Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Engenharia Elétrica

Trabalho de Conclusão de Curso

Monitoramento de ativos na etapa da aciaria em um processo siderúrgico utilizando o *software Zabbix*

Carine Ariane Ferreira

João Monlevade, MG
2024

Carine Ariane Ferreira

Monitoramento de ativos na etapa da aciaria em um processo siderúrgico utilizando o *software Zabbix*

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Ouro Preto como parte dos requisitos para obtenção do Título de Bacharel em Engenharia Elétrica pelo Instituto de Ciências Exatas e Aplicadas da Universidade Federal de Ouro Preto.
Orientador: Wendy Yadira Eras Herrera

Universidade Federal de Ouro Preto
João Monlevade
2024

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

F383m Ferreira, Carine Ariane.
Monitoramento de ativos na etapa da aciaria em um processo siderúrgico utilizando o software Zabbix. [manuscrito] / Carine Ariane Ferreira. - 2024.
54 f.: il.: color., tab..

Orientadora: Profa. Dra. Wendy Yadira Eras Herrera.
Monografia (Bacharelado). Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Aplicadas. Graduação em Engenharia Elétrica .

1. Controle de processo. 2. Siderurgia. 3. Sistemas de controle digital. 4. Usinas siderúrgicas. 5. Zabbix (Software). I. Herrera, Wendy Yadira Eras. II. Universidade Federal de Ouro Preto. III. Título.

CDU 681.5

Bibliotecário(a) Responsável: Flavia Reis - CRB6-2431

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E APLICADAS
DEPARTAMENTO DE ENGENHARIA ELETRICA

FOLHA DE APROVAÇÃO

Carine Ariane Ferreira

Monitoramento de ativos na etapa da aciaria em um processo siderúrgico utilizando o *software Zabbix*

Monografia apresentada ao Curso de Engenharia Elétrica da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de bacharel em Engenharia Elétrica

Aprovada em 21 de fevereiro de 2024

Membros da banca

Dra. Wendy Yadira Eras Herrera - Orientadora - Universidade Federal de Ouro Preto
Dr. Márcio Feliciano Braga - Universidade Federal de Ouro Preto
Dr. Marcelo Moreira Tiago - Universidade Federal de Ouro Preto

Wendy Yadira Eras Herrera, orientadora do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 28/02/2024

Documento assinado eletronicamente por **Wendy Yadira Eras Herrera**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 28/02/2024, às 17:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0675452** e o código CRC **5518A37F**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3808-0818 - www.ufop.br

Dedico este trabalho à minha família, pelo amor incondicional, apoio e incentivo constantes ao longo desta jornada acadêmica. Em especial ao meu pai, Múcio, que infelizmente não está mais entre nós, mas que sempre será minha motivação para seguir em frente. Sem vocês, nada disso seria possível!

Agradecimentos

Agradeço primeiramente a Deus por nunca me desamparar nesta jornada e por colocar pessoas especiais em meu caminho, cujas contribuições foram fundamentais para a realização deste sonho.

Aos meus queridos pais, Flávia e Múcio, dedico uma gratidão especial por acreditarem em mim e por serem os verdadeiros pilares da minha jornada. O apoio incondicional e amor sincero foram essenciais para enfrentar os desafios que surgiram ao longo da vida acadêmica.

Não poderia deixar de agradecer também às minhas irmãs, Camila e Cristiane, e a toda a minha família, cujo carinho e encorajamento me fortaleceram em todos os momentos.

À equipe de manutenção da aciaria, expresso minha gratidão por compartilharem generosamente seus conhecimentos e experiências. Aprendi muito ao lado de vocês e agradeço por tornarem meu ambiente profissional tão enriquecedor e inspirador.

À minha orientadora, Wendy, sua dedicação, paciência e críticas foram cruciais para o desenvolvimento deste projeto. Sou verdadeiramente grata pela oportunidade de aprender com alguém tão experiente e por todo o apoio que me proporcionou.

Não posso deixar de expressar minha gratidão aos colegas da turma, compartilhamos momentos marcantes, enfrentamos desafios acadêmicos juntos e, acima de tudo, formamos laços de amizade que levarei para toda a vida.

Por fim, agradeço a todas as pessoas que, de alguma forma, contribuíram para a concretização deste trabalho e em minha jornada acadêmica. A todos vocês, meu mais sincero obrigada!

"Não podemos resolver nossos problemas com o mesmo pensamento que tínhamos quando os criamos."

Albert Einstein

Resumo

Este trabalho apresenta a incorporação de uma ferramenta de monitoramento de desempenho, o *Zabbix*, a fim de realizar o gerenciamento reativo e proativo das falhas dos dispositivos das redes de controle e supervisão da etapa da aciaria de um processo siderúrgico. Essa necessidade se reforça ao analisar os resultados das paradas de processo da planta de estudo, que revelam que aproximadamente 15% das interrupções operacionais estão diretamente associadas a deficiências na infraestrutura de rede e falhas dos ativos dos níveis de controle e supervisão. Assim, a aplicação dessa ferramenta visa proporcionar maior confiabilidade ao processo da aciaria, mitigando potenciais riscos à rede de automação e assegurando uma operação mais segura e confiável. Para alcançar os objetivos propostos, foi realizada uma análise detalhada dos requisitos de monitoramento de desempenho da aciaria, identificando os dispositivos de rede críticos e os principais indicadores de desempenho a serem monitorados. Em seguida, foi realizada a instalação e configuração do *Zabbix*, incluindo a definição de alertas e a criação de painéis de monitoramento. O monitoramento vem sendo realizado continuamente, permitindo a identificação de falhas e a avaliação da eficácia da ferramenta. Como resultado da implementação do *Zabbix*, houve uma redução na detecção e correção de falhas de rede, contribuindo para uma operação mais eficiente e segura. Além disso, a capacidade de prever problemas antes que eles causem interrupções no processo levou a uma redução de 15% para 6,5% no tempo de inatividade não planejado. Esses resultados demonstram o impacto positivo da utilização do *Zabbix* na gestão de desempenho da aciaria do processo siderúrgico.

Palavras-chave: *Zabbix*, gerenciamento de falhas, processo siderúrgico, aciaria.

Abstract

This work presents the incorporation of a performance monitoring tool, Zabbix, aimed at carrying out reactive and proactive management of failures in the control and supervision networks of the steelmaking stage of a steelmaking process. This need is reinforced by analyzing the results of process shutdowns in the study plant, which reveal that approximately 15% of operational interruptions are directly associated with deficiencies in the network infrastructure and failures of control and supervision level assets. Thus, the application of this tool aims to provide greater reliability to the steelmaking process, mitigating potential risks to the automation network and ensuring a safer and more reliable operation. To achieve the proposed objectives, a detailed analysis of the steelmaking performance monitoring requirements was carried out, identifying critical network devices and key performance indicators to be monitored. Then, the installation and configuration of Zabbix were performed, including the definition of alerts and the creation of monitoring dashboards. Monitoring has been continuously conducted, allowing for the identification of faults and the assessment of the tool's effectiveness. As a result of the implementation of Zabbix, there has been a reduction in the detection and correction of network faults, contributing to a more efficient and safer operation. Furthermore, the ability to predict problems before they cause process interruptions has led to a reduction from 15% to 6.5% in unplanned downtime. These results demonstrate the positive impact of using Zabbix on the performance management of the steelmaking process in the steel industry.

Keywords: *Zabbix, failure management, steel process, steel mill.*

Lista de ilustrações

Lista de tabelas

Lista de siglas

API	Interface de Programação de Aplicação (API, do inglês *Application Programming Interface*)
BOF	Forno de Oxigênio Básico (BOF, do inglês *Basic Oxigen Furnace*)
CAN	Rede de Área de Controle (CAN, do inglês *Control Area Network*)
CPU	Unidade Central de Processamento (CPU, do inglês *Central Processing Unit*)
E/S	Entrada e Saída
ICMP	Protocolo de Mensagens de Controle da Internet (ICMP, do inglês *Internet Control Message Protocol*)
IHM	Interface Homem Máquina (IHM, do inglês *Human Machine Interface*)
IOS	Sistema Operacional Interligado (IOS, do inglês *Internetwork Operating System*)
IPMI	Interface de Gerenciamento de Plataforma Inteligente (IPMI, do inglês *Intelligent Platform Management Interface*)
LD	Linz-Donawitz (LD)
LTS	Suporte de Longo Prazo (LTS, do inglês *Long-term Support*)
MES	Sistemas de Execução de Manufatura (MES, do inglês *Manufacturing Execution Systems*)
MLC	Máquina de Lingotamento Contínuo (MLC)
MOC	Máquina de Oxi-Corte (MOC)
OID	Identificador de Objeto (OID, do inglês *Object Identifier*)
OPC	Comunicação de Plataforma Aberta (OPC, do inglês *Open Platform Communication*)
OSI	Interconexão de Sistemas Abertos (OSI, do inglês *Open System Interconnection*)
PCs	Computadores Pessoal (PCs, do inglês *Personal Computer*)
PIB	Produto Interno Bruto

PIMS	Sistemas de Gerenciamento de Informações da Planta (PIMS, do inglês *Plant Information Management Systems*)
PLC	Controlador Lógico Programável (PLC, do inglês *Programmable Logic Controller*)
QoS	Qualidade do Serviço (QoS)
SAP	Desenvolvimento de Programas para Análise de Sistema (SAP, do alemão *Systemanalysis Programmentwicklung*)
SCADA	Sistema de Supervisão e Aquisição de Dados (SCADA, do inglês *Supervisory Control and Data Acquisition*)
SDCDs	Sistemas Digitais de Controle Distribuído (SDCDs)
SNMP	Protocolo Simples de Gerenciamento de Redes (SNMP, do inglês *Simple Network Management Protocol*)
TI	Tecnologia da Informação (TI, do inglês *Information Technology*)
TA	tecnologia da automação (TA, do inglês *Operational Technology*)
VMs	Máquinas Virtuais (do inglês, *Virtual Machines*)

Sumário

1 Introdução

As redes industriais desempenham um papel essencial na automação industrial e são cruciais na siderurgia, uma indústria fundamental para a economia global. No entanto, a gestão dessas redes enfrenta desafios, incluindo falhas que podem afetar a produção e a segurança. Portanto, a detecção de falhas nessas redes torna-se uma prioridade para manter a operação contínua da indústria siderúrgica, além de preservar sua competitividade econômica.

1.1 Contextualização

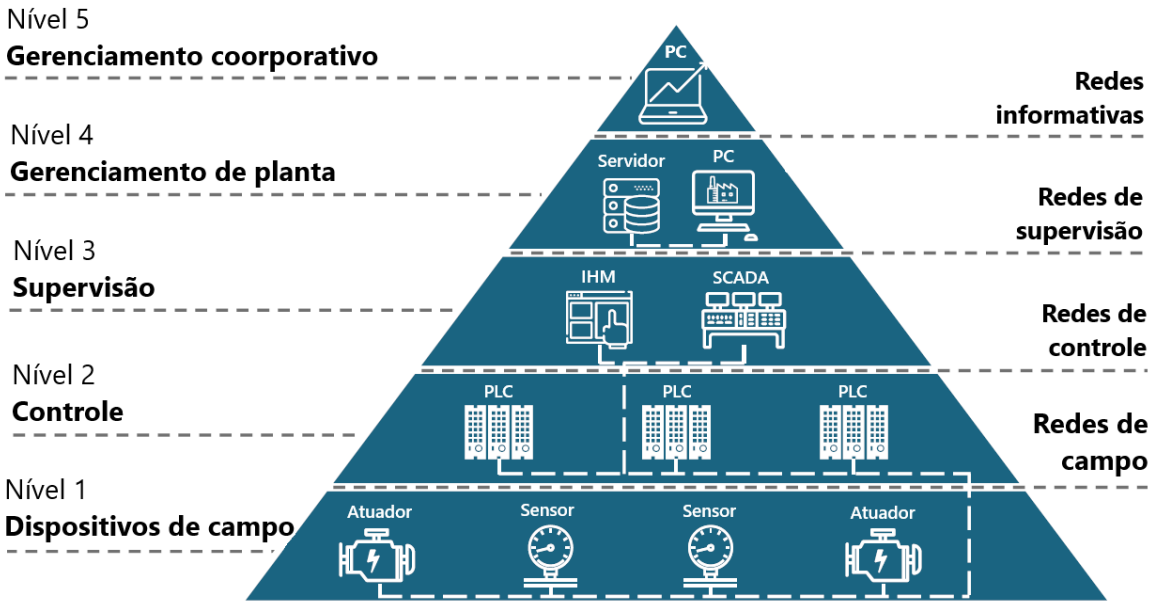
A automação refere-se à aplicação de tecnologia para realizar tarefas repetitivas e nocivas sem intervenção humana, buscando eficiência, precisão e aumento da produtividade (RIBEIRO, 2005). A relevância dos sistemas de automação transcende a execução de tarefas repetitivas, estendendo-se para uma evolução integral na eficiência operacional e na qualidade dos produtos, por meio da implementação de tecnologias avançadas, como sensores, atuadores, Controlador Lógico Programável (PLC, do inglês *Programmable Logic Controller*) e o Sistema de Supervisão e Aquisição de Dados (SCADA, do inglês *Supervisory Control and Data Acquisition*).

Um exemplo concreto desse impacto pode ser observado no processo de produção de aço, no qual o PLC é utilizado, por exemplo, para controle de abertura e fechamento de válvulas de silos de materiais utilizados na produção dos aços, através do comando realizado pelos sistemas SCADA. Em seguida, é retirado amostras do aço, a fim de analisar sua composição química, as informações obtidas nesta análise podem ser acompanhadas pelo sistema de supervisão, que permitem a reintervenção do PLC, quando necessário, para ajuste da adição de ligas, a fim de atender às especificações exatas do aço desejado. Ao incorporar a automação em processos industriais, as empresas buscam alcançar níveis mais elevados de produtividade, redução de custos, e o aprimoramento das condições de trabalho (BRANQUINHO et al., 2014).

A interconexão dos equipamentos responsáveis pelo sistema de automação é essencial para garantir o funcionamento do sistema em sua totalidade (RIBEIRO, 2005). Nesse sentido, a pirâmide de automação emerge como um conceito para ilustrar a hierarquia e a interconexão dos diferentes níveis de automação em um sistema industrial, como pode ser observado na Figura 1. Essa estrutura hierárquica representa a organização dos sistemas de automação, abrangendo desde os dispositivos de campo até as camadas de supervisão e gerenciamento em ambientes industriais.

Segundo Mondadori (2016), o nível 1 da pirâmide é composto de dispositivos de campo, ou seja, os dispositivos de entrada e saída, responsáveis pela coleta e execução de

Figura 1 – Pirâmide da automação.



Fonte: Adaptado de Kiesel et al. (2021).

dados no ambiente de produção. A comunicação com este nível é realizada pelos protocolos de redes de campo, como, por exemplo, a *DeviceNet*, *FieldBus*, entre outras. O nível 2 é composto por dispositivos de controle, como o PLC e Sistemas Digitais de Controle Distribuído (SDCDs), que interpretam e processam os dados provenientes do chão de fábrica, realizando ajustes dinâmicos nos processos. A interconexão é viabilizada pelos protocolos de redes de controle, como, por exemplo, as redes *Ethernet/IP*, *Profibus*, *Control Net*, entre outras (DJIEV, 2016).

O nível 3 é composto pelos sistemas supervisórios, estações de engenharia, Computadores Pessoal (PCs, do inglês *Personal Computer*), Interface Homem Máquina (IHM, do inglês *Human Machine Interface*) e servidores (GALLOWAY; HANCKE, 2012), que monitoram e controlam as operações em tempo real, garantindo o funcionamento eficiente e seguro dos processos industriais. A interligação neste nível ocorre por meio dos protocolos de redes de supervisão como, por exemplo, *FieldBus*, Comunicação de Plataforma Aberta (OPC, do inglês *Open Platform Communication*) e a *Ethernet/IP* (LUGLI; SANTOS, 2014).

O nível 4 é composto por *softwares* de gerenciamento e estações de engenharia, que se concentram na coordenação e otimização das atividades de produção em toda a planta industrial, visando melhorar a eficiência global e atender aos objetivos de produção. O último nível é composto de *softwares* de gestão de vendas e financeiro, como, por exemplo, o Desenvolvimento de Programas para Análise de Sistema (SAP, do alemão *Systemanalysis Programmentwicklung*), uma solução que integra uma variedade de processos empresariais, incluindo contabilidade, recursos humanos, distribuição e gerenciamento de

cadeia de suprimentos (GALLOWAY; HANCKE, 2012). A comunicação nos dois últimos níveis é geralmente realizada por meio de redes informativas ou também conhecidas como corporativas convencionais, como, por exemplo, as redes *Ethernet*.

A confiabilidade dos sistemas de automação está atrelada ao desempenho adequado de cada componente e do funcionamento das redes industrias (RIBEIRO, 2005). A gestão de falhas constitui a área do gerenciamento de redes dedicada a abordar essa preocupação específica. Conforme apresentado por Forouzan (2009), um sistema de gerenciamento de falhas é constituído por dois subsistemas distintos: o gerenciamento de falhas reativo e o gerenciamento de falhas proativo.

O gerenciamento de falhas reativo concentra-se na detecção, isolamento e correção imediata de falhas, minimizando o impacto negativo na operação. Um exemplo de falha detectada por este gerenciamento seria um meio de transmissão danificado, que poderia interromper a comunicação entre dois dispositivos ou gerar um número excessivo de erros (FOROUZAN, 2009).

Em contrapartida, o gerenciamento proativo visa prevenir a ocorrência de falhas, adotando estratégias preventivas baseadas em análise preditiva (VARGAS, 2020). Esse tipo de gerenciamento é possível através da análise do histórico de dados da rede, através da observação de tendências na análise de desempenho de seus dados. Para exemplificar, considere a ocorrência frequente de uma falha de transmissão em um dado ponto de uma rede, assim seria viável realizar a reconfiguração da arquitetura nesse ponto. Outra forma de aplicar este gerenciamento é através das especificações do fabricante de um equipamento, como a configuração e vida útil, seguir essas orientações é uma forma de gerenciamento proativo.

O gerenciamento de desempenho é o recurso que permite a detecção das falhas, através da percepção de anormalidades dos dados coletados. Essa abordagem visa quantificar o desempenho da rede utilizando medidas mensuráveis, tais como capacidade, tráfego e tempo de resposta, que contribuem no monitoramento e controle da rede a fim de aumentar sua confiabilidade (FOROUZAN, 2009).

As falhas em redes industriais podem originar-se de diferentes fontes, como falhas de *hardware*, *software*, configuração, entre outras (TURNER et al., 2010). Falhas relacionadas a *hardware* estão frequentemente associadas ao uso inadequado do equipamento como, uso excessivo de Unidade Central de Processamento (CPU, do inglês *Central Processing Unit*); influências externas como, falta de alimentação ou interferência eletromagnética (SILVA; JÚNIOR, 2011); à obsolescência (CESAR et al., 2020), exigindo investimentos para a atualização ou substituição desses componentes. Além disso, essas falhas podem ser influenciadas devido ao ambiente que os equipamentos operam, gerando maior possibilidade de ocorrer em ambientes hostis como, por exemplo, ambientes com muita poeira, altas temperaturas, entre outros (BHARGAVA; BANGA; SINGH, 2014).

Falhas de *software* podem decorrer da necessidade de atualizações ou substituições

de sistemas, demandando investimentos em desenvolvimento e implementação de novas soluções (CESAR et al., 2020). Um exemplo dessas falhas são *softwares* que não funcionam por estarem desatualizados, configuração incorreta, incompatibilidade com *hardware*, entre outros (TURNER et al., 2010).

No que se refere às falhas de configuração, elas frequentemente requerem investimentos em treinamento ou contratação de mão de obra qualificada, além de auditorias periódicas para garantir que as configurações estejam alinhadas com as melhores práticas de segurança. Um exemplo dessa falha seria sobrecarga de dados de uma rede devido ao excesso de ativos interconectados, ou conectados com uma arquitetura inapropriada.

No contexto das falhas citadas, é evidente que uma boa gestão do desempenho das redes e dos ativos a elas vinculados é fundamental para a implementação de estratégias gerenciais reativas e proativas. Essa abordagem é viabilizada por meio da análise do parâmetro como o tráfego de dados, a taxa de utilização da CPU, temperatura do dispositivo, utilização de disco, entre outros parâmetros relevantes (TURNER et al., 2010).

Assim, é evidente que o gerenciamento de desempenho de redes apresenta um papel relevante na gestão desses eventos. Opções populares de ferramentas de monitoramento para redes incluem o *Nagios* (BARTH, 2008), o *Zabbix* (ZABBIX, 2014) e o *SolarWinds* (PEISERT et al., 2021).

O *software Nagios* é uma ferramenta de código que oferece recursos de monitoramento de rede e é altamente personalizável, permitindo aos usuários adaptá-lo às suas necessidades específicas. No entanto, o *Nagios* pode exigir uma curva de aprendizado íngreme e requer configuração manual detalhada (BARTH, 2008).

Por outro lado, o *software SolarWinds* é uma solução comercial popular conhecida por sua interface amigável e conjunto abrangente de recursos. Ele oferece monitoramento em tempo real, alertas proativos e relatórios detalhados, tornando-o uma escolha atraente para organizações que valorizam a facilidade de uso e a funcionalidade abrangente. No entanto, o *SolarWinds* pode ser mais caro em comparação com outras opções devido à sua natureza comercial (PEISERT et al., 2021).

O *software Zabbix*, por sua vez, destaca-se pela sua capacidade de monitoramento avançado e escalabilidade. Ele oferece uma ampla gama de recursos, incluindo monitoramento de desempenho em tempo real e alertas configuráveis. Além disso, o *Zabbix* é gratuito e sua arquitetura flexível e modular permite a integração com uma variedade de dispositivos e sistemas, tornando-o uma escolha versátil para organizações que buscam uma solução abrangente de monitoramento de desempenho de redes (ZABBIX, 2014).

Conforme observado, cada uma dessas ferramentas apresenta características distintas, proporcionando alternativas para atender às necessidades específicas de diferentes ambientes industriais. A escolha do *Zabbix* como ferramenta de monitoramento para a rede *Ethernet* Industrial na planta de estudo fundamenta-se na facilidade de visualização das informações coletadas, acessibilidade à informação para implementação da ferramenta,

gratuidade do *software* e eficácia previamente comprovada pelo amplo reconhecimento em grandes empresas (ZABBIX, 2014). O *Zabbix* oferece recursos avançados de coleta e análise de dados, permitindo uma visão do desempenho dos ativos de controle e supervisão. Uma desvantagem potencial do *Zabbix* é o consumo de recursos. Por ser uma ferramenta abrangente, o *Zabbix* pode consumir mais recursos de hardware, como CPU e memória, em comparação com soluções mais simples.

Este trabalho visa realizar o monitoramento de uma rede *Ethernet Industrial*, adaptação da rede *Ethernet* convencional para conexão de sistemas e dispositivos inteligentes em ambientes industriais, com foco específico no gerenciamento de falhas da redes que operam com os protocolos *Ethernet/IP* e *Profinet*, utilizados para interconexão dos equipamentos dos níveis de controle e supervisão da etapa da aciaria de um processo siderúrgico. A implementação da ferramenta visa aprimorar a avaliação de desempenho dos dispositivos de rede, permitindo o gerenciamento reativo e proativo de falhas na rede e nos equipamentos conectados como, por exemplo, PLC, *switches*, servidores, *clients*, *workstations* e computadores.

Neste trabalho, consideram-se as falhas de *hardware* e de configuração como, por exemplo, análise de tráfego de dados, *status* de dispositivos, a utilização da CPU, uso do disco, uso de memória e a temperatura operacional. Ademais, destaca-se que, anteriormente na aciaria, não havia monitoramento do desempenho dos ativos, contudo, por meio da implementação do *Zabbix*, tornou-se possível a realização desse acompanhamento.

Embora a maioria dos estudos encontrados na literatura se concentre predominantemente na aplicação de estratégias de gerenciamento de desempenho em PLC e servidores no domínio da automação industrial, optou-se por incorporar elementos adicionais, como *switches*, *clients*, *workstations* e computadores. Essa decisão foi motivada pela escolha estratégica e exigências específicas inerentes à infraestrutura da planta de pesquisa em questão. A pesquisa aborda a utilização do Protocolo Simples de Gerenciamento de Redes (SNMP, do inglês *Simple Network Management Protocol*) em paralelo à ferramenta de monitoramento, *Zabbix*, para coleta e visualização de dados, e configuração das informações coletadas.

1.2 Estado da arte

Apesar da escassez de estudos específicos na literatura sobre o monitoramento do desempenho da rede de automação industrial, existem alguns estudos realizados em ambientes distintos que forneceram valiosas contribuições para a realização deste trabalho. Essas pesquisas aplicadas em contextos diversos são essenciais para embasar e fundamentar as abordagens adotadas neste estudo, permitindo a adaptação e aplicação dos conhecimentos existentes para o contexto da automação industrial.

Ivankio (2019) destaca a contribuição das redes industrias no monitoramento de

parâmetros que auxiliam na redução do número de interrupções no processo de transmissão de energia na subestação Curitiba Norte. No entanto, essas redes muitas vezes carecem de sistemas de segurança, que conseguem expor a produção dos serviços a riscos e causar danos aos equipamentos. Com o avanço das tecnologias de telecomunicações, houve uma convergência entre a TI e a TA, revelando as fragilidades desses ambientes. O estudo enfatiza que a rede de automação é complexa e requer não apenas *software* e *hardware* específicos, mas também profissionais capacitados para garantir seu funcionamento adequado. Além disso, as redes de automação fornecem uma variedade de aplicações e dados em tempo real, tornando cada vez mais importante o monitoramento contínuo da Qualidade do Serviço (QoS). O monitoramento contínuo dos parâmetros de QoS, como largura de banda e latência, em uma rede de automação consegue antecipar problemas relacionados a vírus e defeitos de equipamentos, como *switches*. Nesse contexto, o objetivo do trabalho em questão é realizar o monitoramento remoto de equipamentos da rede de automação, como *switches* e servidores instalados nas subestações. Esses equipamentos utilizam o SNMP. Neste trabalho, a ferramenta *Zabbix* é utilizada para implantar um servidor que execute o monitoramento e armazene os dados coletados.

Forouzan (2009) conceitua o gerenciamento de redes como um conjunto de atividades abrangendo monitoramento, teste, configuração e diagnóstico de componentes de rede, com o propósito de atender a requisitos específicos estipulados por uma organização. Os requisitos acentuam a operação estável da rede, garantindo a entrega da qualidade previamente definida de serviços aos usuários. O sistema de gerenciamento de redes, objeto de discussão no capítulo, emprega uma sinergia de *hardware*, *software* e intervenção humana. O trabalho aborda inicialmente concisamente as funções gerais de um sistema de gerenciamento de redes, direcionando posteriormente seu foco ao SNMP, destacado como o padrão predominante de gerenciamento de redes. Dada a complexidade das redes, constituídas por centenas ou até milhares de componentes, a confiabilidade da operação depende do desempenho de cada elemento, tanto individual quanto coletivamente. O gerenciamento de falhas é identificado como a área especializada responsável por abordar essa problemática. O autor enfatiza a presença de dois subsistemas no sistema de gerenciamento de falhas: o gerenciamento reativo e proativo, ambos interligados ao gerenciamento de desempenho.

Branquinho et al. (2014) aborda conceitos essenciais relacionados ao estabelecimento da governança de segurança em ambientes de rede industrial. O autor destaca instrumentos cruciais para a gestão de infraestruturas críticas, como modelos de gestão, normas de referência e elementos para a elaboração de políticas. Além disso, são desenvolvidos conceitos que proporcionam uma visão sobre a segurança nesse contexto, incluindo a gestão da continuidade de negócios. O foco se direciona para o monitoramento dos servidores críticos de uma rede de automação. É relevante destacar que o autor explora o conceito de qualidade de serviço e sua relação com a saúde da rede, enfatizando

parâmetros essenciais para a detecção de anomalias causadas por agentes maliciosos. O trabalho apresenta diversas provas de conceito, fornecendo testes realizados contra dispositivos e servidores de automação para ilustrar a importância do monitoramento contínuo na garantia da segurança e integridade do sistema. Vale ressaltar que, no contexto do monitoramento de desempenho em redes industriais, o autor cita explicitamente o uso da ferramenta *Zabbix* como parte integrante da estratégia de monitoramento adotada. Essa ferramenta desempenha um papel relevante na supervisão e análise do desempenho, contribuindo para a eficácia do sistema de segurança e integridade da rede industrial.

Valente (2023) aborda a importância do monitoramento contínuo e em tempo real dos ativos em uma mina com uma ampla arquitetura de rede. A falta de um sistema proativo e em tempo real dificulta a detecção ágil de problemas, o que pode resultar em atrasos no processo produtivo. A implementação da ferramenta *open source Zabbix* foi avaliada como uma solução para melhorar a eficiência e a segurança operacional. Os resultados mostraram que o *Zabbix* contribuiu para reforçar a segurança da rede, aprimorar a detecção de falhas e viabilizar manutenções preditivas, destacando-se como uma ferramenta eficaz para o monitoramento de ativos em rede de automação.

Tostes (2022) implementa um sistema de monitoramento e controle avançado para um *Data Center* do Instituto Federal de Minas Gerais - Campus Ouro Preto, um ambiente crítico que requer controle preciso das condições ambientais e operacionais. A integração do *Arduino* com o *Zabbix* possibilita uma supervisão em tempo real e uma resposta rápida a eventos que comprometam a operação do *Data Center*. Ao integrar o *Zabbix*, com o *Arduino*, uma plataforma flexível e de baixo custo, o sistema alcança um equilíbrio entre desempenho e acessibilidade. Isso não apenas beneficia o Instituto Federal de Minas Gerais – Campus Ouro Preto em termos de eficiência operacional e segurança do *Data Center*, mas também demonstra uma abordagem inovadora e acessível para o monitoramento de infraestruturas críticas. Além disso, a aplicação bem-sucedida do protótipo destaca a viabilidade e eficácia da solução proposta, destacando-se como uma contribuição significativa para a comunidade acadêmica e profissional interessada em soluções práticas e acessíveis para monitoramento de *Data Centers*.

1.3 Justificativa

A relevância do tema escolhido para este trabalho é ressaltada devido à centralidade das indústrias no atual panorama econômico. Esses complexos industriais não são apenas pilares de produção, são, essencialmente, motores que impulsionam o crescimento econômico, com impacto substancial no Produto Interno Bruto (IAB, 2016) e sua influência na geração de empregos. Portanto, otimizar e assegurar a eficiência das redes industriais em plantas siderúrgicas transcende a mera operacionalidade, tornando-se uma estratégia imperativa para garantir a resiliência e viabilidade do segmento industrial.

Essa necessidade ganha contornos ainda mais críticos ao considerar os ambientes intrinsecamente desafiadores em que essas plantas industriais estão inseridas. Em tais contextos, marcados por condições extremas e alta demanda de disponibilidade, os equipamentos eletrônicos das redes industriais das instalações estão continuamente expostos a fatores que potencializam as chances de falhas (BHARGAVA; BANGA; SINGH, 2014). Seja devido a condições adversas como superaquecimento, umidade, corrosão ou acúmulo de poeira, a vulnerabilidade de equipamentos que compõe as redes de controle e supervisão torna-se uma preocupação latente, ressaltando a importante estratégia de análise de desempenho e mitigação das falhas.

Dentro desse cenário de complexidade e desafios, é imperativo reconhecer que a evolução constante dos sistemas de automação amplifica as demandas sobre as infraestruturas existentes. À medida que as indústrias se adaptam ao crescente tráfego de dados e aos avanços tecnológicos, a rede industrial se torna ainda mais suscetível a falhas, caso seu avanço não seja acompanhado por uma análise de arquitetura e capacidade de comunicação (FOROUZAN, 2009). Neste contexto dinâmico, a implementação de estratégias proativas de monitoramento de desempenho não é apenas uma abordagem prudente, mas uma necessidade urgente.

Ao considerar a planta de estudo deste trabalho, destaca-se um desafio adicional, a presença predominante de infraestruturas industriais obsoletas. Essa obsolescência abrange tanto o *hardware* quanto o *software*, amplificando significativamente as chances de falhas e interrupções no sistema (CESAR et al., 2020). Ademais, a interação desses equipamentos em um ambiente operacional agressivo, como é caracterizado os ambientes siderúrgicos, cria um cenário propício para falhas. O desgaste natural desses componentes, combinado com a incapacidade de acompanhar plenamente as demandas contemporâneas, amplifica os riscos de interrupções e falhas críticas.

Aprofundando essa perspectiva, a análise detalhada da planta de estudo revela estatísticas preocupantes. Ao longo de um período de 12 meses, aproximadamente 15% das interrupções operacionais estão diretamente associadas a deficiências na infraestrutura de rede e falhas dos ativos dos níveis de controle e supervisão. Dada a vastidão de equipamentos em ambientes industriais siderúrgicos, detectar precocemente tais falhas se transforma em um desafio monumental, ampliando as vulnerabilidades operacionais e evidenciando a imperativa necessidade de intervenções estratégicas.

Diante dessas considerações e desafios delineados, torna-se claro que a análise de desempenho das redes industriais de controle e supervisão nas plantas siderúrgicas não é apenas uma visão técnica, mas uma necessidade estratégica para a planta de estudo. A busca incessante por eficiência e adaptabilidade em meio a ambientes operacionais reitera a importância deste estudo.

1.4 Objetivos

O objetivo deste trabalho é implantar a ferramenta *Zabbix* para gerenciamento de desempenho das redes dos níveis de controle e supervisão da rede *Ethernet* industrial da etapa da aciaria de um processo siderúrgico, com aplicação para os protocolos *Profinet* e *Ethernet/IP*, visando contribuir para a eficiência e confiabilidade da rede da planta de estudo e, consequentemente, do processo produtivo.

Para alcançar esse objetivo, são definidos objetivos específicos, tais como:

- Definir as categorias de ativos que serão monitorados;
- Especificar os ativos que serão monitorados em cada categoria;
- Determinar os parâmetros de monitoramento que serão adquiridas;
- Estabelecer os parâmetros de monitoramento que serão adquiridas;
- Implantar a ferramenta *Zabbix* na rede *Ethernet* industrial da aciaria de um processo siderúrgico;
- Aquisição dos dados e analise os resultados obtidos.

1.5 Estrutura do trabalho

Este trabalho está dividido em cinco capítulos. O Capítulo 1 introduz o tema por meio de uma contextualização, apresentando o problema em questão, os objetivos a serem alcançados, bem como as justificativas para o estudo e sua aplicação.

No capítulo 2, é realizada uma revisão bibliográfica breve, sobre estudos relacionados ao tema em questão. É abordado a descrição da fundamentação teórica, por meio da conceituação da automação industrial; explicação sobre as redes industriais; esclarecimento sobre a importância do monitoramento de ativos e da rede de automação, explanação sobre ferramentas de monitoramento de redes — *Zabbix*, focando em sua arquitetura, funcionalidades e protocolos suportados; e a abordagem de outras ferramentas de monitoramento de redes industriais.

No capítulo 3 é apresentado o desenvolvimento do trabalho, por meio da apresentação da metodologia do trabalho, descrição do ambiente industrial utilizado para o estudo; explicação sobre a configuração do *Zabbix* para monitoramento de ativos e da rede de automação; definição dos parâmetros de monitoramento a serem adquiridas e aquisição de dados.

No capítulo 4 são apresentados os resultados alcançados da aplicação da ferramenta *Zabbix* em um ambiente industrial, destacando os ativos monitorados e os parâmetros que são objeto de monitoramento.

Por fim, no capítulo 5, são apresentadas as considerações finais e sugestões de trabalhos futuros.

2 Revisão teórica

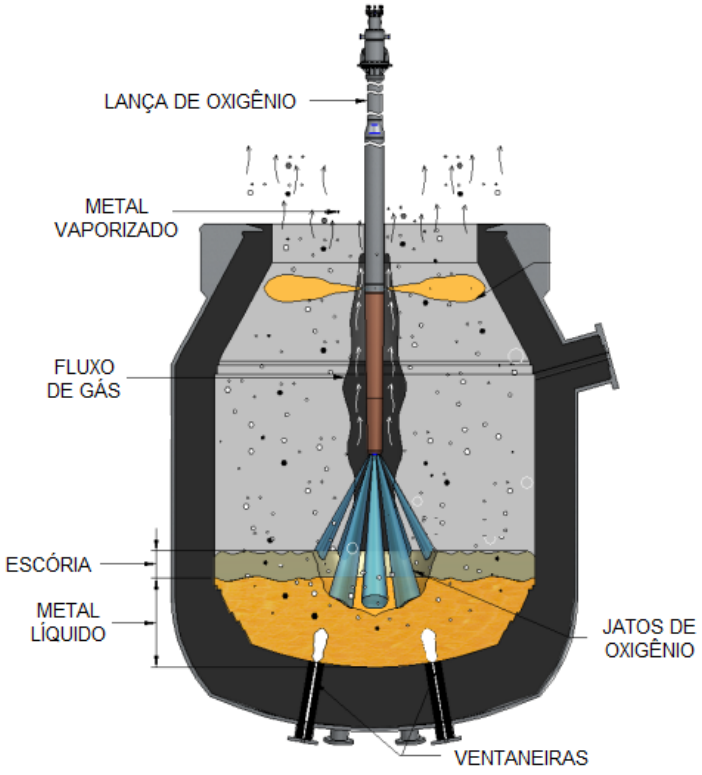
Neste capítulo, serão apresentados alguns estudos relevantes constituídos na literatura, que abordam e contribuem para o entendimento do processo de produção da aciaria e do tema de gerenciamento de falhas de redes, visando proporcionar uma compreensão das principais técnicas, ferramentas e soluções disponíveis, com o foco na ferramenta *Zabbix*, utilizada para o desenvolvimento deste trabalho.

2.1 Processo de produção da aciaria

A aciaria é uma parte da instalação industrial de uma siderúrgica, responsável pela produção de aço. Ela é composta por uma série de equipamentos e sistemas que realizam a fusão do ferro-gusa e sua transformação em aço (TÂMEGA, 2017), essas etapas são realizadas no forno Linz-Donawitz (LD) e na Máquina de Lingotamento Contínuo (MLC) (MOURÃO et al., 2007).

Um dos equipamentos da aciaria é o LD, também conhecido como convertedor ou Forno de Oxigênio Básico (BOF, do inglês *Basic Oxigen Furnace*), conforme apresentado na Figura 2.

Figura 2 – Convertedor LD.

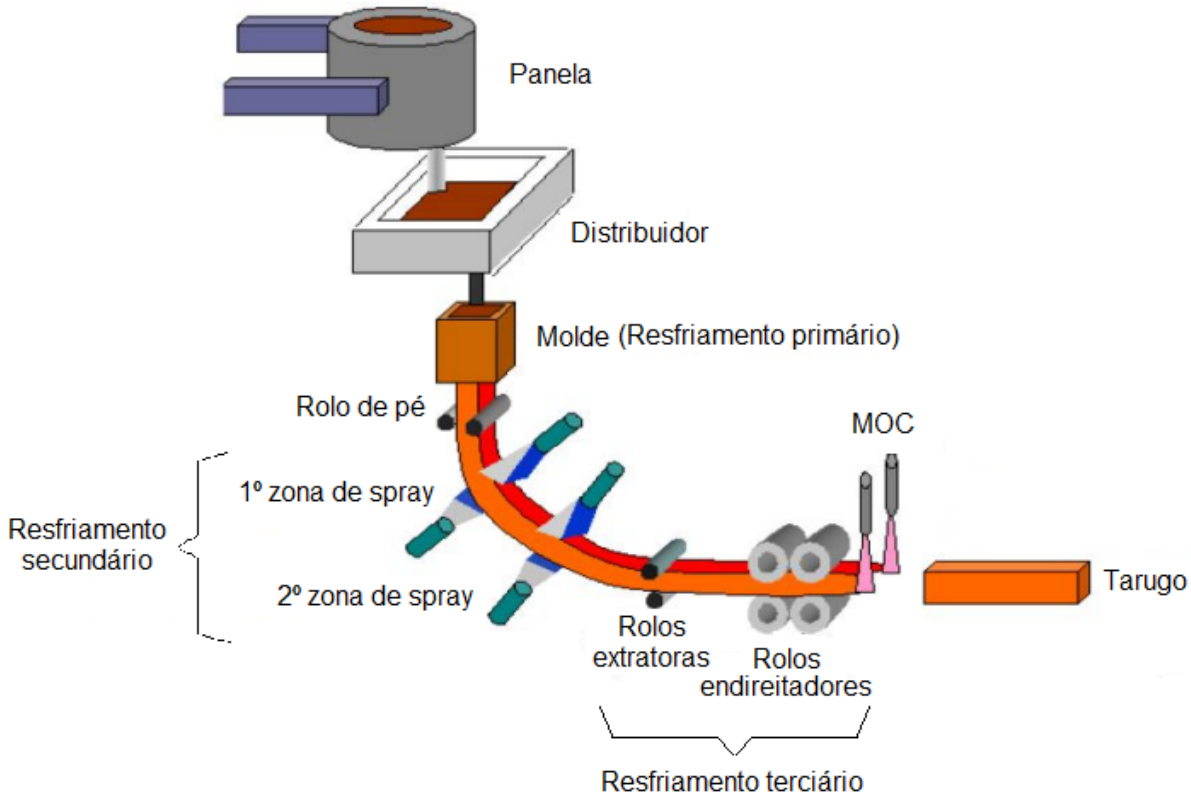


Fonte: Adaptado de Maia et al. (2018).

Segundo TÂMEGA (2017), o processo de produção de aço no forno LD é baseado na oxidação das impurezas presentes no ferro-gusa através do O_2 injetado no forno. Para isso, ainda segundo TÂMEGA (2017), o ferro-gusa é fundido e então transferido para o forno LD. Em seguida, uma lança de oxigênio, é introduzida no convertedor e realiza o sopro do O_2. A alta pressão e temperatura do oxigênio resultam na queima das impurezas, eliminando-as na forma de escória (MACHADO, 2006). O aço resultante do processo de refino no forno LD é caracterizado por um baixo teor de impurezas e carbono.

De acordo com TÂMEGA (2017), após a fusão, o aço líquido é transferido para a MLC, Figura 3, equipamento este responsável por transformar o aço em lingotes, ou também conhecido como tarugos. Desenvolvida na década de 1950, a MLC consiste em um processo de fundição contínua do aço em lingotes (MACHADO, 2006). Antes do surgimento dessa tecnologia, a produção de aço era feita por meio de processos mais lentos e com interrupções, como o vazamento do aço fundido em moldes de areia ou em lingoteiras (TÂMEGA, 2017).

Figura 3 – Máquina de lingotamento contínuo.



Fonte: Adaptado de Ferreira (2010).

Nesta etapa do processo, o aço fundido é despejado em um distribuidor que o direciona para um molde metálico. O molde é uma forma retangular refrigerada por água que mantém a temperatura do aço em níveis adequados para a solidificação (TÂMEGA, 2017), a geometria do molde é projetada conforme o perfil desejado do produto final.

Ao redor do molde se encontra o agitador, dispositivo que tem a função de garantir movimentação interna do metal líquido, a fim de reduzir a formação de bolhas de gás, trincas e outros defeitos de solidificação. Desta forma, conforme apresentado por Soares (2017), o bom desempenho dos agitadores está diretamente relacionado à qualidade do aço produzido, e por esse motivo seu bom funcionamento é fundamental na produção de aços.

Ao passar pelo molde, o aço começa a ter sua casca solidificada e desce pelo raio da máquina, trajetória curva que conduz o aço até os rolos extratoras. Durante esse percurso, o aço é puxado pelos rolos, equipamentos responsáveis por ajudar a controlar a sua velocidade e direção. Além disso, segundo Soares (2017), a máquina de lingotamento contínuo é dividida em três zonas de resfriamento, cada uma com sua própria função e equipamentos específicos. O resfriamento primário é a zona de pré-resfriamento, região onde o aço fundido entra em contato com o molde resfriado por água e começa a se solidificar, formando assim uma casca. A zona seguinte é a zona de resfriamento secundário, onde o aço é resfriado por jatos de água enquanto desce pelo raio da máquina, ajudando a estabilizar a temperatura do aço e a reduzir as tensões internas. A última é a zona de resfriamento terciário, onde o aço solidificado é cortado no tamanho desejado, pela Máquina de Oxi-Corte (MOC), Figura 3, ferramenta de corte que utiliza jato de oxigênio para cortar o aço sólido em pedaços menores, conhecidos como tarugos.

Nesse cenário, ressalta-se a importância dos sistemas de automação no contexto da produção da aciaria. Eles desempenham um papel fundamental no controle e supervisão dos equipamentos envolvidos, desde o funcionamento do forno LD até a operação da MLC.

2.2 Redes industriais

Redes industriais referem-se a sistemas de comunicação interconectados que permitem a troca de dados entre dispositivos e sistemas em ambientes industriais (RIBEIRO, 2005), desempenhando um papel importante no gerenciamento e controle dos processos industriais. Elas consistem em sistemas de comunicação automatizados e especializados, desenvolvidos para atender às demandas únicas e complexas das instalações industriais modernas. Elas têm se tornado cada vez mais importantes no contexto da indústria moderna, permitindo a integração entre diversos dispositivos, equipamentos e plantas de processos produtivos. Segundo Mondadori (2016), essas redes são as responsáveis pela comunicação (ou seja, troca de informações) entre sensores, atuadores, controladores, supervisórios, PLC e outros dispositivos, permitindo o controle e a automação de processos de forma mais assertiva e segura.

2.2.1 Classificação

As redes industriais são, normalmente, classificadas em seis tipos: *SensorBus*, *DeviceBus*, *FieldBus*, *DataBus*, *Ethernet* Industrial e *Wireless* (CARLSSON, 2023). Essa categorização reflete a diversidade de tecnologias disponíveis para suportar as necessidades complexas e variadas de comunicação em ambientes industriais. A escolha adequada da tecnologia de rede utilizada é crucial para garantir não apenas a transmissão rápida de dados, mas também a segurança e a confiabilidade dos processos industriais. Essa decisão depende de fatores como largura de banda, confiabilidade, alcance e requisitos específicos de aplicação.

As *SensorBus* são as redes que conectam sensores, atuadores e outros dispositivos localizados no chão de fábrica, permitindo a obtenção de dados em tempo real e o controle do processo produtivo (LUGLI; SANTOS, 2014). São caracterizadas por serem utilizadas em controle de lógica, possuírem um baixo custo, trafegam dados em formato de bits e atingem pequenas distâncias. Elas enviam dados para a camada superior da rede, onde são processados e utilizados para o controle do processo.

DeviceBus são as redes que conectam os dispositivos de *I/O* e seus periféricos, como, por exemplo, o Controlador Lógico Programável (PLC, do inglês *Programmable Logic Controller*) e IHM, permitindo a programação e o monitoramento do processo produtivo (RIBEIRO, 2005). São caracterizadas por serem utilizadas para controle de processo, possuírem transmissão de dados em *bytes* ou *words* e atingem distâncias de centenas de metros. Nessa camada, são utilizados *switches*, roteadores e *gateways* para possibilitar a comunicação entre os dispositivos de controle e os dispositivos das camadas inferiores e superiores da rede.

FieldBus são as redes que conectam os dispositivos inteligentes, como, por exemplo, os sistemas de supervisão, permitindo a obtenção de dados e informações do processo produtivo para análise e tomada de decisões. São caracterizadas por serem utilizadas no controle de processo, possuem uma transmissão de dados em *words* ou blocos e uma frequência de comunicação de milissegundos. Nessa camada, também são utilizados *switches*, roteadores e *gateways* para possibilitar a comunicação entre os supervisórios e os dispositivos das camadas inferiores da rede, e também à rede corporativa para que nela seja possível realizar a análise dos dados obtidos pelo processo de produção (FERNANDEZ, 2015).

DataBus são as redes que conectam os computadores (*hosts*), ou seja, elas realizam uma transferência maciça de dados (RIBEIRO, 2005). São caracterizadas pelo envio de dados em blocos ou arquivos e possui uma frequência de comunicação em segundos ou minutos, devido ao grande número de dados.

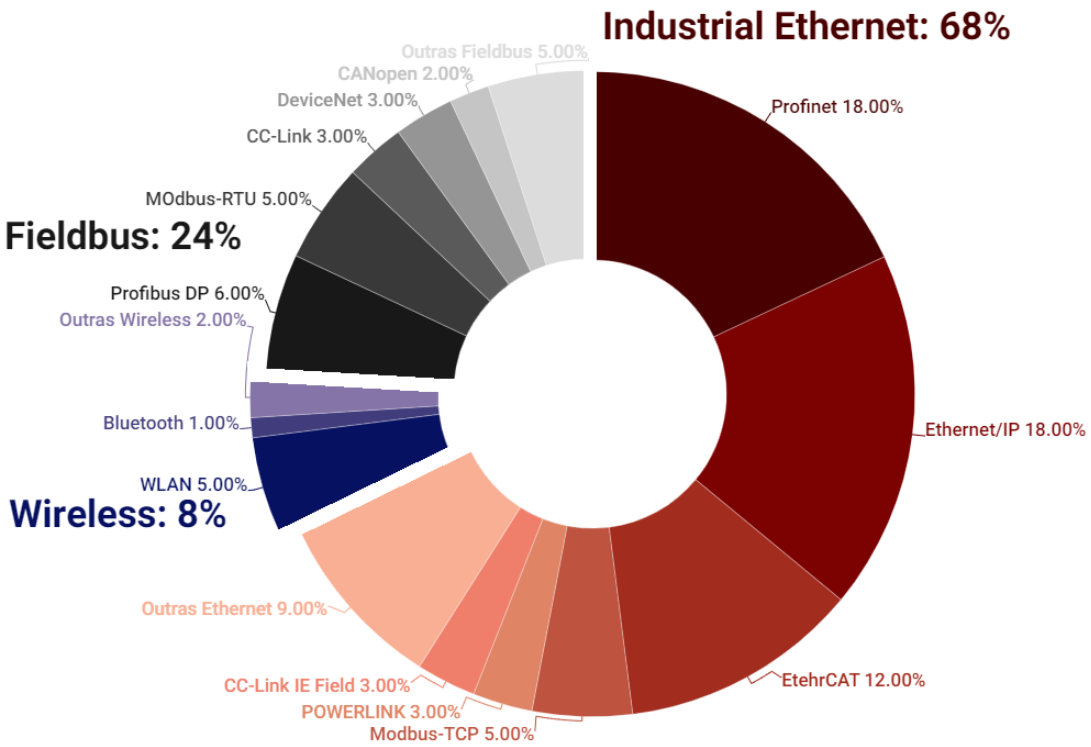
As redes *Ethernet Industrial* são redes projetadas para conectar dispositivos industriais, como controladores e sensores, viabilizando a comunicação em ambientes industriais rigorosos (MARCHALL; RINALDI, 2004). Utilizadas no controle de processo, essas redes

transmitem dados em pacotes, garantindo rapidez e precisão na troca de informações. Na infraestrutura, são empregados *switches* industriais, roteadores e *gateways* para integrar dispositivos e sistemas de supervisão. Essa integração permite análises em tempo real dos dados de produção, contribuindo para a eficiência operacional e tomada de decisões informadas.

As redes *Wireless* são sistemas que possibilitam a comunicação sem fio entre dispositivos, incluindo ambientes industriais (ALVES; SILVA, 2003). Adaptadas para locais desafiadores, essas redes oferecem flexibilidade na conectividade e transmissão de dados. Em ambientes industriais, são empregadas para controle de processo e lógica, podem transmitir dados em diversas unidades, como bits, bytes, palavras ou blocos, dependendo da configuração específica e dos protocolos utilizados. Dispositivos como roteadores garantem a integridade e segurança da comunicação. Essa tecnologia viabiliza a coleta e análise de informações em tempo real, facilitando a tomada de decisões e otimização dos sistemas industriais.

Um estudo conduzido pela *HMS Networks* (empresa internacional na área de tecnologia de informação e comunicação industrial) em 2023 (CARLSSON, 2023), apresenta resultados significativos em relação à prevalência e adoção das principais tecnologias de redes industriais, conforme mostrado na Figura 4.

Figura 4 – Uso das redes industriais em 2023.



Fonte: Adaptado de Carlsson (2023).

Notavelmente, entre as três categorias mencionadas, a rede *Ethernet* industrial

emergiu como a mais amplamente utilizada no cenário industrial. A predominância da *Ethernet* industrial pode ser atribuída às suas características vantajosas, tais como alta velocidade de transmissão de dados, baixa latência e capacidade de suportar uma variedade de protocolos de comunicação (GALLOWAY; HANCKE, 2012).

Além disso, a adaptabilidade dessa tecnologia a uma ampla gama de aplicações industriais, desde controle de processos até comunicação em níveis superiores da pirâmide de automação, contribui para sua proeminência no cenário atual. Dessa forma, à medida que a *Ethernet* industrial se torna a líder de mercado, torna-se ainda mais importante direcionar a atenção para o gerenciamento de falhas nessa tecnologia, dada sua predominância e relevância no contexto industrial. O foco nesse aspecto é importante para garantir a robustez e a confiabilidade das redes e dos sistemas de automação, sustentando a posição proeminente que a *Ethernet* industrial ocupa no ambiente de automação industrial.

2.2.2 Arquitetura

A arquitetura das redes industriais é vital para a eficácia e segurança operacional, especialmente à medida que expandem. A escolha correta entre as arquiteturas, seja estrela, barramento, árvore, anel ou malha, depende dos requisitos específicos de cada aplicação. Cada uma apresenta suas particularidades, vantagens e desafios, desde a facilidade de instalação até a confiabilidade e a capacidade de identificação e solução de problemas. Assim, a seleção de uma arquitetura apropriada é crucial para o sucesso e a sustentabilidade das operações industriais.

A arquitetura das redes industriais desempenha um papel fundamental na eficiência e confiabilidade das operações industriais. À medida que as redes se expandem para abranger mais dispositivos e sistemas, surge a necessidade de uma estrutura que suporte o crescimento. Para enfrentar esses desafios, surgem as arquiteturas das redes industriais.

À medida que as redes se expandem, a conexão ponto a ponto torna-se problemática. Embora acessível e simples, a conexão entre dois dispositivos com um cabo torna-se insustentável à medida que a rede se desenvolve com o tempo (ZOROTEO et al., 2018).

A arquitetura estrela possui todos os componentes conectados a um ponto central, como um *switch*, por meio de conexões ponto a ponto (ZOROTEO et al., 2018). Esta configuração possui fácil instalação, manutenção e rápida identificação de problemas de conexão são alguns dos benefícios da arquitetura estrela. No entanto, a redundância é menos confiável nesta estrutura devido à possibilidade de falha no ponto central que pode comprometer toda a rede.

Dispositivos conectados na arquitetura do barramento, com o uso de conectores "T", formam um longo cabo funcionando como um barramento, dai o nome da arquitetura de barramento, conforme (CAVALLIN, 2016). O sinal viaja nos dois sentidos, no entanto, a integridade do sinal depende do número de conexões e da distância, portanto, limitada.

A consequência de conexões com falha é generalizada, pois a detecção é complexa e afeta todos os dispositivos conectados.

A arquitetura de árvore possui apenas um caminho para chegar a um nó, esta arquitetura é combinação da arquitetura de barramento e estrela. Essa estrutura evita problemas de roteamento, mas pode resultar no cancelamento da conexão ao longo do caminho se houver problemas de rede. Conforme relatado por Mondadori (2016), a conexão pode ser interrompida se houver uma falha em qualquer parte da rede.

A arquitetura em anel é um tipo de rede comumente usado com sua topologia circular permitindo a comunicação direta entre dispositivos adjacentes (CAVALLIN, 2016). É apreciado por sua confiabilidade e redundância, pois se um dispositivo falhar, a comunicação pode ser redirecionada por outro dispositivo. No entanto, diz-se que essa configuração pode ser um desafio para gerenciar e configurar.

A rede em malha oferece uma solução de conectividade em que cada dispositivo está interconectado com todos os outros dispositivos na rede. Conforme apontado por Mondadori (2016), essa arquitetura é amplamente utilizada em redes de grande escala, sistemas de comunicações críticas e em aplicações onde a alta disponibilidade e a confiabilidade são essenciais, garantindo a continuidade das operações mesmo em cenários adversos.

A aplicação determinará a escolha ideal da arquitetura, considerando os fatores ambientais industriais e as necessidades de desempenho, confiabilidade e segurança. Toda arquitetura possui vantagens e desvantagens, portanto a escolha deve ser realizada com atenção conforme as necessidades e requisitos específicos da aplicação.

2.2.3 Protocolos de comunicação

Dentre os diversos protocolos de comunicação disponíveis no mercado, alguns dos mais utilizados para automação são o *Profibus*, *Profinet*, *DeviceNet* e *EtherNet*/IP.

A *Profibus* é uma rede de comunicação de dados digitais desenvolvida pela Siemens em 1987, utilizada para a conexão de dispositivos em uma ampla variedade de aplicações industriais (MONDADORI, 2016). Essa rede é baseada em um barramento serial que suporta velocidades de transmissão de até 12 Mbps e opera na camada física e de enlace de dados do modelo Interconexão de Sistemas Abertos (OSI, do inglês *Open System Interconnection*). Segundo Cavallin (2016), a rede *Profibus* é comumente utilizada em aplicações de automação industrial, como controle de processos, monitoramento de máquinas e dispositivos, e sistemas de energia.

A *Profinet* é uma rede de comunicação de dados industriais baseada na tecnologia *Ethernet*, desenvolvida pela Siemens em 1999 (LUGLI; SANTOS, 2014). Essa rede consegue transmitir dados com altas taxas de transferência, suportando velocidades de transmissão de até 100 Mbps. A *Profinet* utiliza a camada de aplicação do modelo OSI e é amplamente utilizada em aplicações de automação industrial, incluindo controle de pro-

cessos, monitoramento de máquinas, sistemas de energia, entre outros (MONDADORI, 2016).

A *DeviceNet* é uma rede de comunicação de dados industriais desenvolvida pela Rockwell Automation em 1994 (MONDADORI, 2016). A velocidade de transmissão no protocolo *DeviceNet* é uma característica variável. As taxas usuais de transmissão para redes que adotam o *DeviceNet* são de 125 kbps a 500 kbps. No entanto, é importante observar que essas taxas podem variar em função de diversos fatores, como a configuração específica da rede e a natureza dos dispositivos utilizados. Essa rede é utilizada para conectar dispositivos eletrônicos em uma ampla variedade de aplicações industriais e opera na camada física e de enlace de dados do modelo OSI. De acordo com Cavallin (2016), a *DeviceNet* utiliza a Rede de Área de Controle (CAN, do inglês *Control Area Network*) para a transmissão de dados e é comumente utilizada em aplicações de automação industrial, como controle de processos, monitoramento de máquinas e dispositivos, e sistemas de energia.

A *EtherNet/IP* é uma rede de comunicação de dados industriais desenvolvida pela Rockwell Automation em 2001, baseada na tecnologia *Ethernet* (LUGLI; SANTOS, 2014). Essa rede possui altas taxas de transferência de dados e suporta velocidades de transmissão de até 100 Mbps. Segundo Mondadori (2016), a *EtherNet/IP* utiliza a camada de aplicação do modelo OSI e é amplamente utilizada em aplicações de automação industrial, incluindo controle de processos, monitoramento de máquinas, sistemas de energia, entre outros.

Cada uma dessas redes possui suas características, vantagens e desvantagens, e é importante escolher a mais adequada para cada aplicação, considerando a velocidade de transmissão necessária, o tamanho da rede, a complexidade da aplicação, entre outros fatores. Além disso, a implementação dessas redes requer um planejamento cuidadoso, envolvendo a escolha dos dispositivos de comunicação adequados, a definição da topologia da rede, a configuração dos dispositivos, entre outros aspectos que devem ser considerados para garantir a eficiência e a segurança da rede industrial.

2.2.3.1 Protocolo SNMP

O Protocolo Protocolo Simples de Gerenciamento de Redes (SNMP, do inglês *Simple Network Management Protocol*) encontra também ampla aplicação nas redes *Ethernet* industrial, embora seus objetivos nesse contexto sejam ligeiramente distintos dos protocolos apresentados anteriormente. O SNMP é uma estrutura padrão de comunicação utilizada para o gerenciamento de dispositivos em redes IP (BRANQUINHO et al., 2014). Originalmente concebido como uma forma de monitorar e gerenciar dispositivos de rede, o SNMP tornou-se uma ferramenta para administradores de rede e profissionais de TI e TA, permitindo o monitoramento remoto e a configuração de dispositivos em uma infraestrutura de rede.

A versatilidade e eficácia do SNMP são evidenciadas por sua ampla adoção em

diversos setores e aplicações. Um exemplo notável de uso do SNMP é em ambientes de *data center*. Nesses cenários, o protocolo é frequentemente empregado para monitorar a saúde e o desempenho de servidores, *switches*, roteadores e outros dispositivos críticos (FONSECA et al., 2013). Por meio de consultas SNMP, é possível obter informações relevantes, como utilização de largura de banda, temperatura, *status* da energia e outros parâmetros operacionais (STALLINGS, 1993). Essa capacidade de monitoramento em tempo real permite uma resposta rápida a qualquer anomalia ou problema potencial, otimizando assim a disponibilidade e a eficiência operacional dos dispositivos.

Além disso, o SNMP também desempenha um papel relevante em ambientes industriais, como o setor siderúrgico mencionado anteriormente (FONSECA, 2004). Em instalações industriais complexas, o protocolo é utilizado para monitoramento da rede industrial, podendo monitorar o desempenho desde equipamentos de produção até sistemas de automação. Através do SNMP, os engenheiros e operadores podem obter visões detalhados sobre o desempenho de máquinas, condições ambientais e integridade de sistemas, facilitando a manutenção preventiva, a otimização da produção e a redução de tempos de inatividade não planejados (GELLE; KOCH; SAGER, 2005).

Além disso, é notável ressaltar o papel que o SNMP desempenha na integração com PLC em ambientes industriais. O PLC, frequentemente empregado para automação e controle de processos industriais, beneficia-se da capacidade do SNMP de fornecer uma interface padronizada para monitoramento e gerenciamento (LEE et al.,). Por meio dessa integração, é possível obter dados cruciais sobre o *status* operacional do PLC, permitindo uma supervisão das operações industriais. Essa aplicação específica do SNMP contribui significativamente para a eficiência operacional e a manutenção proativa, aspectos importantes em ambientes industriais dinâmicos e complexos (OLIVEIRA et al., 2009).

2.3 *Zabbix*

Nesta seção, serão abordados tópicos básicos para entender o *Zabbix*, uma ferramenta de monitoramento de redes. Aspectos relevantes da ferramenta, desde sua arquitetura até capacidades e recursos, serão apresentados para fornecer uma perspectiva geral da plataforma. É importante ressaltar que o conhecimento desses tópicos é fundamental para o entendimento da implementação do *Zabbix* no monitoramento das redes industriais.

2.3.1 Conceitos

Para entender melhor como funciona o *Zabbix*, é importante compreender os conceitos e os termos usados na plataforma. Alguns dos conceitos importantes incluem *hosts*, agentes, itens, *triggers*, gráficos, telas e mapas. Compreender esses conceitos é fundamental para entender como o *Zabbix* coleta e analisa dados de monitoramento para fornecer informações valiosas sobre a rede, servidores e serviços.

- *Hosts*: são dispositivos monitorados pelo *Zabbix*. Podem ser servidores, roteadores, *switches*, impressoras, entre outros. Cada *host* monitorado pelo *Zabbix* deve ter um nome único e um endereço IP válido;
- Grupo de *host*: é um conjunto de *hosts* com características semelhantes, como sistema operacional, função ou localização geográfica. Agrupar *hosts* em grupos pode auxiliar na organização e gerenciamento dos dispositivos monitorados;
- Itens: são valores monitorados em um *host* pelo *Zabbix*. Eles podem incluir a utilização da CPU, uso de memória, *status* de um serviço, entre outros. O *Zabbix* coleta e armazena esses valores para poderem ser exibidos em gráficos ou acionar os *triggers*;
- *Templates*: são modelos de configuração que podem ser aplicados a um ou mais *hosts*. Eles definem quais itens, *triggers* e gráficos serão monitorados em um *host*. *Templates* também podem ser usados para definir configurações padrão, facilitando a configuração de *hosts* em massa;
- *Triggers*: são regras que monitoram valores dos itens e definem quando um alerta deve ser acionado. Uma *trigger* pode ser criada para monitorar um valor específico de um item em um *host*, por exemplo, quando a utilização da CPU excede um determinado valor.
- Ação: É um conjunto de operações executadas pelo *Zabbix* em resposta a um evento/*triggers*. As ações podem ser configuradas para enviar notificações, executar *scripts*, atualizar itens, entre outras possibilidades;
- *Script*: código executável que realiza uma determinada ação em um *host* monitorado pelo *Zabbix*. Esses *scripts* podem ser utilizados para coletar informações específicas que não estão disponíveis por padrão no *Zabbix*, ou para automatizar ações de correção de problemas, como reiniciar um serviço ou executar uma limpeza de disco;
- Descoberta: é um processo automatizado que permite ao *Zabbix* detectar automaticamente dispositivos e serviços em uma rede, sem a necessidade de configurar cada *host* manualmente. É possível configurar a descoberta de *hosts*, redes, interfaces de rede, volumes de disco, entre outros;
- *Dashboard*: É uma página personalizada que exibe gráficos, tabelas, mapas e outros elementos visuais com informações sobre o desempenho dos sistemas monitorados pelo *Zabbix*. É uma forma de apresentar informações importantes de maneira visual e fácil de entender.

2.3.2 Arquitetura

A arquitetura do *Zabbix* é uma solução de monitoramento distribuída, que oferece recursos de monitoramento em um único pacote integrado. O *Zabbix* monitora vários parâmetros da rede, dos *hosts* e da saúde dos serviços, e utiliza um mecanismo flexível de notificação que permite configurar alerta por e-mail para praticamente qualquer evento (ZABBIX, 2014). De acordo com Lima (2014), o *software* suporta tanto *pooling* (servidor solicita a informação aos dispositivos de rede) quanto *trapping* (dispositivos enviam informações ao servidor a partir de um determinado gatilho) e oferece uma interface *web* que permite avaliar o estado da rede e da saúde dos *hosts* de qualquer local.

Dividido em quatro camadas, o *Zabbix* é uma plataforma de monitoramento de rede que consegue coletar, visualizar e analisar dados em tempo real de várias fontes. O fluxo na arquitetura do *Zabbix* começa no *back-end*, onde os dados de monitoramento são coletados, processados e armazenados em um banco de dados. Em seguida, a API possibilita a integração com outras aplicações e permite que os usuários acessem os dados e configurem o sistema (VALENTE, 2023). O *front-end* fornece a interface de usuário para configurar *hosts*, visualizar gráficos, tabelas e relatórios, além de receber alerta quando eventos críticos ocorrem. Os usuários interagem com o *front-end* para monitorar e gerenciar seus sistemas e redes, enquanto o *back-end* lida com a coleta contínua de dados e a geração de alerta para manter a infraestrutura sob controle.

2.3.3 Componentes do *Zabbix*

O componente central do *Zabbix* é o *Zabbix Server*. Ele gerencia toda a configuração do sistema de monitoramento, solicita a coleta de dados, armazena todo o histórico do banco de dados e executa lógicas de alerta quando identificado um gatilho/*trigger* (ZABBIX, 2014). O *Zabbix Server* também pode ser configurado para executar ações automaticamente em resposta a problemas de monitoramento (TOSTES, 2022).

A aquisição de dados de redes externas é o trabalho do *Zabbix Proxy*. Ele funciona como um mediador entre o servidor *Zabbix* e os *hosts* remotos. O *Proxy* é responsável por coletar dados das redes externas, retransmitidos de volta ao servidor para processamento posterior (LIMA, 2014).

O *Zabbix Agent* é responsável pela coleta de dados de *hosts* específicos, como máquinas com *Linux*, *UNIX* e *Windows*, reportando ao *Zabbix Server* ou *Zabbix Proxy*, entregando os dados coletados (VALENTE, 2023). Para ser possível de se realizar o monitoramento o agente precisa ser instalado no *host* desejado, com isso é possível coletar informações como uso de CPU, uso de memória e uso de disco. As aquisições de dados do agente são classificadas como passivas (solicitada pelo *Server*/*Proxy* e retornada pelo agente) ou ativas (lista de itens a ser processado de forma independente em um determinado período). Existe uma lista padrão de chaves que é possível de se obter de um *host*

com o *Zabbix Agent*, como nome do *host*, verificação de disponibilidade do agente, versão do *Zabbix Agent*, entre outros, mas também é possível incrementar *scripts* personalizados para fornecer informações de monitoramento adicionais.

O *Zabbix Web*, ou interface *web* do *Zabbix*, é o componente responsável pela apresentação dos dados de monitoramento ao usuário. Ele fornece uma interface gráfica para exibir gráficos de tendências, visualizações de mapas de rede, alerta, execução de *scripts*, emissão de alerta, controle de usuários e muito mais. Para que essas informações sejam apresentadas, os usuários precisam inserir os *hosts* que desejam monitorar.

Uma solução de monitoramento é obtida através da utilização desses componentes. Essa solução é altamente versátil e facilmente escalável para atender aos requisitos de monitoramento de uma infinidade de redes.

2.3.4 Monitoramento com o *Zabbix*

Existem diversas componentes que podem ser monitorados com o *Zabbix* como, por exemplo, monitoramento de desempenho de rede (disponibilidade e tráfego de dispositivos de rede, como roteadores, *switches* e *firewalls*) (BRANQUINHO et al., 2014); monitoramento de servidores (análise de desempenho de servidores, como a utilização de CPU, memória e disco); monitoramento de máquinas virtuais; monitoramento de banco de dados; e monitoramento de *hosts*, através do *Zabbix Agent*, Interface de Gerenciamento de Plataforma Inteligente (IPMI, do inglês *Intelligent Platform Management Interface*) ou agente SNMP.

O *Zabbix Agent* é uma componente essencial na abordagem do *Zabbix* para o monitoramento, possibilitando a coleta de informações detalhadas diretamente dos *hosts* (LIMA, 2014). Com a instalação do *Zabbix Agent* nos sistemas que compõem a infraestrutura, os administradores podem acessar dados específicos de desempenho, como utilização de CPU, memória e disco, proporcionando um panorama mais granular e detalhada. Essa capacidade é particularmente valiosa para monitorar servidores (TADER, 2010). O *Zabbix Agent* reforça, assim, a flexibilidade da ferramenta para lidar com uma variedade de ativos e oferecer uma concepção do ambiente monitorado. Com essa funcionalidade adicional, o *Zabbix* destaca-se como uma solução versátil e adaptável para atender às complexidades das infraestruturas modernas.

O padrão de gerenciamento de *hardware* conhecido como IPMI permite que os administradores de sistema monitorem e manipulem servidores remotamente sem a necessidade de proximidade física (OLUPS, 2016). Para auxiliar na vigilância da rede, o *Zabbix* é uma solução que possui recursos de varredura IPMI que permitem aos administradores gerenciar e monitorar facilmente seus servidores à distância (OLUPS, 2016). Extremamente valiosas, as verificações do IPMI estão em cenários onde os servidores são difíceis ou impraticáveis de acessar, como em *data centers*. Usando verificações IPMI, o

Zabbix simplifica o gerenciamento remoto e o monitoramento de servidores, proporcionando maior eficiência.

O agente SNMP pode ser utilizado para monitorar equipamentos como impressoras, *switches*, roteadores, *nobreaks*, PLC, entres outros, desde que eles possuam o protocolo SNMP disponível. Para que isso aconteça é preciso inicialmente verificar se o SNMP está ativado no dispositivo desejado e em seguida descobrir a Identificador de Objeto (OID, do inglês *Object Identifier*) que se deseja monitorar, informação normalmente disponível na documentação do equipamento ou que pode ser obtida através do comando *snmpwalk* no *prompt* de comando da máquina que esta hospedando o *Zabbix*. O *Zabbix* é compatível com SNMP nas versões 1, 2 e 3, permitindo a configuração de parâmetros de segurança, como autenticação e criptografia de dados (TOSTES, 2022).

A variedade está no centro do arsenal de recursos da ferramenta de monitoramento *Zabbix*, um dos quais inclui a capacidade de configurar alerta com base em limites predefinidos (ZABBIX, 2014). Devido a esses alerta, os administradores podem detectar e solucionar problemas antes que se tornem árduos (LIMA, 2014). Exibindo gráficos e relatórios de dados em tempo real, o *Zabbix* consegue acompanhar o desempenho do equipamento através dos olhos de um administrador. Ademais, o *Zabbix* permite a criação de *triggers* e ações para notificar quando um problema é identificado, além da criação de gráficos e relatórios para análise do desempenho e histórico de monitoramento (TOSTES, 2022).

Para exemplificar alguns exemplos de ativos que podem ser monitorados com o *Zabbix*, podemos citar: servidores físicos e virtuais; roteadores e *switches*; *Firewalls*; PLC; computadores; bancos de dados, como *MySQL* e *Oracle*; serviços em nuvem, etc. Como é possível perceber, o *Zabbix* é uma ferramenta com muitas possibilidades, o que a torna capaz de atender às necessidades de monitoramento de uma diversidade de ativos e tipos de redes.

2.4 Considerações parciais

Neste capítulo foi apresentado o processo de produção da aciaria para proporcionar uma breve percepção sobre as complexidades envolvidas na indústria siderúrgica. A análise das redes industriais, sua classificação e arquitetura, foi realizada para destacar a importância do gerenciamento de falhas e para proporcionar uma compreensão mais aprofundada da rede utilizada na planta de estudo.

No âmbito dos protocolos de comunicação, o SNMP foi destacado como uma ferramenta para a obtenção de informações em dispositivos de rede. Essa discussão fornece a base para a compreensão de como as informações críticas são acessadas em ambientes industriais.

A introdução à ferramenta *Zabbix* ofereceu uma perspectiva da ferramenta de mo-

nitoramento, revelando sua classificação empresarial e capacidade de gerenciar uma ampla variedade de parâmetros relacionadas a redes e aplicativos. A exploração dos conceitos, arquitetura e componentes do sistema *Zabbix* estabelece a base teórica necessária para sua implementação prática.

3 Desenvolvimento

Este capítulo proporciona uma análise sobre a infraestrutura, implementação e desafios enfrentados durante a integração do sistema de monitoramento *Zabbix* na planta de produção da aciaria em estudo. Detalhes sobre a descrição das redes industriais, ativos utilizados no processo, implementação da ferramenta e seus parâmetros de monitoramento são abordados. Além disso, a análise dos custos associados e os desafios enfrentados, como a ausência de acesso à internet e a complexidade na configuração inicial do *Zabbix*, são discutidos. O capítulo conclui enfocando as medidas de segurança adotadas para resguardar a integridade e confidencialidade dos dados críticos. Este panorama do desenvolvimento fornece uma base sólida para a compreensão da implementação do sistema de monitoramento na aciaria, destacando seu impacto e eficácia no contexto industrial.

3.1 Descrição da rede industrial estudada

A planta da aciaria em estudo apresenta uma infraestrutura de rede industrialmente segmentada, composta por três redes distintas: redes A, B e C, conforme apresentado na Figura 5. Essa segmentação é fundamental para garantir a eficiência e a integridade das operações em áreas específicas da aciaria, cada uma com suas características e protocolos de comunicação próprios.

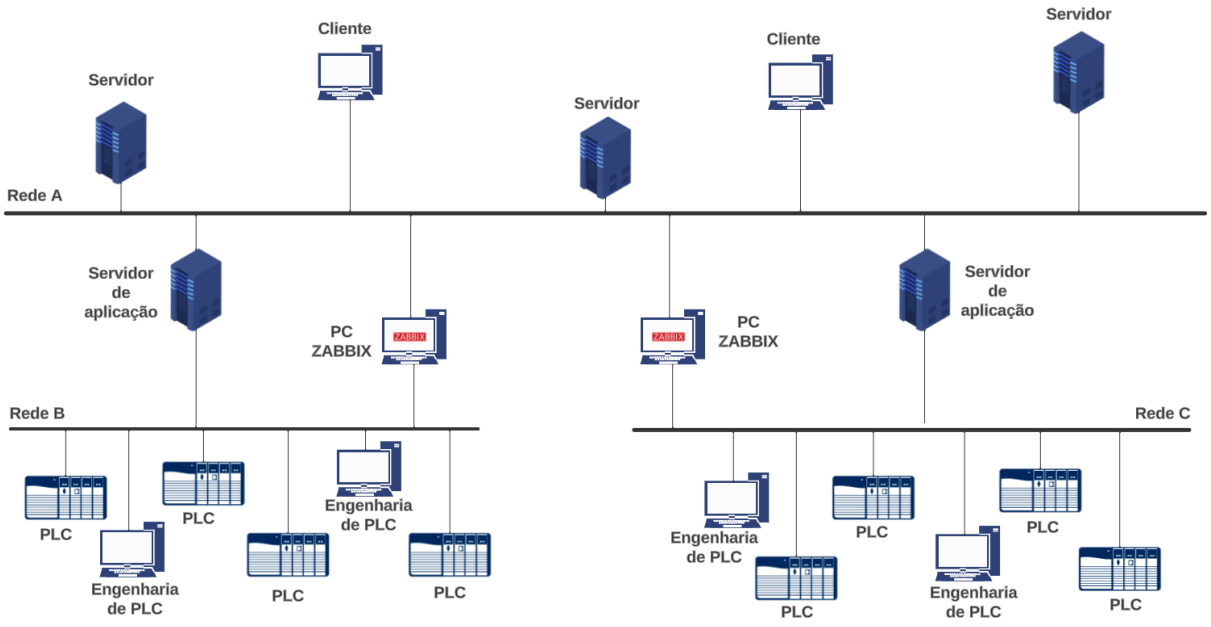
A primeira área da aciaria, o LD, está associada à rede B. Nessa rede, é utilizado o protocolo *Ethernet/IP*, uma extensão do padrão *Ethernet Industrial* comumente empregado em ambientes industriais para comunicação em tempo real. A rede B interconecta diversos dispositivos, como PLC, IHM e estações de trabalho, possibilitando a coordenação e o controle das operações relacionadas ao LD.

A segunda área, a MLC, possui sua rede de controle designada como rede C. Nesse contexto, o protocolo *Profinet* é adotado para a comunicação entre os diversos componentes, proporcionando uma infraestrutura adequada para as necessidades específicas dessa área. O *Profinet* é amplamente utilizado em ambientes industriais para comunicação em tempo real, sendo especialmente projetado para integração de sistemas de automação e controle.

É válido destacar que as redes B e C operam isoladamente uma da outra, conforme representado na Figura 5, contribuindo para a segurança e a estabilidade do ambiente industrial. Essa segregação impede interferências e possíveis conflitos entre as áreas, garantindo que cada parte da aciaria mantenha seu desempenho sem comprometer a operação da outra.

Além dessas redes específicas para controle industrial, a planta da aciaria incorpora a rede A, destinada à conexão dos equipamentos ligados ao sistema de supervisão. Essa

Figura 5 – Rede da aciaria da planta estudada.



Fonte: Autoria própria.

rede abrange todo o processo da aciaria, proporcionando pontos de acesso tanto na área do LD quanto na MLC.

Entre as três redes, tem-se dois servidores de aplicação, responsáveis por fazer a leitura dos dados do PLC e repassar informações ao sistema supervisório, que se encontra conectado à rede A; e 2 computadores para aplicação do *Zabbix*, ou seja, os servidores de monitoramento.

3.1.1 Ativos utilizados no processo e suas falhas

A etapa de supervisão da aciaria da planta de estudo é um componente fundamental para garantir o funcionamento dos sistemas de automação. Isso inclui onze servidores e vinte e dois computadores, que compõem essa infraestrutura. Esses sistemas são projetados para operar e supervisionar uma variedade de aplicativos, incluindo os sistemas SCADA, Sistemas de Gerenciamento de Informações da Planta (PIMS, do inglês *Plant Information Management Systems*), *IBA-Analyzer*, *Zabbix* e um *software* interno de automação desenvolvido especificamente para armazenar dados relativos ao processo de produção da planta.

O nível de controle é igualmente crítico, uma vez que lida diretamente com o controle das operações. Nesse nível, encontram-se trinta e quatro PLCs, dez módulos remotos adicionais e dezesseis computadores, todos desempenhando funções de controle do processo. Isso inclui o controle dos dois fornos LD, dos seis veios da máquina de lingotamento contínuo, dos carros de aço e de outros sistemas operacionais.

Além dos ativos de controle e supervisão, o uso dos *switches* é essencial no sis-

tema de automação, uma vez que esses dispositivos são responsáveis pela interconexão e comunicação entre todos os componentes. A planta em análise está equipada com treze *switches*, responsáveis por permitir a interligação de todos os dispositivos.

Falhas nas redes de supervisão e nos ativos que a compõem, sofrem por vezes de problemas de *hardware*, como elevado consumo de CPU, disco e memória; aumento da temperatura; e falhas de comunicação, que podem levar a interrupções nas operações de supervisão. A indisponibilidade de servidores, a falha de *hardware* ou problemas na transmissão dos dados, pode impactar negativamente a capacidade de coleta e análise de dados do processo em tempo real, afetando a tomada de decisões informadas.

No que diz respeito à rede de controle e aos ativos a ela conectados, como PLC e módulos remotos, as falhas mais comuns envolvem problemas de comunicação e falhas de *hardware*, como sobrecarga de processamento e altas temperaturas. Falhas em PLC podem resultar em uma perda de controle crítico sobre o processo de produção, levando a desvios nos parâmetros e, potencialmente, à necessidade de paradas de emergência. Da mesma forma, falhas nos módulos remotos podem prejudicar a capacidade de controlar componentes específicos do processo, o que pode impactar diretamente na disponibilidade dos equipamentos e na segurança do ambiente de trabalho.

Os *switches* também estão suscetíveis a falhas comuns que podem ter um impacto significativo nas operações. Entre as falhas mais frequentes, destacam-se problemas de *hardware*, como elevado consumo de CPU, defeito em suas portas e congestionamento do tráfego de rede.

A CPU dos *switches* tem duas funções principais, executar processos do Sistema Operacional Interligado (IOS, do inglês *Internetwork Operating System*) para operar como um *switch* de rede e enviar/receber pacotes do *hardware* de comutação. A CPU realiza essas funções simultaneamente, mas pode ficar sobrecarregada se um processo IOS consumir muito tempo ou se houver muitos pacotes do *hardware* de comutação. A alta utilização da CPU pode resultar em processos IOS não conseguindo acesso ao recurso da CPU. A utilização normal da CPU varia de 5 a 40% em *switches* não empilháveis e é ligeiramente maior em *switches* empilhados. De acordo com Cisco (Acesso em 27/02/2024), o valor ideal é que este consumo seja inferior a 50% para que sua capacidade de responder a eventos na rede não seja prejudicada.

Essas falhas podem resultar em interrupções na comunicação entre os ativos de controle e supervisão, levando a atrasos na detecção de falhas e comprometendo a eficiência operacional. Portanto, uma gestão eficaz que inclui estratégias de manutenção preventiva, como o *Zabbix*, é fundamental para mitigar e contribuir na identificação das falhas em ativos de supervisão e controle. Compreender e notificar essas falhas com agilidade é vital para garantir a confiabilidade das redes de automação, que desempenham um papel essencial no funcionamento do processo de produção.

3.2 Implementação da ferramenta

Inicialmente, é necessário providenciar os computadores de monitoramento para realizar a instalação e configuração do *Zabbix*. Isso inclui a seleção de computadores adequados, que pode ser verificado no site do *Zabbix* conforme o número de itens coletados, e a instalação do *software Zabbix*. Para a planta de estudo serão menos de 1000 dados coletados para cada servidor *Zabbix*. Para este caso, Zabbix (2014) orienta computadores com duas CPU e 8 GB, que representa a configuração mínima para implementação da ferramenta.

Uma vez que o *hardware* esteja pronto, a próxima etapa envolve realizar uma avaliação dos ativos de controle e supervisão, bem como dos *switches* na infraestrutura da aciaria. Isso inclui a identificação de equipamentos, a verificação da compatibilidade com o *Zabbix* e a seleção de dispositivos que requerem monitoramento. Em seguida, é necessário realizar a instalação e ativação dos agentes em servidores, PLC, clientes e computadores que serão monitorados, garantindo que eles estejam prontos para enviar os dados coletados.

A configuração do *Zabbix* também requer a definição de parâmetros de monitoramento, a criação de *triggers* para a detecção de falhas e a configuração de painéis de controle para visualização de dados em tempo real.

É importante notar que a implementação de um sistema de monitoramento, como o proposto, é um processo contínuo e dinâmico, que requer uma abordagem estruturada e acompanhamento constante para garantir sua eficácia e eficiência na detecção de falhas e na otimização das operações na indústria siderúrgica.

3.2.1 Instalação do *Zabbix*

A instalação do *Zabbix* para o monitoramento dos sistemas nas áreas do LD e MLC envolve a preparação de dois computadores dedicados, cada um destinado a monitorar um lado específico do processo industrial. Os computadores são equipados com o sistema operacional *Windows 10 Pro*, discos de 1 *terabyte*, 8 GB de RAM e quatro núcleos Intel(R) Core(TM) i5-7500 3,40 GHz, proporcionando uma configuração robusta para suportar as demandas da planta e pensando na necessidade futura de novos monitoramentos.

Optando por uma abordagem de virtualização, pelo fato da ferramenta não poder ser instalada diretamente no sistema operacional *Windows*, utiliza-se a ferramenta gratuita *VirtualBox* para criar Máquinas Virtuais (do inglês, *Virtual Machines*) dedicadas ao *Zabbix*. Para o sistema operacional das VMs, opta-se pelo *Debian* versão 12. Vale ressaltar que o *Debian* é utilizado apenas nas VMs de monitoramento, todos os outros PCs constituídos na rede possuem sistema operacional *Windows*.

Quanto à versão do *Zabbix Server*, optou-se pela versão 6.0. O banco de dados *MySQL* foi escolhido para armazenar os dados do *Zabbix*, considerando a familiaridade

da equipe de automação com essa tecnologia.

O *Zabbix Agent*, ferramenta de monitoramento em dispositivos com sistema operacional, deve apresentar a mesma versão do *Zabbix Server*, para que seja possível a comunicação entre eles. O processo de instalação do *Zabbix Server* e *Zabbix Agent* é apresentado por Zabbix (2014), e o procedimento de instalação das VMs é demonstrado por Lima (2014). É importante destacar que a instalação do agente deve ser feita manualmente. Até o momento, não há métodos disponíveis para uma instalação em lote e automática.

O serviço *web Apache* foi selecionado como o servidor *web* para o *Zabbix*. Essa escolha visa garantir uma interface *web* eficiente e segura para o monitoramento, facilitando a navegação e a gestão das informações geradas pela ferramenta.

3.2.2 Definição dos grupos de *hosts* monitorados

A definição dos grupos de *hosts* desempenha um papel importante na organização e no gerenciamento de falhas de um sistema de monitoramento como o *Zabbix*. Ao agrupar os *hosts* em categorias específicas, é possível obter uma perspectiva mais clara e estruturada do ambiente monitorado. No contexto deste estudo, como o objetivo é monitorar os ativos da rede *Ethernet industrial* dos níveis de supervisão e controle, dispositivos nos quais não possuíam uma forma de monitoramento na planta de estudo, optou-se por separar os *hosts* em quatro grupos principais: PLC, servidores, *switches* e os PCs.

Os grupos são estruturados da seguinte forma: o grupo de PLC será composto por PLC e remotas, dos fabricantes *Siemens* e *Rockwell*; o grupo de servidores será composto pelos servidores da rede de supervisão e os servidores de gerenciamento de planta, como PIMS e o Sistemas de Execução de Manufatura (MES, do inglês *Manufacturing Execution Systems*); o grupo de *switches* será composto por todos os *switches* utilizados nesta rede, que, na planta em questão, são dos fabricantes *Cisco* e *3COM*; e por último, o grupo de computadores, será composto pelos computadores de engenharia de PLC, *clients* do SCADA e computadores de acompanhamento de processo, sendo compostos pelos sistemas operacionais *Windows XP*, *Windows 7* e *Windows 10*.

Esta separação dos *hosts* em grupos ofereceram benefícios importantes, tais como:

- **gerenciamento simplificado:** possibilita o agrupamento dos *hosts* com características semelhantes, facilita a aplicação de configurações em massa, como *templates*, itens, ações e *triggers*, para todos os *hosts* do grupo;

- **monitoramento específico:** cada grupo de *hosts* terá requisitos de monitoramento exclusivos. Por exemplo, o PLC irá exigir monitoramento de parâmetros e *status* de dispositivos específicos, enquanto os servidores irão requerer parâmetros de desempenho, como uso de CPU e memória. Separar os *hosts* em grupos permitirá configurar itens, *triggers* e gráficos de forma personalizada, conforme as necessidades específicas de cada grupo;

- **controle de acesso às informações:** através da separação dos grupos é possível definir permissões distintas para cada usuários e equipes, determinando quais dados e recursos de monitoramento cada um terá acesso. Um exemplo prático dessa aplicação é a separação dos alertas por grupos. Na planta de estudo em questão, o profissional responsável pela manutenção do PLC difere daquele encarregado dos servidores. Essa abordagem permite uma segmentação adequada das informações, garantindo que cada usuário ou equipe tenha acesso apenas aos dados relevantes para suas responsabilidades;

- **visualização simplificada dos dados:** dividir os *hosts* em grupos, a interface do *Zabbix* pode fornecer uma visualização hierárquica do ambiente monitorado. Isso facilita a navegação e a identificação rápida de *hosts* específicos dentro de cada grupo, proporcionando uma compreensão mais clara da topologia da rede e dos componentes envolvidos.

3.2.3 Definição dos parâmetros de monitoramento

Os parâmetros servem como indicadores que avaliam o desempenho, a disponibilidade e a integridade dos componentes e processos que estão sendo monitorados. Ao identificar esses parâmetros relevantes para o sistema específico que está sendo monitorado, é importante considerar as necessidades e os objetivos do sistema.

Como mencionado anteriormente, a separação dos equipamentos em grupos é importante, por facilitar o monitoramento, visto que todos os integrantes possuirão a necessidade das mesmas informações. Considerando os objetivos deste trabalho e a necessidade da equipe de trabalho, são apresentados na sequência os parâmetros que se deseja monitorar para os respectivos grupos de *hosts*.

- **Servidores**: *status* do dispositivo, uso da CPU, uso do disco, uso da memória, tráfego de rede, temperatura;

- **PLC**: *status* do dispositivo, trafego de rede, temperatura do dispositivo, diagnóstico de erros do PLC;

- **PCs**: *status* do dispositivo, uso da CPU, uso da memória, uso do disco, tráfego de rede, temperatura;

- ***Switches***: *status* do dispositivo, uso da CPU, uso da memória, tráfego de rede, temperatura.

A monitoração de itens como status do dispositivo, uso da CPU, disco, memória, tráfego de rede, temperatura, entre outros, é fundamental para manter os grupos de hosts operando de maneira otimizada e segura. Verificar o status do dispositivo ajuda a assegurar que todos estão funcionando e acessíveis. Monitorar o uso da CPU e da memória

pode prevenir sobrecargas que afetam o desempenho. Acompanhar o uso do disco e o tráfego de rede é crucial para evitar congestionamentos e falhas na transmissão de dados. A temperatura é monitorada para prevenir superaquecimento, que pode danificar fisicamente os dispositivos. Os parâmetros para cada um desses itens são definidos com base nas especificações técnicas fornecidas pelos fabricantes, assegurando que os dispositivos operem dentro de limites seguros e eficientes.

3.2.4 Acesso às informações

No contexto da implementação do *Zabbix* na infraestrutura de controle e supervisão da aciaria, o acesso ao banco de dados é uma parte fundamental do processo de monitoramento. A equipe de manutenção poderá monitorar as informações por meio de um sistema *web* seguro de *login* e senha, que garante a autenticação e a proteção dos dados.

O objetivo principal desta ferramenta é configurar as coletas de dados e o armazenamento de informações conforme as necessidades específicas do ambiente. Isso é feito para evitar sobrecarregar o banco de dados com informações irrelevantes ou redundantes.

Além disso, está prevista a realização de *backups* semanais do banco de dados. Essa medida é significativa para garantir a integridade e a disponibilidade dos dados em caso de perda ou corrupção. Os *backups* semanais servem como uma camada adicional de segurança e recuperação de informações, oferecendo tranquilidade à equipe de manutenção em relação à confiabilidade do sistema.

3.3 Considerações parciais

Neste capítulo, são abordados informações referentes à infraestrutura, implementação e desafios encontrados durante a integração do sistema de monitoramento *Zabbix* na planta de produção da aciaria em estudo. A análise minuciosa das redes industriais, a descrição dos ativos utilizados, a implementação da ferramenta e os parâmetros de monitoramento estabelecerão uma base sólida para compreender a complexidade desse processo.

A descrição da segmentação da rede industrial em três redes distintas (A, B e C) e a análise das áreas associadas a essas redes (LD e MLC) proporcionaram informações importantes sobre a topologia da aciaria. A necessidade de uma abordagem especializada para monitoramento e gestão foi evidenciada, justificando a escolha do *Zabbix* devido à sua versatilidade e capacidade de integração com diferentes protocolos.

A análise dos ativos utilizados no processo, desde servidores e PLC até *switches*, destacou a importância de um monitoramento para garantir o funcionamento contínuo dos sistemas de automação. Os parâmetros definidas para cada grupo de *hosts* proporcionam uma visão detalhada, permitindo uma gestão mais precisa.

A implementação do *Zabbix*, desde a escolha do *hardware* até a configuração do sistema, foi amplamente discutida. A virtualização das VMs, a escolha do sistema operacional *Debian* e a definição dos grupos de *hosts* monitorados são destacados como componentes cruciais do processo.

O acesso às informações monitoradas por meio de uma interface *web* segura foi apresentado como um elemento essencial. A proteção dos dados, juntamente com a segmentação adequada do acesso, assegura que apenas usuários autorizados tenham visibilidade sobre as informações relevantes.

Por fim, a consideração sobre a realização de *backups* semanais do banco de dados ressalta a importância da segurança e recuperação de dados. Essa prática oferece uma camada de proteção adicional, reforçando a confiabilidade do sistema.

4 Resultados

Este capítulo apresenta uma análise aprofundada do desempenho do sistema após a implementação do monitoramento com o uso do *software Zabbix* na planta de produção da aciaria. São destacados exemplos de melhorias observadas no ambiente, fornecendo uma ideia sobre como a ferramenta contribui para a eficiência operacional, o gerenciamento proativo e reativo de falhas e a segurança da infraestrutura de automação industrial. Além disso, são abordados os custos associados à implementação da ferramenta, os desafios enfrentados durante o processo e as medidas de segurança implementadas para auxiliar na integridade e confidencialidade dos dados críticos.

4.1 Ativos monitorados

A implementação do sistema de monitoramento *Zabbix*, na infraestrutura da aciaria resulta no monitoramento de diversos ativos, proporcionando maior visibilidade sobre o ambiente de automação. A Tabela 1 resume a distribuição de ativos monitorados e não monitorados, destacando a abrangência do sistema implementado.

Tabela 1 – Ativos monitorados e não monitorados utilizando o *Zabbix*.

	Ativos monitorados	**Ativos não monitorados**
PCs	38	0
Servidores	11	0
Switches	13	0
PLCs	40	4
Total	102	4

Fonte: Autoria pória.

Conforme apresentado na Tabela 1, o sistema de monitoramento *Zabbix* abrange o gerenciamento de desempenho dos computadores, *switches*, servidores e PLCs na infraestrutura da aciaria, totalizando 102 ativos monitorados. Quatro PLCs não foram incluídos no escopo de monitoramento devido à falta de suporte ao protocolo SNMP. Esses PLCs, por serem de modelos mais antigos, não oferecem recursos adequados para o gerenciamento por meio do *Zabbix*.

Nesse caso, seria necessário substituir esses PLCs por modelos mais recentes e compatíveis com o sistema de monitoramento implementado. Essa iniciativa visa não apenas ampliar a abrangência do monitoramento, mas também garantir a continuidade da operação e aprimoramento da confiabilidade operacional, visto que a obsolescência é um fator preocupante na automação industrial (CESAR et al., 2020).

4.2 Tipos de monitoramento

No escopo da presente pesquisa, para os grupos selecionados, PCs, *servers*, *switches* e PLCs, foram utilizados três principais métodos de monitoramento: monitoramento simples, *Zabbix Agent* e SNMP. Cada um desses métodos desempenha seu papel na coleta de dados específicos e para ilustrar a abrangência desses métodos de monitoramento, a Tabela 2 apresenta o número de itens coletados para cada tipo de monitoramento em cada grupo de dispositivos.

Tabela 2 – Número de itens monitorados por tipo de monitoramento.

	Monitoramento simples	***Zabbix Agent***	**SNMP**	**Total**
PCs	3	12	0	15
Servidores	3	13	0	16
Switches	3	0	10	13
PLCs	3	0	7	10

Fonte: Autoria pória.

O *Zabbix Agent* possibilita o monitoramento apenas em dispositivos com sistema operacional, o SNMP é aplicado em dispositivos com suporte ao protocolo, e o monitoramento simples pode ser utilizado em todo dispositivo conectado à rede.

4.3 Itens monitorados

Os itens coletados são organizados e apresentados nas Tabelas 3, 4 e 5, fornecendo uma melhor interpretação dos elementos monitorados para cada tipo de monitoramento da ferramenta implementada, apresentando o nome do item monitorado, grupos que possuem esse item, descrição do item e a *trigger* associada.

Conforme apresentado na Tabela 3, o monitoramento simples oferece uma abordagem dos parâmetros básicos de qualquer tipo de dispositivo conectado à rede, possibilitando o fornecimento de informações como, *status* de disponibilidade na rede, tempo de resposta e perda de dados ICMP. Esta abordagem simplificada é particularmente útil para obter rápidas informações sobre o *status* geral do dispositivo, permitindo o gerenciamento reativo, no caso de indisponibilidade do *host*, e proativo, no caso de identificação de perdas de pacotes ICMP ou aumento do tempo de resposta.

A Figura 6 apresenta um período do monitoramento do dispositivo nomeado como PLC_DES01. Conforme observado, o dispositivo ficou indisponível por um longo período. Essa falha foi ocasionada pela desenergização do equipamento para realização de manutenção programada. Entretanto, a análise do gráfico revela que o *Zabbix* respondeu conforme o esperado ao detectar uma perda total de pacotes, atingindo 100%, e um *status* do item *Ping ICMP* igual a 0 ao longo desse período. Além disso, conforme apresentado na parte inferior esquerda da Figura 6, foi emitido o alerta de indisponibilidade do *host*.

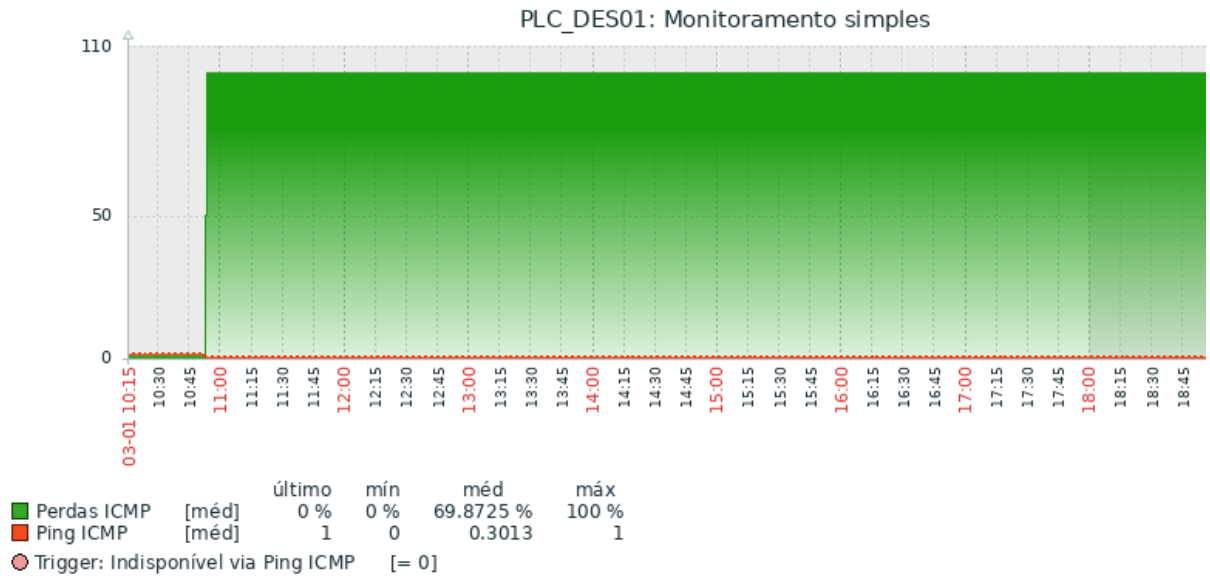
Tabela 3 – Dados coletados com o monitoramento simples.

Item	**Grupos**	**Descrição**	***Trigger***
Ping ICMP	*Servers*, PCs, PLCs e *switches*	Monitora o *status* do dispositivo por meio do Protocolo de Mensagens de Controle da Internet (ICMP, do inglês *Internet Control Message Protocol*). *Status* 0 indica indisponibilidade, *status* 1 indica disponibilidade.	Avalia se o *status* é igual a 0.
Perdas ICMP	*Servers*, PCs, PLCs e *switches*	Monitora a perda de pacotes ICMP. *Status* igual a 0% indica que não houve perda de pacotes; *status* maior que 0% representa a porcentagem de pacotes perdidos durante o *ping*.	Avalia se a perda de pacotes ICMP no dispositivo nos últimos 5 minutos está acima do limite de 20% e abaixo de 100%.
Tempo de resposta ICMP	*Servers*, PCs, PLCs e *switches*	Monitora o tempo de resposta de um dispositivo a um pacote ICMP. *Status* igual a 0 indica que o dispositivo não está disponível. *Status* diferente de 0 representa o tempo, em milissegundos, que o dispositivo demora para responder ao pacote ICMP.	Avalia se o tempo médio de resposta do *ping* no dispositivo, calculado nos últimos 5 minutos, excede 0,15 segundos.

Fonte: Autoria pória.

A ausência de uma rápida identificação desse tipo de falha pode levar a consequências adversas, tais como interrupções não planejadas no processo produtivo. Em ambientes industriais, a falta de comunicação com um PLC pode resultar em falta de controle sobre os dispositivos associados, levando a possíveis falhas e impactos na qualidade, eficiência e segurança da produção. A capacidade do *Zabbix* de emitir alertas durante essas condições é importante para permitir intervenções rápidas da equipe de automação, minimizando assim o tempo de inatividade.

Figura 6 – Monitoramento simples do PLC_DES01.



Fonte: Autoria própria.

Tabela 4 – Dados coletados com o *Zabbix Agent*.

Item	**Grupos**	**Descrição**	***Trigger***
Disponibilidade do agente *Zabbix*	*Servers* e PCs	Monitora a disponibilidade do agente *Zabbix* em um dispositivo. *Status* igual a 1 se o agente está disponível, e 0 se o agente não está disponível.	Avalia se o agente *Zabbix* no dispositivo está indisponível.
Utilização CPU	*Servers* e PCs	Monitora a utilização da CPU de um dispositivo.	Avalia se a utilização da CPU no dispositivo, nos últimos 5 minutos, está acima de 90%.
Fila CPU	*Servers* e PCs	Monitora a fila de espera de processos na CPU, indicando quantos processos estão aguardando para serem executados.	Avalia se a quantidade mínima de processos na fila do dispositivo, nos últimos 5 minutos, ultrapassa três.

Tabela 4 – Dados coletados com o *Zabbix Agent* (Continuação).

Item	**Grupos**	**Descrição**	***Trigger***
CPU privilegiada	*Servers* e PCs	Monitora a porcentagem de tempo que a CPU do sistema gasta em modo privilegiado, que se refere à execução de instruções privilegiadas do sistema operacional.	Avalia se a taxa do tempo de uso da CPU no modo privilegiado, nos últimos 5 minutos, ultrapassa o limite crítico máximo de 50%.
Memória	*Servers* e PCs	Monitora o uso da memória em um dispositivo.	Avalia se a utilização da memória do dispositivo, nos últimos 5 minutos, ultrapassa o limite de 80% da memória total.
Utilização do espaço do disco	*Servers* e PCs	Monitora a utilização de espaço de armazenamento em um dispositivo.	Avalia se a utilização do espaço em disco está acima de 80%, se a diferença entre o espaço total e o espaço usado é inferior a 10 GB ou se o tempo restante estimado para o espaço em disco ser menor que 1 dia.
Status operacional da interface	*Servers* e PCs	Monitora o *status* operacional de uma interface de rede. Se a interface está operacional, o *status* é igual a 1 (ativo); caso contrário, o *status* é igual a 2 (inativo).	Avalia se o *status* da interface de rede é igual a 1 (ativo).
Bits enviados	*Servers* e PCs	Monitora o número de *bits* recebidos pela interface.	Avalia se a média de *bits* enviados nos últimos 15 minutos é maior que 95% da banda máxima.
Bits recebidos	*Servers* e PCs	Monitora o número de *bits* recebidos pela interface.	Avalia se a média de *bits* recebidos nos últimos 15 minutos é maior que 95% da banda máxima.

Tabela 4 – Dados coletados com o *Zabbix Agent* (Continuação).

Item	**Grupos**	**Descrição**	***Trigger***
Pacotes de entrada com erros	*Servers* e PCs	Monitora a quantidade de pacotes recebidos com erros em uma interface de rede.	Avalia se os erros de entrada ou saída na interface de rede ultrapassam 2 nos últimos 5 minutos.
Interface de pacotes de saída com erros	*Servers* e PCs	Monitora a quantidade de pacotes enviados com erros em uma interface de rede.	Verifica se os erros de entrada ou saída na interface de rede ultrapassam 2 nos últimos 5 minutos.
Velocidade da interface	*Servers* e PCs	Monitora a velocidade da interface de rede do dispositivo.	Avalia se a taxa média de entrada ou saída de dados da interface de rede nos últimos 15 minutos é maior, ou igual que 90% da capacidade máxima da interface.
Temperatura do disco	*Servers*	Monitora a temperatura da CPU do dispositivo em graus *Celsius*.	Avalia se a temperatura da CPU do dispositivo é igual ou superior a 70ºC.

Fonte: Autoria própria.

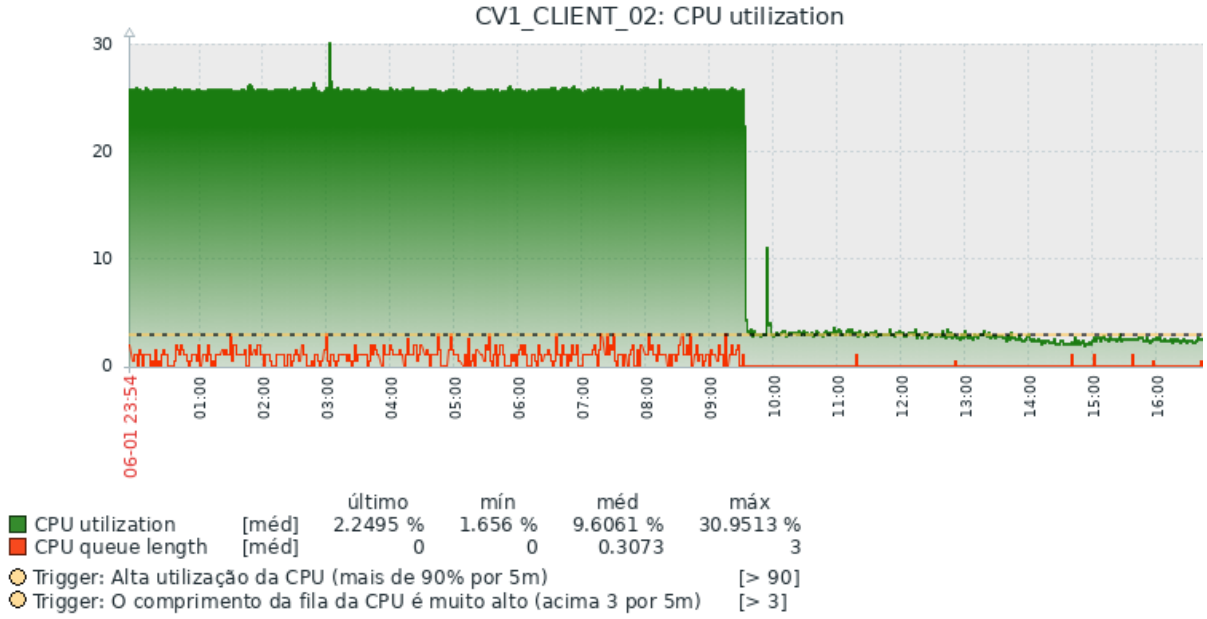
Conforme apresentado na Tabela 4, o *Zabbix Agent*, por sua vez, permite o monitoramento de uma maior variedade de parâmetros. A implementação deste tipo de monitoramento amplia a capacidade de coleta de dados, contribuindo para uma análise mais refinada e personalizada dos dispositivos que utilizam sistemas operacionais. Um exemplo de monitoramento utilizando o *Zabbix agent* pode ser observado na Figura 7.

A Figura 7 apresenta um período da coleta dos dados do dispositivo nomeado como CV1_CLIENT_02. Conforme observado, o dispositivo apresentou variações na fila de privilégios e alto consumo de CPU no período analisado. Essas flutuações na fila de privilégios indicam instabilidade na priorização de tarefas da máquina, podendo resultar em atrasos imprevisíveis no processamento de informações críticas. Isso é particularmente problemático em ambientes industriais, onde a sincronização precisa e o tempo de resposta consistente são essenciais para garantir o bom funcionamento do sistema de automação.

Além disso, o consumo variável de CPU do dispositivo pode levar a inconsistências no desempenho do cliente do sistema supervisório, resultando em atrasos na atualização e exibição de dados em tempo real no SCADA. Essa inconsistência na resposta do cliente pode prejudicar a capacidade da equipe de monitorar e controlar o processo, introduzindo potenciais riscos operacionais.

Para mitigar as variações na fila de privilégios e o consumo de CPU no dispositivo,

Figura 7 – Monitoramento via *Zabbix agent* do CV1_CLIENT_02.



Fonte: Autoria própria.

são implementadas medidas de otimização e estabilidade no ambiente de execução do *host*. Inicialmente, realizou-se um ajuste na configuração de prioridades das tarefas executadas pelo dispositivo, visando estabilizar a fila de privilégios e promover uma distribuição mais consistente dos recursos do sistema. Ademais, foram identificadas tarefas não essenciais em execução que foram encerradas, liberando recursos do processador.

Tabela 5 – Dados coletados com o SNMP.

Item	**Grupos**	**Descrição**	***Trigger***
Utilização de memória	*Switches*	Monitora a utilização da memória do dispositivo.	Avalia se a utilização de memória no dispositivo nos últimos 5 minutos ultrapassou 90% do valor total.
Temperatura	*Switches*	Monitora a temperatura do dispositivo.	Avalia se a média da temperatura nos últimos 5 minutos é superior a 50°C.
Utilização da CPU	*Switches*	Monitora a utilização da CPU do dispositivo.	Avalia se a utilização da CPU nos últimos 5 minutos é superior a 50% do valor total.

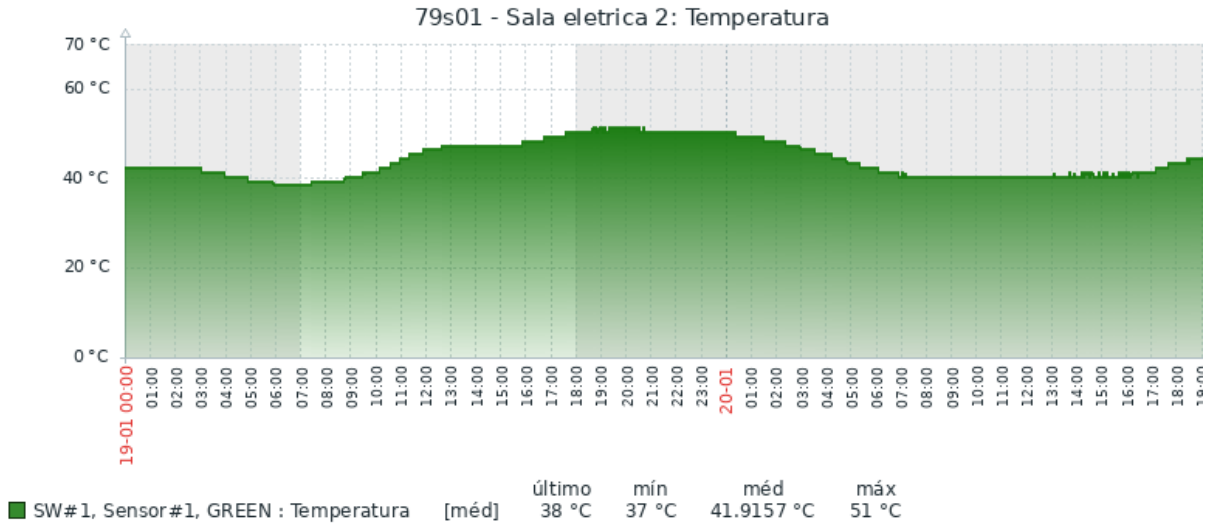
Tabela 5 – Dados coletados com o SNMP (Continuação).

Item	**Grupos**	**Descrição**	***Trigger***
Disponibilidade do agente SNMP	*Switches* e PLCs	Monitora a disponibilidade do agente SNMP. *Status* igual a 0 significa que o dispositivo não está disponível para monitoramento com o SNMP, indicando uma possível falha ou indisponibilidade na comunicação com o dispositivo.	Avalia se o valor da coleta é igual a 0 por mais de 5 minutos, se for indica indisponibilidade do dispositivo.
Velocidade	*Switches* e PLCs	Monitora a velocidade de cada interface de entrada ou saída do dispositivo.	Avalia se a taxa de tráfego de entrada ou saída na interface ultrapassa 90% do valor total.
Status operacional	*Switches* e PLCs	Monitora o *status* de operação da interface de entrada ou saída, tal que, *status* igual a 1 (ativo), 2 (inativo), 3 (em teste) e 4 (desconhecido).	Avalia se o *status* de operação da interface de entrada ou saída sofreu uma mudança de 1 para 2 ou qualquer mudança com diferença maior ou igual a 1 unidade.
Bits enviados	*Switches* e PLCs	Monitora o número de *bits* recebidos pela interface.	Avalia se a média de *bits* enviados nos últimos 15 minutos é maior que 95% da banda máxima.
Bits recebidos	*Switches* e PLCs	Monitora o número de *bits* recebidos pela interface.	Avalia se a média de *bits* recebidos nos últimos 15 minutos é maior que 95% da banda máxima.
Pacotes de entrada com erros	*Switches* e PLCs	Monitora a quantidade de pacotes recebidos com erros em uma interface de rede.	Avalia se os erros de entrada ou saída na interface de rede ultrapassam 2 nos últimos 5 minutos.
Pacotes de saída com erros	*Switches* e PLCs	Monitora a quantidade de pacotes enviados com erros em uma interface de rede.	Avalia se os erros de entrada ou saída na interface de rede ultrapassam 2 nos últimos 5 minutos.

Fonte: Autoria própria.

A utilização do SNMP é aplicável a dispositivos que não podem ser monitorados com o *Zabbix Agent* e que suportam o protocolo SNMP. Conforme observado na Tabela 5, o SNMP coleta informações específicas desses dispositivos, incluindo a utilização da CPU, a velocidade, *status* operacional das interfaces, entre outros parâmetros importantes para o funcionamento das redes industriais.

Figura 8 – Monitoramento via SNMP do *switch* 79s01.



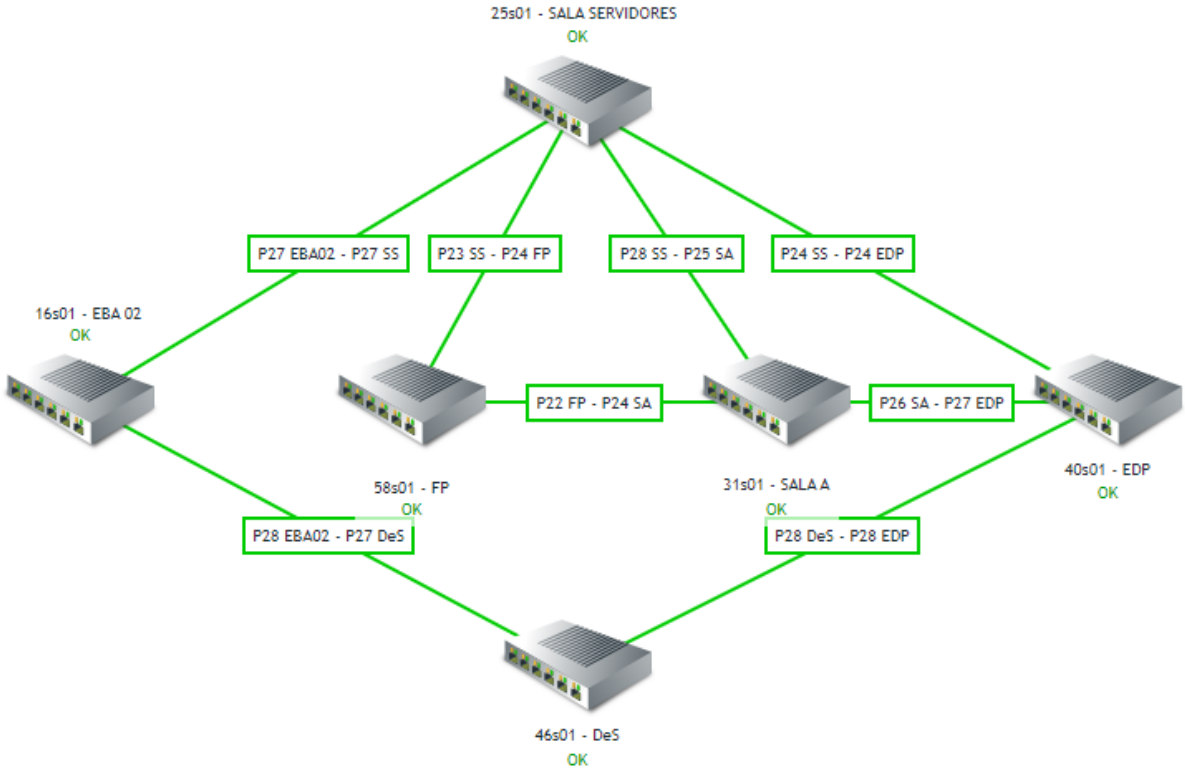
Fonte: Autoria própria.

A Figura 8 apresenta um período da coleta dos dados de um *switch* nomeado como 79s01 - Sala elétrica 2. Conforme observado, o dispositivo apresentou variações em sua temperatura, atingindo uma temperatura máxima de 51 °C. Essa oscilação decorreu de uma falha no sistema de ar condicionado da sala elétrica que abriga o *switch*, sendo que a temperatura normalizou após a restauração da refrigeração. Problemas como esse são motivo de preocupação nas redes industriais, pois variações extremas de temperatura podem afetar o desempenho e a confiabilidade dos dispositivos, podendo levar a falhas operacionais e prejuízos no processo produtivo. Essa preocupação é ainda mais relevante quando se refere aos *switches*, que desempenham um papel fundamental ao possibilitar a interconexão de todo o sistema industrial. A estabilidade desses componentes é essencial para garantir a continuidade das operações e a segurança dos processos na planta industrial.

Outro recurso relevante do *Zabbix* são os mapas, uma forma de visualização da interligação dos dispositivos monitorados, permitindo criar representações dinâmicas que refletem o estado em tempo real do ambiente, conforme apresentado na Figura 9.

Essa funcionalidade é útil para auxiliar na compreensão da topologia da rede e as relações entre os dispositivos. No contexto deste estudo, explora-se essa capacidade da

Figura 9 – Mapa dos *siwtches* da rede B da etapa da aciaria.



Fonte: Autoria própria.

ferramenta ao gerar mapas para os *switches* da rede da planta de estudo, Figura 9. Os mapas não apenas ofereceram uma perspectiva visual da disposição física dos *switches*, mas também permitem um gerenciamento proativo das alterações de trafego de rede entre eles, através da alteração das cores das linhas que os interconectam, facilitando assim a identificação de potenciais pontos de falha e áreas críticas na infraestrutura de rede.

4.4 Limitações

Além dos itens monitorados mencionados anteriormente, é importante abordar os itens não incluídos no escopo de monitoramento devido às limitações técnicas. Entre esses itens estão a temperatura do PLC e o diagnóstico de erros desse dispositivo. A impossibilidade de monitorar esses aspectos críticos foi identificada como uma lacuna no sistema, pelo fato do protocolo SNMP não permitir a coleta desses dados.

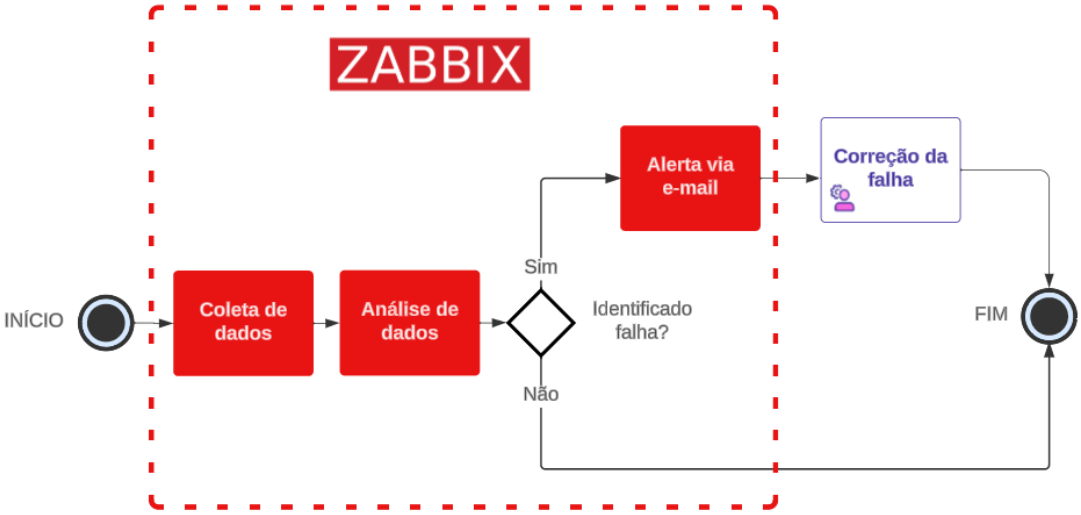
Pesquisas realizadas indicaram a viabilidade de superar uma dessas limitações utilizando ferramentas especializadas, como o *Pop Protect* SNMP (VOLT, 2023). *Hardware* com protocolo SNMP que pode ser conectado a um sensor a fim de possibilitar a coleta de temperatura de um determinado local via SNMP. Esta funcionalidade torna-se particularmente relevante quando instalada nos *racks* dos painéis de PLCs, proporcionando

informações importantes sobre as condições térmicas desses dispositivos críticos para o processo industrial.

4.5 Desempenho da ferramenta

O *Zabbix* oferece uma série de contribuições para o gerenciamento de falhas, uma vez que anteriormente ao uso da aplicação, a planta não possuía nenhum tipo de monitoramento de desempenho dos dispositivos dos níveis de controle e supervisão. Uma das principais vantagens é sua capacidade de fornecer uma resposta rápida a alterações na coleta de dados e emissão de alertas por *e-mail*, devido ao seu fluxo de funcionamento, conforme apresentado na Figura 10.

Figura 10 – Fluxo de funcionamento a cada ciclo de coleta do *Zabbix*.

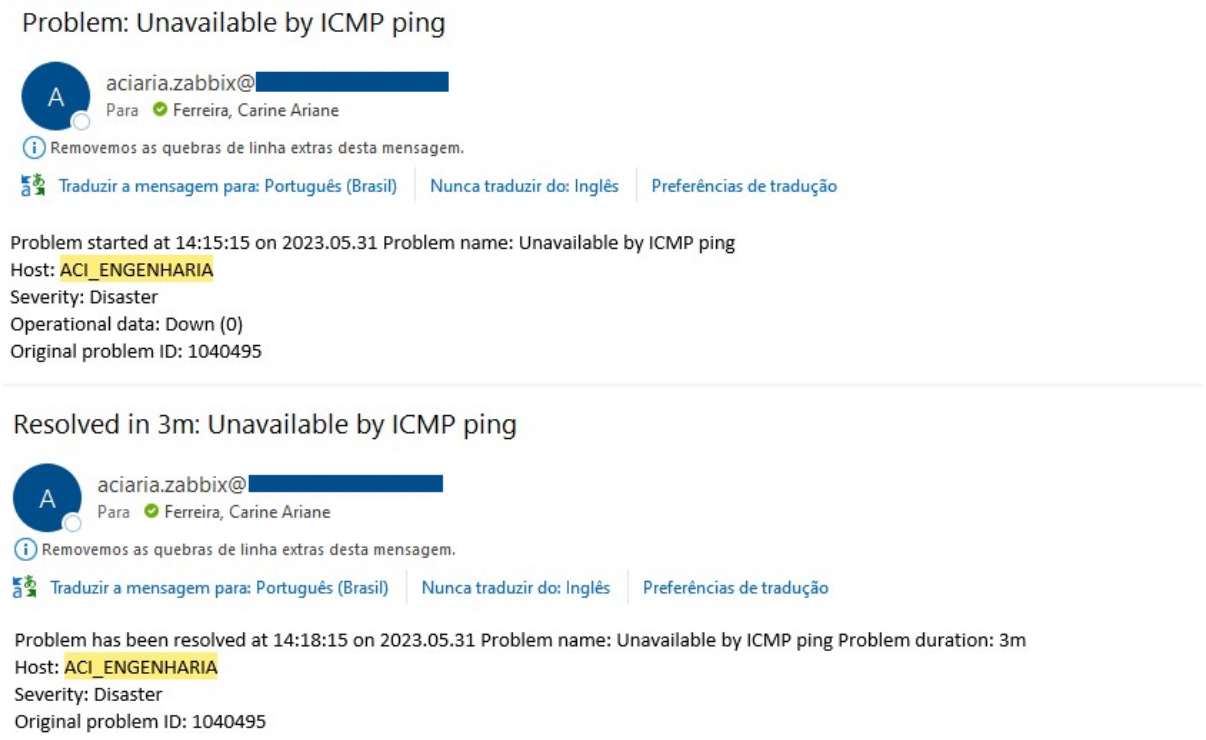


Fonte: Autoria própria.

Assim, observa-se que para todo dado coletado é feita a análise se é identificada uma falha através do *trigger*. Em caso afirmativo o *e-mail* é enviado conforme configurado na ferramenta *web* e o problema é solucionado pela equipe de automação. Para dados que não são identificadas falhas durante a análise do parâmetro coletado, o ciclo se encerra com o seu armazenamento no banco de dados, pelo período configurado. Um exemplo de coleta e alerta de incidente é apresentado na Figura 11, obtida após a simulação de uma falha de indisponibilidade de um dos servidores na rede. Para a realização da simulação, o dispositivo foi reiniciado às 14:14:47 do dia 31/05/2023.

Como pode ser observado na Figura 11, a ferramenta de monitoramento possui uma resposta ágil à coleta de dados e emissão de alerta através da análise lógica de seus *triggers*. Assim, a equipe de automação consegue responder de forma mais rápida

Figura 11 – Alerta por *e-mail*.

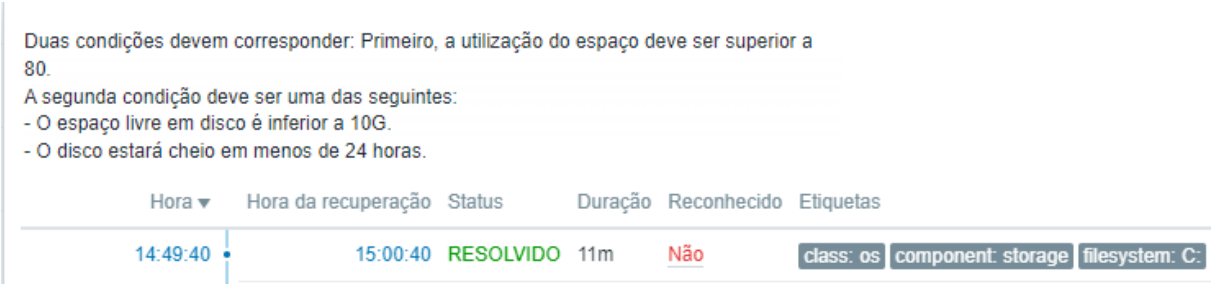


Fonte: Autoria própria.

e assertiva a falhas reativas e falhas proativas, minimizando o tempo de inatividade e garantindo a confiabilidade operacional.

Além disso, o *Zabbix* oferece um ambiente de fácil visualização e entendimento dos dados. Recursos como descrição de itens e *triggers* tornam os dados coletados e as condições de acionamento dos *triggers* acessíveis a qualquer pessoa, independentemente de sua familiaridade com a configuração da ferramenta, conforme apresentado na Figura 12.

Figura 12 – Exemplo de descrição da *trigger*.



Fonte: Autoria própria.

A Figura 12 mostra um exemplo de descrição de *trigger* para o alerta de pouco espaço de armazenamento no *host* ACI_ ENGPLC_ BOF, que se trata de uma estação de engenharia para PLCs. Conforme observado Figura 12, mesmo sem saber qual a expressão

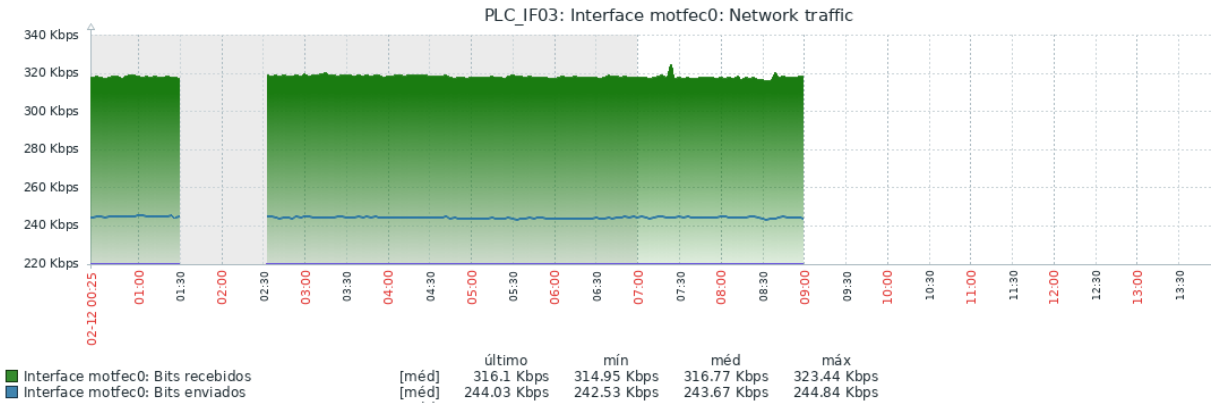
lógica para ativação deste incidente, pela descrição sabe-se que o alerta é emitido caso o valor coletado seja menor que 80% do disco total, se o espaço em disco livre é menor que 10 GB ou se o tempo de previsão para o disco alcançar sua capacidade total é menor que 24 horas.

Outro aspecto importante é a possibilidade de visualização de diversos dados em função do tempo num mesmo gráfico, conforme apresentado nas Figuras 6 e 7. Essa funcionalidade permite que os usuários examinem diferentes parâmetros simultaneamente, facilitando a identificação de padrões ou correlações entre os dados.

Dessa forma, ao longo da implementação do *Zabbix* na planta de produção da aciaria, a expectativa é que as falhas reativas sejam reduzidas através do gerenciamento proativo das falhas, uma vez que a equipe de manutenção terá acesso a informações em tempo real para tomar medidas preventivas antes que as falhas ocorram. A avaliação da diminuição das falhas será conduzida por meio da análise comparativa do indicador de tempo de produção antes e após a implementação do *Zabbix*, oferecendo uma base sólida para mensurar o impacto positivo da solução no gerenciamento proativo de falhas na planta industrial.

Até o momento, a análise do impacto nas operações destaca uma contribuição para o gerenciamento proativo de falhas e a redução da inatividade. A utilização do *Zabbix* mostrou-se importante, por exemplo, na identificação e análise de problemas que surgiram após a implementação de novos PLCs. O desafio envolvia perdas intermitentes de comunicação entre os PLCs e o sistema de supervisão. Os itens de tráfego de dados revelaram que o problema originava-se nos PLCs, evidenciando uma interrupção completa do tráfego de dados desses dispositivos, conforme apresentado na Figura 13.

Figura 13 – Tráfego de dados do PLC.



Fonte: Autoria própria.

Como pode ser observado na Figura 13, o dispositivo PLC_IF03, apresentou encerramento completo do seu tráfego de dados durante 2 momentos em um mesmo dia e neste caso foi descartada a hipótese de problema na interface, pois o seu *status* no *Zabbix* permaneceu disponível nesse período analisado. Isso facilitou o rastreamento da origem

do problema. Ao entrar em contato com a empresa responsável pelo PLC, foi sugerido aumentar a porcentagem da CPU dedicada à transmissão de dados, passando de 40% para 60%. Segundo Automation (2012), esse valor deve ficar em torno de 75%. Após essa modificação, não foram mais observadas ocorrências do problema.

Esse exemplo corrobora a eficácia do *Zabbix* na gestão proativa de falhas, fornecendo uma base para a tomada de decisões informadas. A identificação precoce desses problemas contribui não apenas para a resolução mais rápida de incidentes, mas também para a otimização contínua do desempenho do sistema industrial.

4.6 Custos de implementação da ferramenta

Para a implementação do sistema de monitoramento na aciaria, realizou-se a incorporação de dois novos computadores destinados ao monitoramento específico das áreas do LD e MLC. Nesse contexto, não houve custos associados à aquisição dos computadores, uma vez que as máquinas utilizados eram recursos disponíveis.

É relevante observar que em situações em que a aquisição de mão de obra especializada fosse necessária, os custos seriam substancialmente menores em comparação com o impacto financeiro de uma hora de parada do processo de produção na aciaria. Utilizando algumas referências da literatura para calcular a produção média por hora de uma siderúrgica no Brasil (IAB, 2016) e assim, sabendo o custo médio de uma tonelada de aço (TRANSITIONZERO, 2022), consegue-se estimar o valor de uma hora de produção de aço, resultando em média 466 mil reais, que equivale a aproximadamente 930% do custo de implementação do *Software Zabbix*. Isso evidencia o valor agregado e o retorno sobre o investimento proporcionado pela utilização do *Zabbix* como ferramenta de monitoramento e gerenciamento de desempenho na indústria siderúrgica.

Considerando a importância do uso da ferramenta de monitoramento, é recomendável investir em treinamento para a equipe, garantindo uma compreensão da ferramenta, seu potencial e suas aplicações, contribuindo para a otimização contínua do processo siderúrgico e a rápida detecção de problemas, visando a máxima eficiência operacional.

4.7 Desafios

A ausência de acesso à internet na rede da planta de produção impôs uma dificuldade durante a implementação do sistema de monitoramento. Dada a política de segurança, a rede industrial não poderia ser conectada à internet, e, consequentemente, os computadores na planta não tinham acesso à *web*. Essa limitação trouxe um desafio significativo, especialmente considerando que a instalação do *Zabbix* e a criação das VMs envolviam o *download* de *softwares* e recursos *online*.

Como solução, todas as VMs precisaram ser configuradas fora da rede de automação industrial, onde havia conectividade com a internet, antes de serem transferidas para as máquinas na planta de estudo. Esse processo destacou a importância de considerar restrições específicas do ambiente industrial durante a implementação de soluções tecnológicas.

O ajuste de desempenho do *Zabbix* foi implementado para otimizar o desempenho da ferramenta, considerando especialmente o volume de dados gerados em ambientes industriais complexos. Uma das principais estratégias adotadas consistiu na otimização da coleta e armazenamento de dados. Isso foi alcançado por meio da configuração do tempo de armazenamento de dados, a fim de não sobrecarregar o sistema. Contrariamente ao padrão do *Zabbix*, que estabelece um período de armazenamento de dados de seis meses com uma frequência de coleta a cada 1 segundo, foi definido que o armazenamento será de no máximo três meses.

O treinamento da equipe de automação foi realizado, mas a equipe de manutenção ainda carece desse conhecimento. Essa lacuna representa um objetivo futuro, visando capacitar toda a equipe para aumento da compreensão e uso da ferramenta de monitoramento. Essa abordagem baseada na demanda e na experiência prática é fundamental para garantir que o *software* atenda aos desafios específicos da aciaria e contribua efetivamente para a melhoria do monitoramento e do controle dos ativos de supervisão e controle, bem como dos *switches* da rede.

4.8 Segurança

A segurança do sistema *Zabbix* é uma prioridade para garantir a integridade e confidencialidade dos dados críticos monitorados na rede de automação industrial. Portanto, foram aplicadas algumas medidas para reforçar a segurança, complementando as existentes na rede de automação, isso inclui a configuração da rede como uma rede fechada, isolada de outras redes que não estejam relacionadas à automação. Além disso, todos os dispositivos são protegidos com controle de acesso e não possuem conectividade com a internet. Desta forma, para implementação do *Zabbix* em rede local foi necessário utilizar um servidor de e-mail *SMTP* interno, já existente na planta. Esta configuração permite o envio de notificações sem necessidade de conexão à internet, assegurando uma comunicação eficaz na infraestrutura corporativa.

Os computadores dedicados ao monitoramento estão isolados virtualmente, o controle de acesso é estritamente gerenciado pela equipe de automação, que utiliza senhas robustas para garantir a autenticação segura nos computadores de monitoramento, nas VMs e na plataforma *web* do *Zabbix*.

A equipe de automação é a única com autorização para acessar os serviços configuráveis relacionados ao *Zabbix*, utilizando senhas fortes para autenticação. Para a equipe

de manutenção, o acesso é concedido apenas com as permissões de apenas leitura.

Adicionalmente, são realizados *backups* semanais do sistema *Zabbix*, visando a pronta recuperação em casos de falhas ou incidentes. O monitoramento constante dos servidores de monitoramento é uma prática adotada para garantir que o armazenamento não seja extrapolado, prevenindo possíveis interrupções nos serviços.

4.9 Considerações parciais

A implementação do sistema de monitoramento *Zabbix* na planta de produção da aciaria trouxe contribuições substanciais para o aprimoramento do desempenho operacional e a eficácia na gestão de ativos críticos. A análise dos resultados evidenciou melhorias significativas no monitoramento dos dispositivos dos níveis de controle e supervisão, proporcionando uma visibilidade mais profunda sobre o desempenho desses dispositivos. A capacidade do *Zabbix* em identificar proativamente problemas e acionar alerta, como demonstrado pelos *triggers*, mostrou-se fundamental para a rápida resposta a incidentes, minimizando o tempo de inatividade e garantindo a confiabilidade operacional.

Após a implementação da ferramenta *Zabbix*, observou-se uma significativa melhora nos resultados relacionados a falhas de automação, originadas por problemas em redes e ativos dos níveis de controle e supervisão. Uma análise comparativa dos últimos anos revelou que o resultado de aproximadamente 15% das interrupções do processo originados por deficiências na infraestrutura de rede e falhas dos ativos dos níveis de controle e supervisão tiveram uma redução para 6,5%, indicando uma tendência de melhoria contínua na estabilidade e confiabilidade dos sistemas monitorados.

O impacto positivo do *Zabbix* na resolução de problemas específicos, como as falhas de comunicação entre os PLCs, destaca a eficácia da ferramenta na identificação precoce e na resolução de possíveis incidentes. A capacidade de registrar eventos, correlacionar perdas de comunicação com a utilização da CPU e fornecer informações detalhadas orientou ajustes precisos nos parâmetros dos dispositivos, contribuindo para a otimização contínua do desempenho do sistema industrial.

Apesar dos desafios enfrentados durante a implementação, como a configuração das redes das VMs e a ausência de acesso à internet na rede da planta, as soluções adotadas demonstraram a adaptabilidade do *Zabbix* a ambientes industriais complexos. Quanto aos custos, a implementação do *Zabbix* não implicou em despesas diretas, pode-se utilizar algumas referências da literatura para calcular a produção média por hora de uma siderúrgica no Brasil (IAB, 2016) e assim, sabendo o custo médio de uma tonelada de aço (TRANSITIONZERO, 2022), consegue-se estimar o valor de uma hora de produção de aço, resultando em média 466 mil reais, que equivale a aproximadamente 930% do custo de implementação do *Software Zabbix*. Isso evidencia o valor agregado e o retorno sobre o investimento proporcionado pela utilização do *Zabbix* como ferramenta de monitoramento

e gerenciamento de desempenho na indústria siderúrgica.

5 Considerações finais

A etapa da aciaria em um processo siderúrgico, marcada por sua complexidade e dinamismo, carecia de uma ferramenta que oferecesse um monitoramento ampla e em tempo real do desempenho dos ativos de controle e supervisão da sua rede industrial.

No cenário prévio à implementação da ferramenta *Zabbix*, a detecção de problemas de desempenho limitava-se a observações empíricas, muitas vezes identificadas somente quando os dispositivos apresentavam anormalidades em seu funcionamento ou, em casos mais críticos, quando ocorriam paralisações inesperadas. Essa abordagem reativa, embora comum em muitos ambientes industriais, acarretava consequências significativas, incluindo períodos de inatividade não planejados, perda de eficiência operacional e potencial impacto na qualidade da produção.

Durante a implementação, os registros de falhas nos níveis de controle e supervisão, que anteriormente resultavam em interrupções no processo correspondentes a 15% do total de falhas, foram reduzidos para 6,5% após a implementação do *Zabbix*. A tendência é que essa taxa de redução aumente com o gerenciamento proativo fornecido pelo *Zabbix*. As falhas evitadas incluem interrupções de PLC por configurações indevidas de tráfego de dados, interrupção de *switches* e servidores por alta temperatura, atraso no tráfego de switch por alto consumo de CPU, e interrupção de clientes por alto consumo de disco. Essas falhas teriam consequências para o processo, incluindo interrupção na produção e risco da segurança dos empregados.

Além disso, a capacidade de criar alertas personalizados e *triggers* específicos para cada grupo de ativos, como PLC, servidores, *switches* e PCs, permitiu um monitoramento mais detalhado e preciso, contribuindo para uma detecção eficiente e gestão das falhas. Em síntese, a implementação do *Zabbix* não apenas preencheu a lacuna previamente existente no gerenciamento de desempenho, mas estabeleceu um novo modo de gerenciamento de falhas reativas e proativas. Além de auxiliar na otimização e eficiência operacional, reduzindo o tempo de inatividade não planejado, mas também proporcionou informações importantes para o aprimoramento continuo da integridade e a confiabilidade dos ativos críticos.

5.1 Trabalhos futuros

Na continuidade do aprimoramento do sistema de monitoramento, alguns tópicos futuros emergem como perspectivas para otimizar ainda mais a eficácia e abrangência do monitoramento das redes de automação. A exploração de outras ferramentas como o *Zabbix* será um passo para avaliar diferentes abordagens e identificar melhorias no cenário de monitoramento.

A integração do Grafana, renomada plataforma de análise e visualização de dados, representa outro ponto relevante a ser explorado. Essa implementação proporcionará recursos avançados de visualização, enriquecendo a análise e apresentação dos parâmetros coletadas.

Além disso, a expansão do escopo de coleta de dados mediante o uso de módulos adicionais é uma estratégia promissora. A incorporação de soluções como o *Pop Protect SNMP* possibilita a obtenção de informações específicas, como a temperatura de dispositivos como o PLC, que, de outra forma, não seriam monitoradas (VOLT, 2023).

Um desdobramento importante concentra-se na adaptação do monitoramento SNMP para incluir redes *Profibus* no escopo do *Zabbix*. O estudo de Bittencourt e Oliveira (2017) serve como referência, abordando a implementação de ferramentas *Profilink* que viabilizam o monitoramento de redes *Profibus* através do protocolo SNMP, ampliando as capacidades de monitoramento da infraestrutura.

Referências

ALVES, N.; SILVA, S. L. P. da. Introdução às redes wireless. *Nota Técnica CBPF-NT-003*, v. 2, 2003.

AUTOMATION, R. Logix5000 controller design considerations. *Milwaukee, USA*, 2012.

BARTH, W. *Nagios: System and network monitoring*. [S.l.]: No Starch Press, 2008.

BHARGAVA, C.; BANGA, V. K.; SINGH, Y. Failure prediction and health prognostics of electronic components: A review. *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, IEEE, p. 1–5, 2014.

BITTENCOURT, A. A.; OLIVEIRA, C. A. Monitoramento de aplicações no ambiente de automação industrial. *21º Seminário de Automação e TI*, São Paulo, p. 228–237, 2017.

BRANQUINHO, M. A. et al. *Segurança de automação Industrial e SCADA*. 1ª. ed. Rio de Janeiro, RJ, Brasil: Elsevier Editora Ltda., 2014.

CARLSSON, T. *Industrial network market shares 2023*. 2023. Acesso em 23/02/2024. Disponível em: <https://www.hms-networks.com/news-and-insights/news-from-hms/2023/05/05/industrial-network-market-shares-2023>.

CAVALLIN, F. Estudo sobre redes de comunicação para automação industrial. 2016. Trabalho de Conclusão de Curso (Especialização em Automação Industrial) - Universidade Tecnológica Federal do Paraná, Curitiba.

CESAR, E. L. et al. Technological obsolescence management: monitoring electrical equipment and automation systems. *IEEE Industry Applications Magazine*, IEEE, v. 26, n. 4, p. 82–87, 2020.

CISCO. *Troubleshooting High CPU Utilization on Cisco Catalyst 3750 Series Switches*. Acesso em 27/02/2024. Cisco. Disponível em <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/cpu_util.html#pgfId-998352>.

DJIEV, S. Hierarchical levels in industrial networks. 2016. Acesso em 28/11/2023.

FERNANDEZ, M. P. Rede de computadores. *UECE, Fortaleza*, 2015.

FERREIRA, N. F. *Controle da temperatura do aço líquido em uma aciaria elétrica*. 2010. Trabalho de Pós-Graduação em Engenharia de Minas, Metalúrgica e de Materiais, para a obtenção do título de Doutor em Engenharia - Universidade Federal do Rio Grande de Sul, Porto Alegre.

FONSECA, M. Desempenho de sistemas de automação-métricas e práticas. *Seminário de automação de processos*, v. 8, p. 18–28, 2004.

FONSECA, M. d. O. et al. Monitoração do desempenho de redes de automação usando SNMP. *Tecnologia em Metalurgia, Materiais e Mineração*, ABM-Associação Brasileira de Metalurgia, Materiais e Mineração, v. 3, n. 1, p. 1–6, 2013.

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. Porto Alegre - RS: AMGH Editora, 2009.

GALLOWAY, B.; HANCKE, G. P. Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, IEEE, v. 15, n. 2, p. 860–880, 2012.

GELLE, E.; KOCH, T. E.; SAGER, P. It asset management of industrial automation systems. p. 123–128, 2005.

IAB. Instituto aço brasil. *http://www. acobrasil. org. br/site/portugues/aco/processo–etapas. asp. Acesso em*, v. 20, n. 05, p. 2016, 2016.

IVANKIO, A. S. Monitoramento de equipamentos da rede de automação em subestações utilizando o protocolo SNMP. Universidade Tecnológica Federal do Paraná, 2019.

KIESEL, R. et al. Cybersecurity in networked production. white paper. Fraunhofer IPT, 2021.

LEE, J. et al. A study on the advanced plc system using the mib and snmp. p. 2363–2367. Seoul, Republic of Korea, 2007.

LIMA, J. dos R. *Monitoramento de Redes com Zabbix: Monitore a saúde dos servidores e equipamentos de redes*. Rio de Janeiro: Brasport, 2014.

LUGLI, A. B.; SANTOS, M. M. D. Redes industriais: Características, padrões e aplicações. *São Paulo: Érica*, 2014.

MACHADO, M. L. P. *Apostila de siderurgia: da matéria prima ao aço laminado*. 2006. Curso siderúrgico.

MAIA, B. T. et al. Lança de oxigênio - multiplas funções durante o tap to tap. *ABM week*, 2018.

MARCHALL, P. S.; RINALDI, J. S. *Industrial Ethernet*. 2004. ISA.

MONDADORI, J. A. P. *Redes Industriais*. 2016. Produção de Materiais Didáticos.

MOURÃO, M. B. et al. Introdução à siderurgia. 2007.

OLIVEIRA, D. N. d. et al. Proposta de um sistema de gerência de redes plc utilizando SNMPv3. Universidade Federal de Goiás, 2009.

OLUPS, R. *Zabbix Network Monitoring*. Birmingham, UK: Packt Publishing Ltd, 2016.

PEISERT, S. et al. Perspectives on the solarwinds incident. *IEEE Security & Privacy*, IEEE, v. 19, n. 2, p. 7–13, 2021.

RIBEIRO, M. A. *Automaçao Industrial*. 5ª. ed. Salvador - BA: Tek treinamento consultoria, 2005.

SILVA, P. S.; JÚNIOR, A. C. G. Análise de falhas em ativos de automação com técnica fta e fmea. *15º seminário de automação e TI industrial*, 2011.

SOARES, A. C. Otimização na programação de aços de uma aciaria através de um modelo matemático de setup dependente da sequência. 2017.

STALLINGS, W. SNMP, SNMPv2, and CMIP: The practical guide to network management. Addison-Wesley Longman Publishing Co., Inc., 1993.

TADER, P. Server monitoring with zabbix. *Linux Journal*, Belltown Media Houston, TX, v. 2010, n. 195, p. 7, 2010.

TÂMEGA, F. Fundição de processos siderúrgicos. *Londrina: Editora e Distribuidora SA*, 2017.

TOSTES, A. R. d. O. Monitoramento e controle da temperatura, umidade, tensão, presença e chama no data center do instituto federal de minas gerais-campus ouro preto. 2022. Monografia (Graduação em Engenharia de Controle e Automação) - Escola de Minas, Universidade Federal de Ouro Preto, Ouro Preto.

TRANSITIONZERO. *Global Steel Cost Tracker*. 2022. <https://www.transitionzero.org/products/global-steel-cost-tracker>. Acesso em 01/02/2024.

TURNER, D. et al. California fault lines: understanding the causes and impact of network failures. San Diego, p. 315–326, 2010.

VALENTE, J. M. Monitoramento de ativos em uma rede de computadores de automação com aplicação da ferramenta Zabbix. 2023. Monografia (Graduação em Engenharia de Controle e Automação) - Escola de Minas, Universidade Federal de Ouro Preto, Ouro Preto.

VARGAS, D. P. Gerenciamento e monitoramento de redes: um estudo de caso da utilização da ferramenta zabbix no âmbito da base administrativa da guarnição de Santa Maria. Pituba, Salvador - BA, 2020.

VOLT. *Pop Protect SNMP*. 2023. <https://volt.ind.br/equipamento/pop-protect-snmp/>. Acessado em 23/02/2024.

ZABBIX, S. Zabbix. *<http://www.zabbix.com/>*, 2014. Acesso em 02/01/2023.

ZOROTEO, D. C. et al. *Conceitos Gerais de Redes Industriais*. 2018. Apostila de atividade prática da disciplina de Redes Industriais, UTFPR - Universidade Tecnológica Federal do Paraná, Paraná, Brasil.