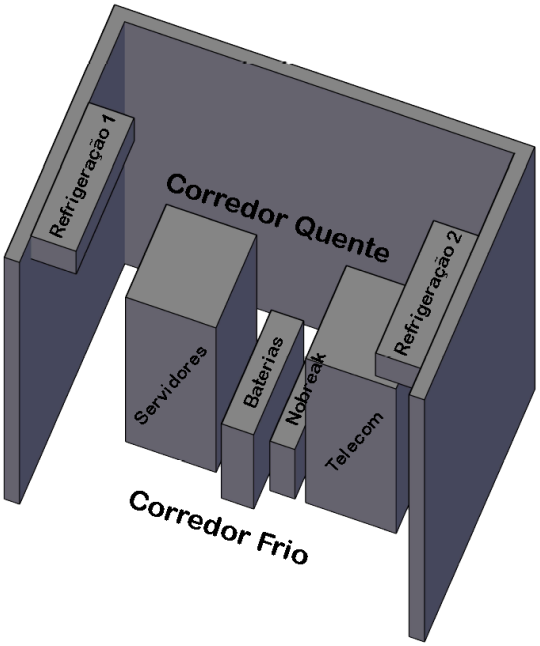

Figura 3. Layout do Data Center (Desenvolvido pelo Autor).

5. Metodologia

Para o desenvolvimento do trabalho, será aplicada uma metodologia com cinco etapas do processo, conforme abaixo:

Figura 4. Etapas de desenvolvimento da plataforma (Desenvolvido pelo Autor).

5.1. Microcontrolador e Sensores

Para a escolha do microcontrolador, foi analisado se o mesmo possui suporte às linguagens C/ C++ que é comumente utilizado na criação de firmwares e bibliotecas para microcontroladores. A possibilidade de uso por comunicação wireless, que em muitos casos favorece e elimina custos para a aplicação, a abrangência de bibliotecas de fabricantes e específicas para o desenvolvimento, o nível de processamento que comporta, como o protocolo em si pode ser expressivo para o microcontrolador processar, desta forma é necessário um microcontrolador que possua desempenho superior e pôr fim a quantidade de portas disponíveis para a integração com sensoriamento. Todas essas análises não estão focadas somente no desenvolvimento deste primeiro projeto, mas também na continuidade do agente com abrangência para toda a empresa, de forma satisfatória e com a maior extensão possível. Sendo assim, foi escolhido o microcontrolador ESP32, que atende as especificações acima.

Para a escolha dos sensores, é necessário levar em consideração os principais parâmetros que são monitorados dentro de um data center e formas de aquisição dos

mesmos. Tendo em vista disto, os parâmetros críticos são o fornecimento de energia, tanto da concessionária, quanto dos nobreaks, detecção de alagamento, temperatura, umidade, fumaça e invasão.

Tendo em vista os parâmetros destacados, comumente os sistemas nobreaks já apresentam placas embutidas com protocolo SNMP, que possuem o monitoramento ativo a partir das mesmas, sendo assim, é possível monitorar a tensão e corrente da rede e também a saída do mesmo. Em muitos casos, também é necessário a instalação de sensoriamento nos grupos geradores para o monitoramento em caso de ativação e avisos em caso de falha. Para a detecção de alagamentos são utilizados sistemas com malhas, que efetuam análises constantes sobre a diferença de potencial entre elas e em caso de possuir uma película de água, a diferença de potencial diminui drasticamente e efetua o acionamento dos alarmes. Enquanto a identificação de invasão fica em conjunto com o sistema de abertura da porta, onde pode ser acoplado um sensor de proximidade, sendo que ao passar um determinado tempo com a porta aberta ou abertura não liberada o mesmo também dispara os alertas. A detecção de fumaça geralmente é instalada em conjunto com os sistemas de combate a incêndio FM200.

A partir das análises comentadas acima, será desejável o monitoramento da temperatura, umidade, chama, gás inflamável e qualidade do ar. Estes são pontos que podem ser analisados dentro de um DTC com parâmetros pré-definidos conforme as condições de trabalhos impostas. Dentro deles, é válido salientar a importância do controle de temperatura (falhas do sistema de refrigeração) e qualidade do ar, os mesmos são fundamentais para o desempenho do DTC, sendo que em casos de aumento brusco de temperatura, os discos presentes nos servidores se deterioram mais rapidamente, podendo ocorrer falhas ou danificá-los de forma irreversível o mesmo ocorre quando há aquecimento nos servidores, podendo acarretar no desligamento dos mesmos. Enquanto o sensor de qualidade do ar, auxilia no controle da sala e em suas impurezas, determinando a quantidade de partículas de poeira dentro do ambiente e também ajustando cronogramas de limpeza da sala e dos servidores pelos índices. Em salas estanques, este sistema é vital para determinar se está bem selada e sem vazamentos que podem acarretar em um consumo maior do gás ou a não funcionalidade do mesmo, em conjunto com esta análise, o sensor também detecta fumaça no ambiente, sendo assim, é possível utilizá-lo como detector de incêndio em conjunto com os sensores de fumaça endereçável.

Para o projeto, foi escolhido o sensor de gás inflamável MQ-2, onde este servirá a função de detectar qualquer gás que tenha teor inflamável dentro da infraestrutura. Para fogo, foi utilizado o sensor de chama, o mesmo efetua uma leitura de fontes de calor com um comprimento de onda entre 760 a 1100nm. Estes dois sensores serão trabalhados com suas saídas digitas, sendo ajustados por seus potenciômetros para serem acionados conforme uma quantidade definida de intensidade. O sensor de poeira e fumaça mede o nível de partículas no ar através do uso de luz infravermelha, fornecendo dados com uma sensibilidade de partículas de até 1µm. O sensor usa o método de contagem para testar a concentração de poeira e fumaça densa no ambiente, para o projeto foi utilizado o *Grove - Dust Sensor*. Por fim, o sensor para a medição da temperatura, umidade e pressão, foi escolhido o módulo que contém o chip BME280 fabricado pela Bosch, pois o mesmo possui precisão nas medições de temperatura, apresentando uma variação máxima 1ºC e 3% de umidade. O módulo possui um regulador 3.3V LM6206 e um tradutor de tensão para o I2C, o consumo do módulo é menor que 1mA e em modo ocioso chega a 5µA.

5.2. Desenvolvimento do Firmware

Com a definição do microcontrolador e do sensoriamento a ser instalado, foi possível executar o desenvolvimento do firmware, necessário para executar o projeto. A primeira etapa foi o teste dos sensores e o entendimento da funcionalidade dos mesmos com a parametrização correta ao ambiente que os mesmos estarão sendo alocados. Neste ponto, é crucial a utilização, se necessário, de bibliotecas das fabricantes dos mesmos, evitando possíveis complicações futuras no andamento do projeto. Com os testes validados, foi implementada a biblioteca do SNMP e suas validações com o uso de um OID genérico, sempre mantendo dentro de uma rede privada para não gerar conflitos externos.

Com todas as bibliotecas e principais funções validadas, foi criada a estrutura do código, sendo que cada sensor foi desenvolvido dentro de uma função. O *loop* somente chamará as funções dentro de um intervalo de 100ms, sendo que as variáveis com dados para a utilização dentro do protocolo foram criadas de forma global. Desta forma, a cada interação do gerente, o mesmo irá buscar as últimas informações coletadas sem atrapalhar o restante do código, sem ser de forma concorrente ou com *delay* no envio, que pode ocasionar perdas na comunicação ou falsos positivos no sistema em geral.

Com o firmware desenvolvido e com as primeiras validações dos sensores e envio pelo SNMP, foi solicitado em conjunto com a IANA um código OID para a execução do projeto e desenvolvimentos futuros. O código endereçado a solicitação é o 56575, onde fará parte da árvore MIB e poderá ser utilizado de forma comercial. A figura a seguir demonstra o fluxograma do firmware.

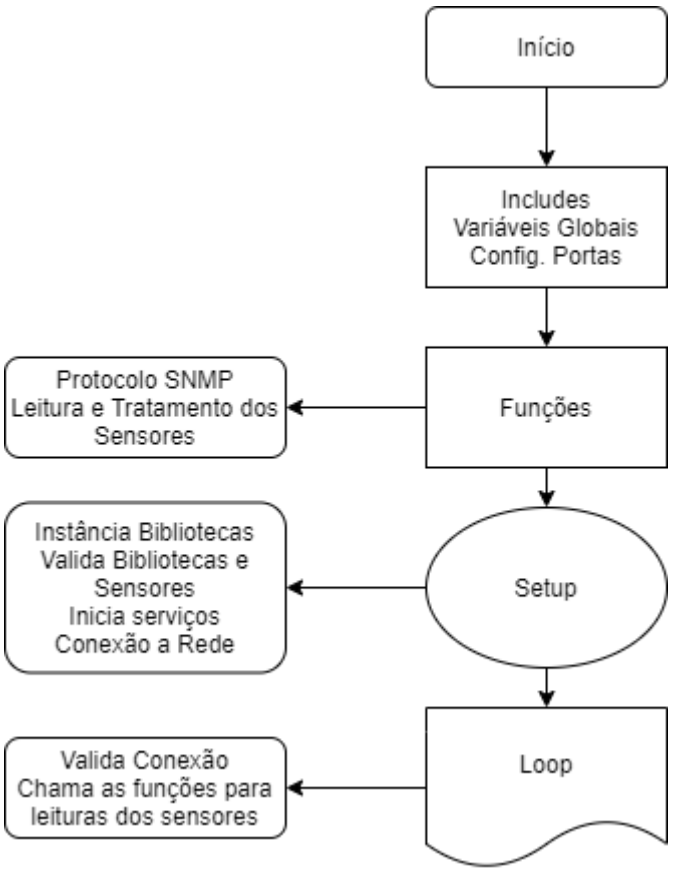

Figura 5. Fluxo do Firmware (Desenvolvido pelo Autor).

5.3. Testes e Validações

Para os testes iniciais, foram analisados a estabilidade da conexão e os valores enviados pelo SNMP, para isso, foi utilizado o software *PowerSNMP Free Manager*, no mesmo, é possível adicionar as OIDs utilizadas e analisar as coletas dos dados em tempo real. O sistema também possui logs que são dedicados as falhas na consulta entre o gerente e o agente, desta forma, foi possível validar a geração e transmissão dos dados e também as análises de erros da mesma.

Para testarmos a confiabilidade do sistema, foi aplicado no mesmo variações induzidas nos sensores, de forma a analisar se o mesmo se tornam constantes dentro de um período grande de análise, desta forma, foram inseridas variações induzidas na temperatura e umidade dentro de um período de 96 horas com alterações intercaladas dentro de 12 horas. Como o sistema utilizado para análise não possui gravação dos dados coletados, foram aferidos os dados dentro dos intervalos de alteração e comparados com um termômetro infravermelho. A cada aferida, também era induzida variação nos demais sensores, com queima de papel ou plástico, para identificar as variações das leituras nos demais sensores e efetuar as calibrações necessárias dos mesmos.

De modo geral, as aferições se demonstraram satisfatórias e também foi possível concluir que mesmo com variações expressivas nas temperaturas de trabalho, o sistema se manteve estável com poucas perdas na comunicação, se tornando apto para o prosseguimento do trabalho.

5.4. Integração

Com a validação do firmware e hardware finalizado, foi possível analisar formas de integração do agente com sistemas gerentes, onde é possível efetuar as etapas finais de validações com histórico de dados, sendo de forma mais assertiva a validação do sistema.

Um dos softwares livres mais utilizados para gerência do protocolo SNMP é o Zabbix, o mesmo é distribuído sobre a versão 2 da *GNU General Public License (GPL)*, possibilitando assim, utilizar de forma comercial e adaptar o mesmo para as necessidades da empresa. Um ponto importante também é a possibilidade de integrações com plataformas de mensageria e visualização de dados de forma gráfica, também é válido ressaltar que é possível efetuar a instalação do mesmo sobre a plataforma Raspberry, tornando assim o candidato ideal para o projeto de validação e de sensoriamento a baixo custo.

Para a visualização dos dados, tanto em modo de *dashboards*, quanto a uma análise temporal mais amigável, foi integrado ao sistema Zabbix o software Grafana, o mesmo também é de software livre. A função dele é coletar por meio de uma API as informações que o Zabbix disponibiliza, e através destes dados gerar gráficos para a criação de *dashboards* mais simplificados.

Um dos pontos principais de um monitoramento são os sistemas de mensageria, sendo assim, foi escolhido o software Telegram, onde é possível a criação de robôs para o envio de mensagem, desta forma, foi integrada ao sistema de mensageria que irá executar o envio de mensagens de alerta por *triggers* cadastradas no sistema, assim, o monitoramento se torna efetivo e com qualquer variação lida pelos sensores, é possível agir de forma mais ágil para a solução dos problemas.

6. Resultados Experimentais

Após a finalização das validações em laboratório, será implementado o agente no ambiente definido. Para a melhor acomodação do sensoriamento e do microcontrolador, foi desenvolvido uma placa de circuito impresso (PCB) e também um suporte para a instalação. Abaixo seguem as figuras do circuito do projeto e da PCB.

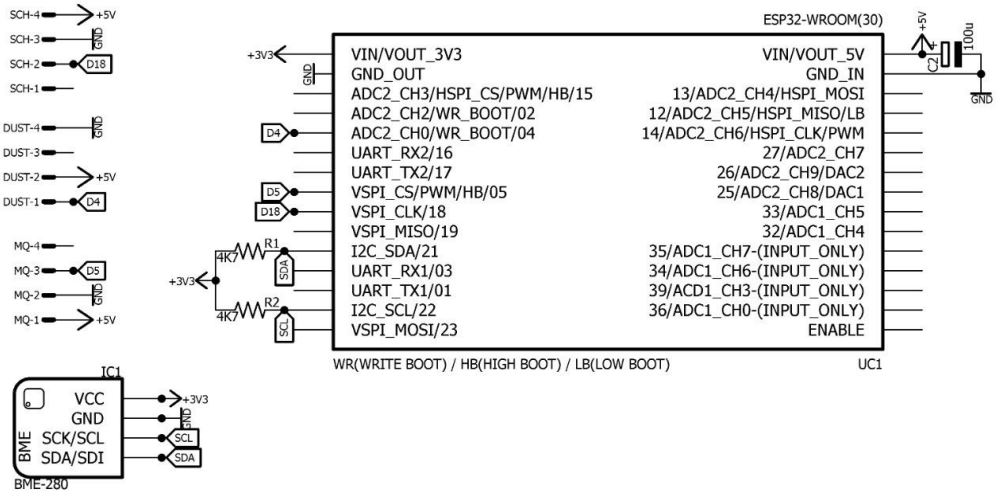

Figura 6. Circuito do Projeto (Desenvolvido pelo Autor).

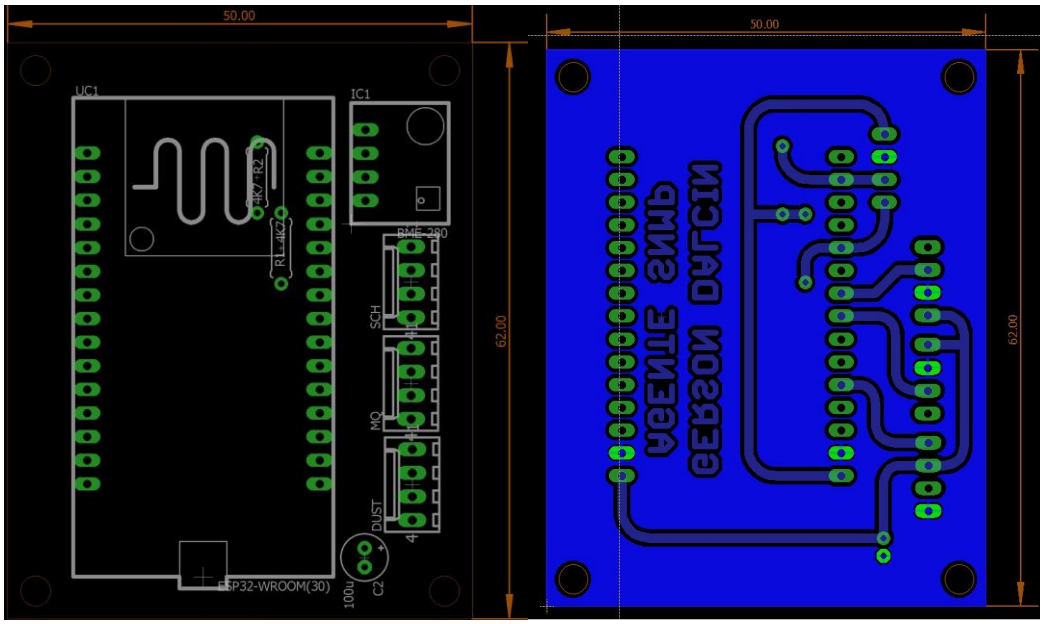

Figura 7. PCB do Projeto (Desenvolvido pelo Autor).

Com o desenvolvimento e confecção da PCB, foi desenhado um suporte para a acomodação de todos os sensores e da PCB, para isso, foi utilizado uma chapa de aço 1010 e efetuado dobras na mesma. O formato final ficou semelhante a um “U”, sendo que os sensores de gás e incêndio estarão na parte superior direcionados para a parte inferior, a fim de obter a maior coleta possível dos mesmos. O sensor de qualidade do ar, foi instalado na parte externa do suporte, de forma que não obstrua a entrada do ar e por fim, o sensor BME280 foi instalado diretamente na PCB.

A alimentação do protótipo se dá pela própria entrada USB do módulo ESP32, sendo este com 5V e possuindo um regulador interno para 3.3V de distribuição para a alimentação do sensoriamento. O protótipo finalizado está demonstrado nas figuras abaixo.

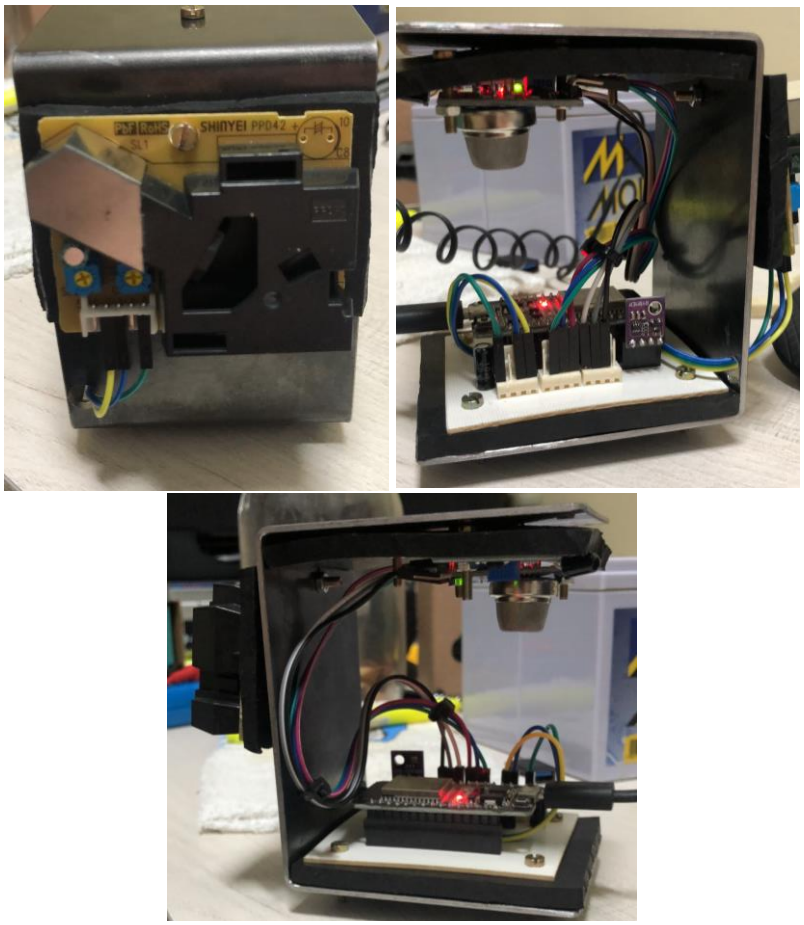

Figura 8. Montagem do Protótipo (Desenvolvido pelo Autor).

Com a parte física pronta para implantação, foi efetuada a instalação e configuração do gerente SNMP selecionado para o projeto. Para o mesmo, foi preparado a Raspberry Pi 3 com o sistema operacional Raspbian Lite, onde o mesmo é baseado em Linux e também é livre para uso comercial. Para o armazenamento e funcionamento do Zabbix, o mesmo necessita de um banco de dados MySQL que também foi embarcado na Raspberry. Para visualização, foi adicionado o sistema Grafana e conectado por meio de API com o banco de dados do Zabbix.

O Zabbix possui formas de tratamentos das variáveis que são fornecidas pelo SNMP, desta forma, todos os componentes OIDs foram inseridos nas coletas e também tratados de forma que os dados analisados se detenham da melhor forma possível, sendo que as análises *On/OFF* que se dão nos pontos de chama e gás, foram convertidas para OK e Perigo, de acordo com o resultado enviado pelo agente. Também foram tratadas as variáveis de temperatura, umidade e pressão para ser possível a aquisição com todas as casas decimais disponíveis pelo sensor. Outro ponto configurado no sistema, foram os dados providos por *ping*, desta forma, o sistema fica em constante monitoramento de falha de comunicação com o agente. Na figura abaixo, é demonstrado os campos cadastrados para coleta no software.

Name ▲	Triggers	Key	Interval	History	Trends	Type
Chama		Chama	10s	90d	365d	SNMP agent
Gas		Gas	10s	90d	365d	SNMP agent
Template Module ICMP Ping: ICMP loss	Triggers 1	icmppingloss	1m	1w	365d	Simple check
Template Module ICMP Ping: ICMP ping	Triggers 1	icmpping	1m	1w	365d	Simple check
Template Module ICMP Ping: ICMP response time	Triggers 1	icmppingsec	1m	1w	365d	Simple check
Pressão		Pressao	10s	90d	365d	SNMP agent
Qualidade do Ar	Triggers 1	QUA_AR	10s	90d	365d	SNMP agent
Temperatura	Triggers 1	Temperatura	10s	90d	365d	SNMP agent
Umidade		Umidade	10s	90d	365d	SNMP agent

Figura 9. Pontos de Coletas Cadastrados (Desenvolvido pelo Autor).

O software Grafana foi configurado à API para efetuar as coletas das informações de forma a simplificar a integração entre os sistemas. Os dados novamente foram validados com a consulta da API e posterior a conferência foi desenvolvido a *dashboard* de monitoramento, onde a mesma estará disponível para a consulta da equipe de suporte responsável na empresa. A tela desenvolvida para monitoramento está apresentada abaixo.

Figura 10. Tela de Monitoramento (Desenvolvido pelo Autor).

Na mesma, é possível efetuar delimitações para que a visualização demonstre caso um dos dados analisados esteja fora dos padrões parametrizados, para assim, visualizar o melhor funcionamento do sistema. A mesma também possui a funcionalidade de alterar o tempo em que o gráfico se atualiza automaticamente e a faixa de datas que são demonstradas nos gráficos temporais. Abaixo segue uma demonstração de variação nos dados adquiridos no ambiente.

Figura 11. Demonstração de variações induzidas (Desenvolvido pelo Autor).

Na análise acima, foi induzido o sistema a uma temperatura acima dos parâmetros cadastrados e também efetuado a poluição do ambiente com fumaça para a detecção. Desta forma, é possível analisar que os gráficos temporais possuem uma tarja vermelha delimitando o nível máximo que deveria ser alcançado e também no mostrador *Gauge* da temperatura, é possível verificar que o número e as barras atingiram os valores limites e alteraram de cor. Neste exemplo, o gás e a chama não foram induzidos para alteração, no entanto, o resultado se assemelha ao mostrador *Gauge*, onde em caso de detecção, o mesmo trocará para a cor vermelha e altera a escrita para Perigo.

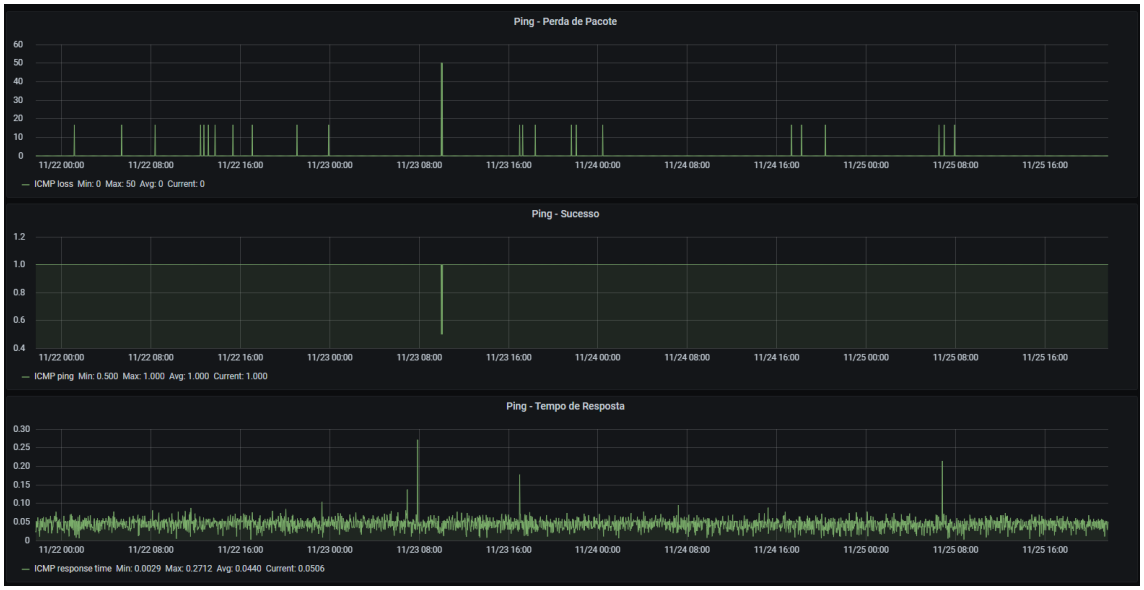

Figura 12. Avaliação de Estabilidade do Sistema (Desenvolvido pelo Autor).

Para a análise de instabilidade do sistema de comunicação, foi também criado uma *dashboard* que monitora as perdas de pacote e falhas na comunicação com o agente. A figura acima demonstra as coletas efetuadas durante 4 dias, onde é possível analisar que mesmo ocorrendo, são poucos casos, o que não torna o sistema instável ou perigoso para instalação em ambientes críticos.

Como uma forma de efetuar o monitoramento por completo, foi integrado o Zabbix com um sistema de mensageria, desta forma, conforme configurado os valores máximos das leituras, o mesmo irá executar um *trigger* que irá encaminhar uma mensagem para o aplicativo Telegram, deixando assim o monitoramento por completo, desde a geração dos dados, demonstração em dashboards e alertas de irregularidades. Para executar a integração com o aplicativo, foi necessário a criação de um robô que possui o *token* de identificação único. Para aumentar a segurança, foi também criado um grupo de mensagens que ambos estão configurados com seus respectivos ID's para alertas de possíveis problemas. As mensagens informam qual sensor indicou a variação e também qual o valor da mesma, ao normalizar o serviço, o mesmo envia uma mensagem de solução para acompanhamento. Na figura abaixo, é possível verificar uma mensagem de exemplo da integração.

Figura 13. Mensagens enviadas para o Telegram (Desenvolvido pelo Autor).

7. Conclusão

Este trabalho conseguiu uma grande abrangência em diversos pontos, desde instrumentação até sistemas operacionais, desta forma, a idealização e execução do mesmo, se torna de grande valia para o entendimento de todo um sistema de monitoramento baseado em SNMP. Neste projeto, é possível analisar diversos pontos que podem ser relevantes para resoluções de problemas nas infraestruturas de DTC e também na continuidade dos mesmos, o sistema de mensageria é de suma importância para a gerência do DTC, onde com os alertas é possível tomar decisões com mais agilidade, sem a presença deste sistema, o tempo de resposta pode ser maior e gerar problemas no desempenho dos servidores.

O trabalho abre um leque de oportunidades para o sensoriamento de diversos pontos dentro de uma empresa, com o atendimento da proposta de ser um dispositivo modular, é de fácil implementação novos sensores para que atenda outros pontos de coletas, sendo assim, uma solução viável e de baixo custo para o desenvolvimento da empresa. Ainda existem pontos que podem ser melhorados tanto no código, quanto na apresentação das informações, mas o estudo até o momento se tornou satisfatório e com uma aplicabilidade alta. Com a finalização do protótipo, todos os objetivos elencados no início do trabalho foram possíveis de serem abordados.

8. Referências

A. Boyko, V. Varkentin and T. Polyakova, "Advantages and Disadvantages of the Data Collection's Method Using SNMP," 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2019, pp. 1-5, doi: 10.1109/FarEastCon.2019.8934069.

J. de C. Silva, P. H. M. Pereira, L. L. de Souza, C. N. M. Marins, G. A. B. Marcondes and J. J. P. C. Rodrigues, "Performance Evaluation of IoT Network Management Platforms," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 259-265, doi: 10.1109/ICACCI.2018.8554364.

Kagermann, H.; Wahlster, W.; Helbig, J. (2013). "Recommendations for implementing the strategic initiative INDUSTRIE 4.0". ACATECH.

S. Sinche et al., "A Survey of IoT Management Protocols and Frameworks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1168-1190, Secondquarter 2020, doi: 10.1109/COMST.2019.2943087.

Santos, F. Sérgio dos (2017). "Aplicação do protocolo SNMP para o monitoramento on line de uma microgeração fotovoltaica", https://repositorio.unesp.br/ handle/11449/150972, Dezembro.

Schneider, J. (2018). "Medição do nível de maturidade do uso de tecnologia em um ambiente da indústria 4.0", https://repositorio.ucs.br/11338/4877, Dezembro.

Silva, J. d. C. (2018). "Performance assessment of management protocols and platforms for internet of things", http://tede.inatel.br:8080/jspui/handle/tede/182, Dezembro.

Machado, L. F. (2015). "Proxy IP de baixo custo e múltiplos sensores para cidades inteligentes", http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui//handle/ tede/560, Dezembro.

W. T. Poloni, R. Becker and R. Balbinot, "Remote control of low cost devices using SNMP agents," 2017 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, 2017, pp. 1-6, doi: 10.1109/PACRIM.2017.8121927.

DataSheet Sensor de Poeira e Fumaça <https://img.filipeflop.com/files/ download/Sensor_de_poeira_fumaca.pdf>. Acessado em 25/11/2020.

DataSheet Sensor de Gás MQ-2 <https://img.filipeflop.com/files/ download/Datasheet_Sensor_Gas_MQ2.pdf>. Acessado em 25/11/2020.

DataSheet Sensor BME280 <https://www.bosch-sensortec.com/media/boschsensortec/ downloads/datasheets/bst-bme280-ds002.pdf>. Acessado em 25/11/2020.

Biblioteca SNMP <https://github.com/0neblock/Arduino_SNMP>. Acessado em 25/11/2020.

IANA Private Numbers < https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>. Acessado em 25/11/2020.

Wide range of Hygrometers <https://www.kandrsmith.org/ RJS/Misc/Hygrometers/ calib_many.html>. Acessado em 25/11/2020.