SEGURANÇA DE DADOS EM AMBIENTES INDUSTRIAIS: UMA ABORDAGEM APLICADA EM AGVS E CLPS

Marcelo M. Oliveira - Faculdade de Tecnologia “Adib Moisés Dib” de São Bernardo do Campo

Marcelo.oliveira134@fatec.sp.gov.br

Weslley K.C. de Oliveira - Faculdade de Tecnologia “Adib Moisés Dib” de São Bernardo do Campo

Weslley.oliveira@fatec.sp.gov.br

Maria W.S. de Lima - Faculdade de Tecnologia “Adib Moisés Dib” de São Bernardo do Campo

Maria.lima74@fatec.sp.gov.br

Prof. William Ap. C. Lopes - Faculdade de Tecnologia “Adib Moisés Dib” de São Bernardo do Campo

william.lopes17@fatec.sp.gov.br

Resumo

A digitalização e automação na Indústria 4.0 exigem uma abordagem estruturada para a segurança de dados. Veículos Guiados Automatizados (AGVs) e Controladores Lógicos Programáveis (CLPs) são essenciais para a eficiência operacional, mas a proteção das informações entre esses sistemas é frequentemente subestimada, tornando-as vulneráveis a riscos cibernéticos. Este estudo investiga a implementação de soluções que garantem a segurança dos dados em ambientes industriais, com o objetivo de desenvolver e aplicar medidas de segurança cibernética para AGVs e CLPs, utilizando a metodologia Design Science Research (DSR) para validar a eficácia das intervenções propostas. A metodologia DSR foi aplicada em cinco etapas: identificação do problema, definição de objetivos, design e desenvolvimento do artefato, demonstração da solução e avaliação dos resultados. A solução proposta integrou o AGV à rede, utilizando o Microsoft Power BI para monitorar dados em tempo real, com comunicação segura. A demonstração revelou que a integração do Power BI com os AGVs facilitou a análise de dados operacionais. Especialistas relataram

melhorias significativas na eficiência operacional, com reduções de até 25% nos tempos de ciclo e 50% nas falhas recorrentes, estabelecendo um padrão para a segurança de dados em AGVs e CLPs.

Palavras-chave: Cibersegurança, Proteção de Dados, Automação Industrial, Manutenção Preventiva, Design Science Research (DSR).

1- INTRODUÇÃO

A crescente digitalização e automação nas indústrias, especialmente na era da Indústria 4.0, demanda atenção especial à segurança de dados. Veículos Guiados Automatizados (AGVs) e Controladores Lógicos Programáveis (CLPs) desempenham papéis cruciais na otimização de processos industriais. No entanto, a proteção dos dados trocados entre esses sistemas é frequentemente negligenciada, expondo as operações a riscos cibernéticos. A segurança cibernética em ambientes industriais, portanto, não é apenas uma questão técnica, mas um requisito estratégico para a continuidade operacional e proteção de ativos (Kumar e Gupta, 2023).

A importância da segurança de dados se reflete em diversas áreas, incluindo a manutenção preventiva, onde a disponibilização de informações em tempo real pode prevenir falhas e aumentar a eficiência. As indústrias enfrentam desafios para integrar soluções que garantam não só a eficiência operacional, mas também a segurança das informações. Essa relevância é destacada no contexto do Internet das Coisas Industrial (IIoT), onde as tecnologias de Operação (OT) e Informação (IT) estão cada vez mais interligadas. A evolução do IIoT traz à tona uma série de ameaças que desafiam a segurança dos dados, exigindo uma abordagem integrada para a proteção das informações em ambientes industriais. Assim, a escassez de pesquisas que tratam da intersecção entre automação, segurança cibernética e gestão de dados se torna ainda mais evidente (Mekala et al., 2023).

Embora existam estudos sobre AGVs e CLPs, há uma lacuna significativa no que diz respeito à segurança dos dados trocados entre eles. A literatura carece de investigações que integrem práticas de segurança cibernética diretamente no design e operação desses sistemas, especialmente em relação à manutenção preventiva. Essa questão é crítica em um contexto onde a manufatura inteligente, impulsionada pela Indústria 4.0, está em ascensão, exigindo a integração de tecnologias de Internet

das Coisas (IoT) e computação em nuvem. A falta de um foco em segurança cibernética nas fases iniciais do desenvolvimento de sistemas de manufatura pode resultar em vulnerabilidades significativas, expondo as operações industriais a riscos de ataques cibernéticos, que podem levar a danos econômicos e à interrupção das operações. Portanto, esta falta de integração entre teoria e prática motiva este estudo, que busca desenvolver soluções que abordem a segurança dos dados em ambientes industriais (Tuptuk & Hailes, 2018).

O objetivo deste estudo é implementar uma solução que forneça a segurança de dados em AGVs e CLPs utilizando o *Design Science Research* (DSR). Este artigo está estruturado em cinco seções: a primeira apresenta a introdução. A segunda seção apresenta a revisão da literatura, focando a disponibilização de dados na manutenção preventiva, a utilização de AGVs na Indústria 4.0 e a função dos CLPs nesse contexto. A terceira seção descreve a metodologia, detalhando o DSR e sua aplicação neste estudo. A quarta seção aborda a análise e discussão dos resultados obtidos, enquanto a quinta seção apresenta as conclusões e recomendações para futuras pesquisas.

Comentado [SADS1]: Trocar por capitulo

2- REVISÃO DA LITERATURA

A revisão da literatura aborda os temas de disponibilização de dados na manutenção preventiva, veículos guiados automatizados (AGVs) e controladores lógicos programáveis (CLPs) se fundamenta em três pilares principais: coleta e análise de dados para manutenção, segurança cibernética no ambiente de automação industrial e interoperabilidade entre sistemas para operações mais seguras e eficientes.

2.1 Disponibilização de dados na Manutenção Preventivas em ambientes industriais

A disponibilização de dados na manutenção preventiva tem se intensificado devido à digitalização nas indústrias e à crescente conectividade dos sistemas. A implementação de modelos baseados em dados possibilita a análise preditiva, utilizando algoritmos de machine learning para antecipar falhas e otimizar a utilização de equipamentos (ZHANG; YANG; WANG, 2019).

A integração de sensores avançados e sistemas de monitoramento contínuo possibilita a coleta de dados de desempenho em tempo real, permitindo intervenções proativas antes da ocorrência de falhas (PECH et al., 2021). Essa abordagem não apenas minimiza o tempo de inatividade não planejado, mas também melhora a produtividade, contribuindo para a eficiência operacional nas indústrias (JIANG et al., 2021).

No entanto, a eficácia da manutenção preventiva em ambientes industriais ainda enfrenta desafios significativos que podem comprometer seu pleno potencial. A ausência de estruturas de dados adequadas e bem definidas limita não apenas a análise aprofundada dos dados coletados, mas também o desenvolvimento de soluções mais eficazes e inovadoras que poderiam otimizar os processos de manutenção (ACHOUCH et al., 2022). Além disso, é crucial ressaltar que a digitalização e a aplicação de tecnologias de big data são fundamentais para a criação de sistemas de manutenção proativa que não apenas aumentem a eficiência operacional, mas também agreguem valor significativo aos processos industriais em geral (PAPADOPOULOS et al., 2021).

A coleta e análise contínua de dados permitem identificar tendências e padrões que, muitas vezes, não são visíveis em inspeções visuais convencionais. Isso resulta em intervenções mais precisas e eficazes, contribuindo para a redução de falhas e melhorando a disponibilidade dos equipamentos (XU et al., 2020). Portanto, para que a manutenção preventiva atinja seus objetivos, é essencial superar as limitações atuais e adotar uma abordagem mais integrada que aproveite as tecnologias emergentes e a análise de dados.

2.2 AGVs na Indústria

Os Veículos Guiados Automaticamente (AGVs) desempenham um papel fundamental na automação dos processos de manufatura, contribuindo para a segurança e a eficiência no transporte de materiais (COSTA; BUENO, 2024). Ao automatizar o transporte interno, os AGVs reduzem a mão de obra humana e, consequentemente, aumentam a eficiência operacional, especialmente em ambientes como armazéns automatizados e linhas de produção (KUBASAKOVA; KUBANOVA; BENCO, 2024).

Equipados com sensores avançados, os AGVs monitoram o desempenho e a condição em tempo real, permitindo a coleta de dados que facilita a implementação de sistemas de manutenção preventiva (JAVED; MURAM; PUNNEKKAT; HANSSON, 2021). Essa abordagem capacita as equipes de manutenção a analisar os dados coletados para identificar tendências e realizar manutenções proativas antes que falhas ocorram, otimizando assim as operações e melhorando o desempenho do sistema (MENDES; GASPAR; CHARRUA-SANTOS, 2023).

Os AGVs estão interconectados por meio da Internet das Coisas (IoT), possibilitando a comunicação em tempo real com outros dispositivos e sistemas sobre localização, estado da carga e necessidades de manutenção (STÓJ et al., 2023). Essa comunicação integrada não apenas otimiza o fluxo de trabalho, mas também apresenta desafios significativos em relação à segurança cibernética (WAI; LEE, 2023).

A adoção de protocolos de segurança a fim de proteger a comunicação e evitar ataques, reduz os riscos à operação e à integridade dos dados. Medidas como autenticação de usuário e criptografia são essenciais para garantir a proteção dos AGVs e assegurar conformidade com normas de segurança cibernética (JAVED et al., 2021).

2.3 Controladores Lógico Programáveis na Indústria 4.0

Os Controladores Lógicos Programáveis (CLPs) são elementos essenciais na automação dos Veículos Guiados Automaticamente (AGVs), possibilitando o controle eficiente e a comunicação entre seus diversos componentes (OYEKANLU et al., 2020).

A falta de padrões de configuração e o desalinhamento com diretrizes dos fabricantes, como as recomendações da Siemens em relação a certificados de autoridade, elevam a vulnerabilidade de segurança e a probabilidade de falhas operacionais (MASIP-BRUIN et al., 2021).

A adoção de padrões como o OPC-UA (Open Platform Communications Unified Architecture) é uma prática recomendada para garantir a interoperabilidade e a segurança de sistemas automatizados (CAVALIERI, 2021). Sem as devidas configurações de segurança implementadas, os Controladores Lógicos Programáveis (CLPs) presentes nos Veículos Autônomos (AGVs) se tornam extremamente

vulneráveis a ataques cibernéticos (OYEKANLU et al., 2020). Para garantir a proteção adequada dos Controladores Lógicos Programáveis (CLPs) em Veículos Guiados Automaticamente (AGVs), é essencial implementar soluções de segurança robustas e manter as configurações atualizadas constantemente (KUBASAKOVA et al., 2024).

A implementação de práticas recomendadas pelos fabricantes de CLP, como a instalação de certificados digitais, adiciona uma camada adicional de segurança, protegendo contra acessos não autorizados e manipulação maliciosa dos sistemas (HAJDA; JAKUSZEWSKI; OGONOWSKI, 2021). Essa conformidade com as melhores práticas não apenas assegura uma comunicação segura entre os dispositivos, mas também aprimora a gestão dos AGVs, promovendo a continuidade das operações e a integridade do sistema.

3- METODOLOGIA

Os métodos utilizados foram a revisão da literatura e o Design Science Research (DSR). A revisão da literatura foi estruturada em três capítulos abordando os temas relacionados a AGV, CLP e Cibersegurança. Os tópicos foram analisados e forneceram os conceitos teóricos para o desenvolvimento do projeto, a partir da revisão de artigos e livros sobre os temas mencionados.

A revisão da literatura é um método de pesquisa acadêmica, que permite a análise das informações existentes sobre um determinado tema. Segundo Fink (2019), trata-se de uma abordagem que busca identificar, avaliar e integrar as contribuições de estudos prévios, identificando lacunas e direcionando novos trabalhos. Esse método serve para fundamentar a aplicação prática das teorias e identificar onde há espaço para inovação.

O Design Science Research (DSR) é uma abordagem voltada para o desenvolvimento de métodos e soluções que buscam resolver problemas complexos em diversas áreas do conhecimento. Essa metodologia, focada na criação e avaliação de artefatos, tem sido aplicada para lidar com desafios práticos e teóricos na Engenharia Industrial, destacando sua capacidade de gerar soluções baseadas em evidências teóricas e práticas (Goecks et al. 2021).

Promovendo melhorias práticas através da criação e avaliação de soluções, o DSR pode ser aplicado na área da engenharia de software ao desenvolver aprimoramento de segurança de sistemas e criação de novas arquiteturas de

computadores. Na área da gestão organizacional é utilizado para otimizar os processos e melhorar desempenhos. Essas aplicações demonstram a flexibilidade do DSR em diferentes contextos visando a inovação (UYSAL; MERGEN, 2021).

A estrutura metodológica do DSR é composta por cinco fases essenciais, a primeira etapa consiste na identificação do problema, que envolve a compreensão do desafio a ser resolvido. Na segunda etapa foca-se na definição dos objetivos de solução, com a elaboração de critérios que guiarão a criação da solução. Em seguida, na terceira etapa é elaborado o design e desenvolvimento do artefato abrangente a construção da solução proposta. Após, na quarta etapa é apresentada a demonstração da solução, por meio de testes e validações para verificar sua eficácia, e finalizando junto a quinta etapa com a avaliação e comunicação, com a finalidade de analisar os resultados obtidos e compartilhados com os envolvidos no desenvolvimento do projeto (Peffers et al 2007).

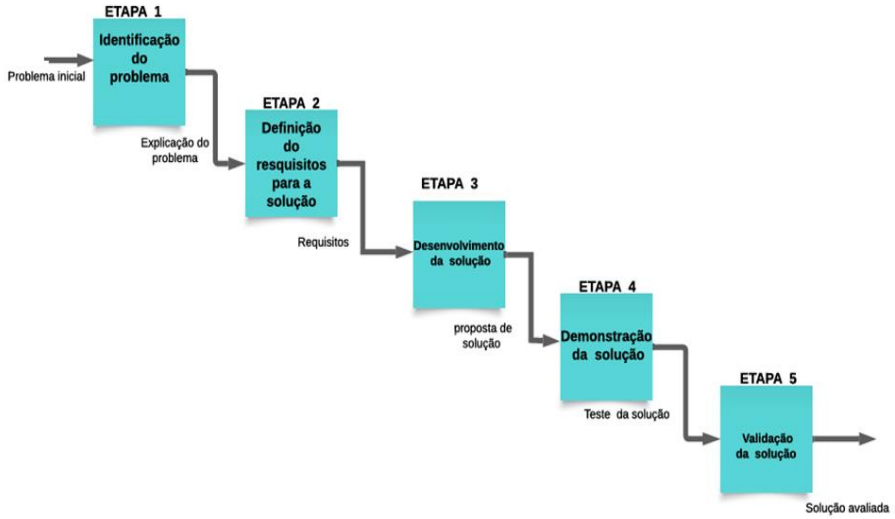

Figura 1: Estrutura das fases do DSR

Fonte: adaptado de Peffers (2007)

Comentado [SADS2]: Padronizar imagem

3.1 Identificação do problema

A primeira etapa do DSR iniciou-se após visitas técnicas a uma empresa fabricante de Veículos Guiados Automatizados (AGVs), alguns problemas foram identificados referentes à segurança dos hardwares e softwares contidos nos AGVs o que gera um comprometimento de acesso a conectividade do equipamento a rede, além do desempenho operacional.

Uma das vulnerabilidades encontradas foi a falta de protocolos de segurança, como autenticação do usuário e criptografia de senhas. Essa falha de segurança causa o risco de acesso indevido ao sistema dos AGVs, expondo a integridade dos dados armazenados.

Outro ponto crítico foi a falta de padrões de configurações aplicados aos CLPs inseridos nos AGVs. A estrutura não atendia as recomendações da fabricante Siemens que sugere a aplicação de certificados de autoridade nas portas de comunicação.

Falta do protocolo HTTPS(Hyper Text Transfer Protocol Secure) para o envio e recebimento dos dados pela Internet, que restringe o desenvolvimento pós-venda de aplicativos e atividades baseadas em análise de dados. A figura 2 apresenta a troca das informações do AGV com o servidor WEB por meio do protocolo HTTPS.

Figura 2: AGV e a interface atual
Fonte: Autores (2024)

3.2 Definições dos requisitos para a solução.

Após as identificações e análises dos problemas a segunda etapa do

Comentado [WL3]: inserir quais pontos serão abordados na melhoria de forma que os resultados venham eliminar as vulnerabilidades/problemas citados no capitulo 4.1

DSR definiu-se os requisitos para serem aplicados na solução em quatro fases conforme indicado na Figura 3.

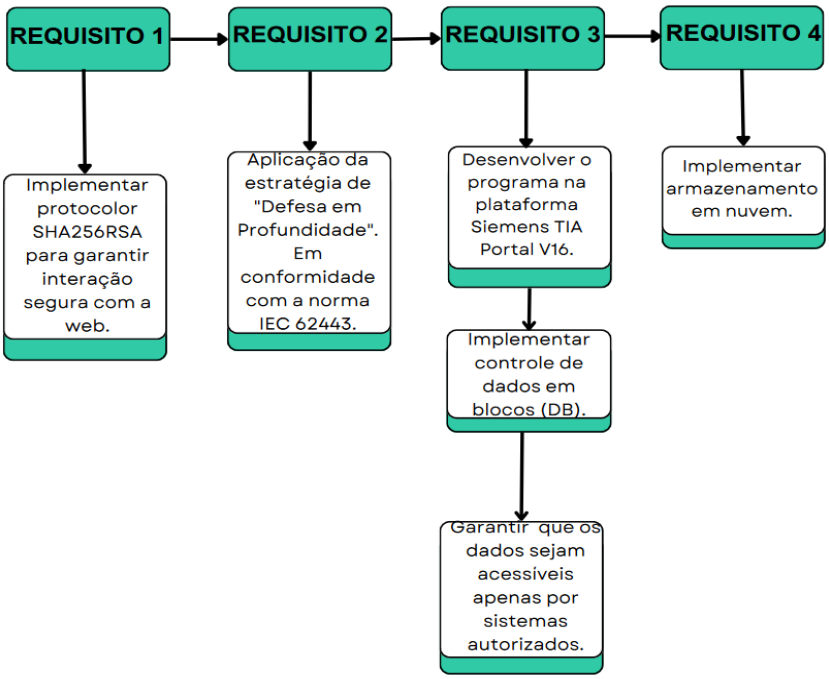

Figura 3: Estrutura da proposta aplicada a solução
Fonte: Autores (2024)

O primeiro requisito visa garantir a interação da segurança dos AGVs com a web, utilizando o protocolo de autoridade SHA256RSA, de acordo com Gollmann (2011), esta função converterá os dados em um único valor de 256 bits, garantindo que qualquer mudança nos dados resultará em uma grande mudança na criptografia. Este protocolo permitirá a criptografia dos dados e autenticação dos usuários, garantindo que apenas sistemas ou usuários autorizados possam acessar informações transmitidas. Este certificado fornece a segurança necessária para proteger o sistema do AGV contra potenciais ameaças, assegurando a confidencialidade das informações transmitidas.

O segundo requisito permite o acesso ao sistema de forma controlada em função da autenticação e criptografia de senhas no hardware dos AGVs. Estes métodos serão complementados pela utilização da estratégia de "Defesa em Profundidade", que consiste em uma abordagem de proteção em várias camadas. Esta estratégia serve para estabelecer defesas contra invasões e garantir a conformidade do sistema com a norma global IEC 62443, que define diretrizes de segurança cibernética para sistemas industriais.

No terceiro requisito será desenvolvido um programa para ser utilizado no CLP responsável pelo controle do AGV, a plataforma utilizada para o desenvolvimento será Siemens TIA Portal V16. Será incluído programas na linguagem de blocos de dados (DB) contento a transmissão das informações do AGV com o objetivo de garantir que todos os dados fundamentais para o funcionamento do veículo estejam disponíveis apenas para os sistemas autorizados e usuários. Neste processo será implementado processos internos de controle e verificação para garantir a integridade das informações.

Por fim, o último requisito será implementado medidas para assegurar o armazenamento de dados do AGV em nuvem, garantindo o acesso remoto às informações coletadas, como o processamento, a integridade, a proteção e a acessibilidade dos dados. Dessa forma será possível monitorar constantemente o AGV, o que elevará a eficiência da manutenção preventiva, reduzindo possíveis falhas inesperadas.

3.3 Desenvolvimento solução

Na terceira etapa do DSR o desenvolvimento da solução iniciou-se com a identificação das vulnerabilidades de segurança nos AGVs, que comprometeram a integridade dos dados e a conectividade. A implementação de protocolos e padrões de segurança tornou-se indispensável para eliminar os riscos. A metodologia empregada baseou-se em requisitos específicos para assegurar a comunicação segura entre os AGVs e a infraestrutura de rede. Este processo envolveu a ativação de protocolos de segurança, a criação de um sistema de autenticação robusto e o desenvolvimento de uma interface de monitoramento, visando garantir a confidencialidade e a integridade dos dados em ambientes industriais.

O primeiro requisito envolveu ativação do protocolo de comunicação por meio da configuração do servidor web na unidade de Controle Lógico Programável (CLP), especificamente na CPU (Central Processing Unit), O protocolo HTTPS foi implementado, restringindo conexões não autorizadas. O certificado de autoridade SHA256RSA foi escolhido, pois oferece segurança, garantindo que qualquer alteração nos dados resulte em modificações significativas na criptografia. Essa escolha foi fundamental para assegurar que apenas usuários e sistemas autorizados possam acessar as informações sensíveis. A Figura 4 ilustra a implementação deste Certificado de Autoridade (CA), demonstrando a segurança aprimorada na troca de dados.

Comentado [p4]: A primeira etapa do requisito

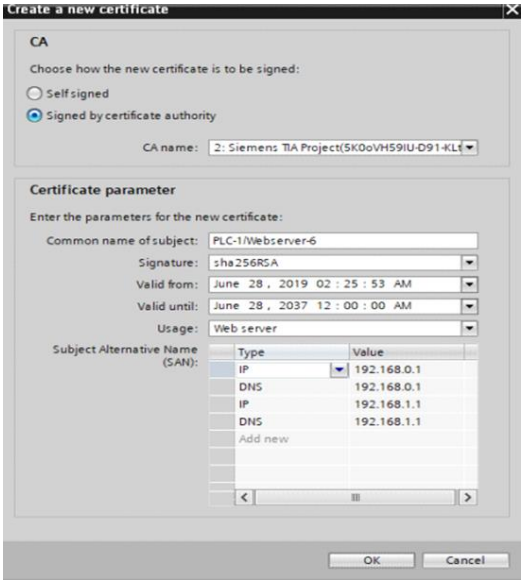

Figura 4: Certificado de autoridade SHA256

Fonte: Autores (2024)

O Certificado de Autoridade (CA) foi exportado da CPU do CLP em múltiplos formatos utilizando o gerenciador de certificados, garantindo compatibilidade com diferentes plataformas. Na sequência, o certificado foi importado e instalado diretamente no navegador web, estabelecendo uma relação de confiança entre o servidor e o cliente. O certificado da interface web foi incorporado ao CLP, assegurando a integridade e a segurança da comunicação. Em seguida, foram criados usuários, definidas senhas e estabelecidos os respectivos privilégios de acesso, como ilustrado na Figura 5.

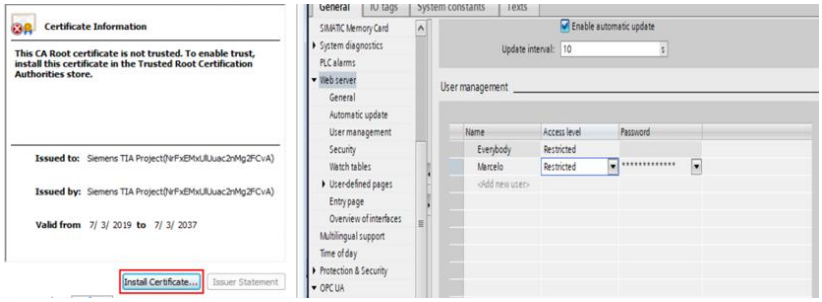

Figura 5. Instalação na web do certificado e criação de usuários e senha

Fonte: Autores (2024)

O segundo requisito, fase de configuração de segurança do CLP, definiu-se um esquema de acesso controlado. Os usuários obtiveram permissão somente para leitura das informações. A autenticação foi assegurada por senhas assinadas e criptografadas, em conformidade com as diretrizes da norma IEC 62443. A implementação de certificados globais para verificação da identidade do usuário garantiu a integridade do sistema, prevenindo acessos não autorizados, conforme demonstrado na Figura 6.

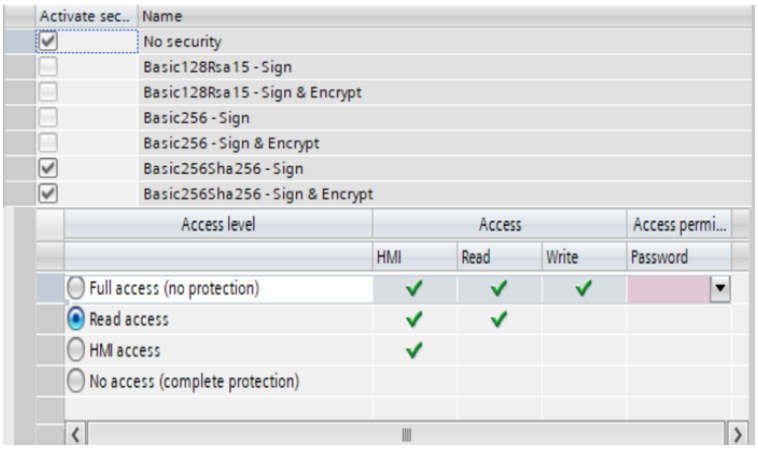

Figura 6. Configuração proteção e segurança.

Fonte: Autores (2024)

No terceiro requisito para desenvolvimento da programação utilizou o software da plataforma Siemens TIA Portal V16, permitindo a programação em linguagem de controle estruturada (*Structured Control Language* - SCL). Uma lista de variáveis

relevantes para o monitoramento dos AGVs foi criada, incluindo parâmetros críticos como estado da bateria e diagnósticos operacionais, direção, horímetros e tração. A implementação de blocos de dados (*Function Block* - FB e *Data Block* - DB) garantiu a captura e armazenamento eficaz dessas informações. Essa escolha de linguagem proporcionou flexibilidade e eficiência na programação, permitindo a replicação do código para diferentes AGVs, como ilustrado na Figura 7, otimizando o gerenciamento de dados operacionais.

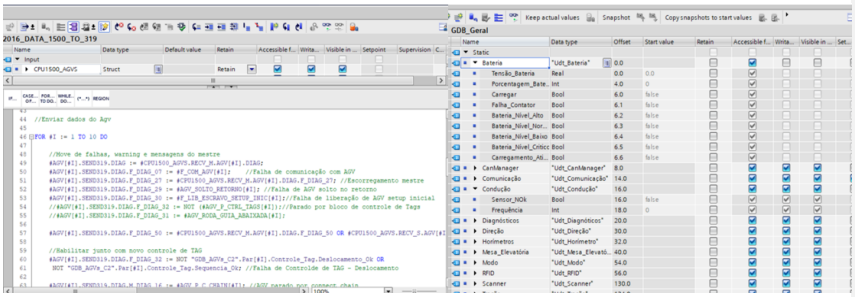

Figura 7: FB - Function Block e Data Block do programa

Fonte: Autores (2024)

No quarto requisito ocorreu a criação de uma interface web no CLP foi realizada utilizando o bloco "WWW", integrado na rotina cíclica (OB1). Esta interface possibilitou a disponibilização dos dados em tempo real para acesso remoto. A configuração da comunicação entre a CPU do usuário e a CPU do CLP garantiu que ambos operassem no mesmo intervalo de IP, facilitando o acesso seguro via navegador. A integração com o Power BI, por meio da URL gerada, permitiu a visualização e análise dos dados coletados, como evidenciado na Figura 8. Essa implementação promoveu a transparência e possibilitou a análise de desempenho junto a manutenção preventiva.

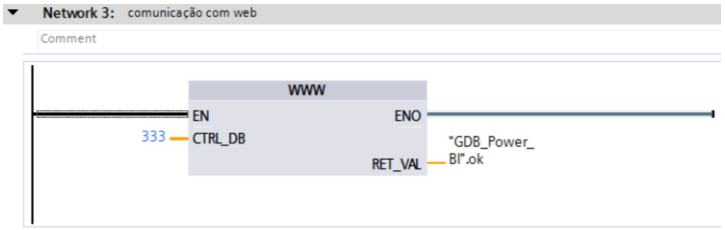

Figura 8: bloco de comunicação com a web.
Fonte: Autores (2024)

3.4 Demonstração da solução

Na quarta etapa do DSR foi realizada a demonstração do funcionamento do projeto, durante a demonstração, o usuário acessou o Power BI e, ao clicar no ícone de atualização, os dados foram incorporados em tempo real aos gráficos do dashboard. A interface dinâmica permitiu que o usuário navegasse facilmente pelos diferentes AGVs, selecionando filtros por mês, dia, número de produção, falhas, nível de bateria e outras variáveis críticas.

A solução apresentou resultados práticos no contexto industrial, oferecendo uma interface intuitiva e segura para a gestão dos AGVs. Além de proporcionar maior transparência nas operações, a integração com o Power BI promoveu uma análise aprofundada dos dados e aprimorou as atividades de manutenção preventiva.

Figura 9: Interface do CLP junto a integração dos dados no Power BI
Fonte: Autores (2024)

3.5 Validação

Na quinta etapa do DSR referente a atividade de avaliação, foram convidados cinco especialistas que participaram desde as primeiras fases do DSR e acompanharam a aplicação da melhoria por sete dias no AGV em uma montadora

automotiva de caminhões. O perfil dos participantes incluiu três líderes de produção, com experiência variando de 15 a 25 anos na empresa, os quais eram responsáveis por monitorar a produção, verificar o funcionamento dos AGVs e registrar quaisquer falhas para direcionamento ao setor de manutenção. Além disso, dois técnicos de manutenção, com 25 anos de experiência, foram incluídos no grupo, sendo encarregados de realizar reparos nos AGVs conforme as ordens de serviço para manutenções corretivas.

Comentado [p5]: Anexar o titulo 3.5 - validação

4.0 Resultados e Discussões

Após a implementação da solução proposta para os AGVs, os resultados operacionais apresentado pelo Power BI com resultados práticos, os especialistas relataram melhorias significativas na eficiência operacional e na manutenção dos equipamentos conforme a figura 10. O Líder de Produção 1 observou uma redução de 25% nos tempos de ciclo, resultando em um fluxo de trabalho otimizado, enquanto o Líder de Produção 2 notou um aumento de 20% na capacidade de transporte, eliminando intervenções manuais desnecessárias.

Figura 10: Resultado dos índices de falhas após a implementação da solução.
Fonte: Autores (2024)

A integração do protocolo de segurança com o Power BI apresentou desafios, como a necessidade de treinamento adicional para a equipe e a harmonização de dados entre os sistemas, conforme destacado pelo Líder de Produção 3. Para aprimorar o monitoramento, especialistas sugeriram a inclusão de um sistema de alerta

em tempo real e a possibilidade de diagnósticos automáticos, que poderiam antecipar falhas. Em relação à interface do sistema, a necessidade de um design mais intuitivo foi consenso entre os especialistas, que propuseram a implementação de tutoriais interativos e um dashboard personalizável. O impacto do projeto na manutenção foi notável, com reduções de até 50% nas falhas recorrentes e melhorias de 35% na eficiência da manutenção preventiva, conforme relatado pelo Técnico de Manutenção 1 e 2.

Com o objetivo de obter dados quantitativos para uma análise mais precisa e comparativa da eficácia da solução implementada, foram elaboradas cinco questões fechadas utilizando uma escala Likert de 1 a 5, variando de "Nada confiável" a "Extremamente confiável", que abordaram aspectos como segurança, eficiência e usabilidade dos AGVs. Além das questões fechadas, foram formuladas cinco questões abertas para aprofundar a compreensão sobre a eficácia da solução e coletar insights qualitativos dos especialistas.

Com base nas respostas obtidas, foi possível avaliar a solução está atendendo às necessidades dos usuários e quais melhorias podem ser feitas para otimizar ainda mais o processo de disponibilidade dos dados a manutenção.

4.1 Validação e avaliação do aplicativo na empresa fabricante ônibus e caminhões

A primeira questão buscou determinar em que grau a implementação da segurança via SHA256RSA aumentou a confiança na integridade dos dados transmitidos 90% dos colaboradores responderam confiável e 10%, não omitiram opinião, desta forma mostra um cenário positivo para a implementação de SHA256RSA, com uma alta taxa de confiança entre os entrevistados.

A segunda questão investigou se a integração com o Power BI facilitou a análise e a visualização de dados operacionais, 100% dos colaboradores concordaram, mostrando um cenário favorável para implementação pois facilitou a visualização dos dados dos AGVs

A terceira questão focou na percepção dos especialistas sobre a redução da ocorrência de falhas não planejadas nos AGVs 100% dos colaboradores concordaram

com uma diminuição significativa das falas recorrentes nos AGVS, desta maneira verificou que a solução teve a eficácia esperada.

A quarta questão avaliou se o sistema atendeu às expectativas em relação à conformidade com a norma IEC 62443, 40% dos colaboradores concordaram que o sistema atendeu porem os outros 60% não opinaram por não saber doque se trata, desta maneira deveremos dar treinamento pros colaboradores que não opinaram.

A quinta questão se recomendariam a aplicação dessa solução para outras linhas de produção que utilizam AGVs. 100% dos colaboradores recomendaria, dando consistência a proposta da solução.

A sexta questão solicitou que os participantes descrevessem os principais benefícios observados após a implementação da solução de segurança 90% comentaram que facilitaram visualizações dos dados gerados pelo agvs. Desta forma auxiliando nas tratativas junto a manutenção.

A sétima questão sobre desafios enfrentados durante a aplicação do sistema e como esses desafios foram superados,100% dos colaboradores responderam que dificuldades foram sanadas pelos treinamentos de utilização, fazendo com que a solução fosse de interação fácil.

A oitava questão pediu sugestões para melhorias na solução proposta, *visando aumentar ainda mais sua eficiência e usabilidade. 80% dos colaboradores sugeriu atualização automático pelo fato de estar usando o power bi gratuito esta função não existe e 20% dos colaboradores comentaram sobre mudanças do layout na máscara do powerbi. estudos serão feitos para futuras melhorias e adequação.*

A nona questão questionou quais impactos foram percebidos na rotina de trabalho após a implementação da solução, 70% dos colaboradores disseram na diminuição de falhas dos agvs reduzindo a intervenção humana, 30% aumento nas rotinas de manutenção preventiva, ficou explicito que os dados foram essências para que a manutenção pudesse ter um norte sobre quais agvs teriam prioridade sobre a preventiva.

A decima questão buscou entender quais características dos AGVs poderiam ser aprimoradas em futuras versões do sistema. 100% dos colaboradores disseram que é necessário coletar mais dados de visualização

As melhorias relatadas pelos especialistas, como a redução nos tempos de ciclo e o aumento na capacidade de transporte, apoiam a literatura existente que discute os avanços na automação industrial e a importância da integração de tecnologias como

IoT e big data no contexto da Indústria 4.0 (BLANCO-NOVOA et al., 2020; RÜSSMANN et al., 2015). No entanto, os desafios identificados durante a integração do protocolo de segurança com o Power BI destacam a complexidade das operações e a necessidade de capacitação contínua dos colaboradores, tema amplamente abordado por Buja et al. (2022) ao discutir a cibersegurança na IIoT.

Comentado [p6]: Anexar o titulo 4- resultado. Alem disso, compilar o teste e a validação .

As sugestões dos especialistas para a inclusão de funcionalidades adicionais, como sistemas de alerta em tempo real, refletem uma preocupação crescente com a proatividade na manutenção, alinhando-se com os princípios de design recomendados para cenários da Indústria 4.0 (HERMANN et al., 2016).

A necessidade de uma interface mais intuitiva também é um ponto crítico, pois interfaces complexas podem limitar a adoção de novas tecnologias, como evidenciado em estudos sobre interação humano-computador (KAGERMANN et al., 2013). O impacto positivo observado na eficiência da manutenção corretiva e preventiva ressalta a relevância da solução proposta para a operação dos AGVs, contribuindo para a literatura sobre automação industrial e oferecendo insights valiosos para futuras implementações (Dempsey, 2017; Piasecki, 2014).

5. Conclusão

A pesquisa realizada não apenas ajuda a demonstrar a necessidade fundamental de integrar a cibersegurança em ambientes industriais, como os AGVs e CLPs, a fim de atender melhor às demandas da indústria 4.0, mas a solução disponibilizada através do Design Science Research ajudou a melhorar a segurança, eficiência e confiabilidade dos AGVs. Com a implementação de protocolos como o SHA256RSA, a integração com ferramentas de análise, como o Power BI e conformidade com normas setoriais, como a IEC 62443, onde a vulnerabilidade foi drasticamente reduzida e o desempenho operacional aprimorado significativamente.

Os resultados obtidos, uma redução de 25% no ciclo de tempo e 50% nas falhas de uso frequente, destacam a abordagem proposta e apontam para a continuidade da ação, conforme sugerido pelos especialistas. Especialmente, melhorias que vão garantir uma integração e acessibilidade com os colaboradores, como alertas em tempo real e uma maior personalização das interfaces, garantindo que as soluções atendam as necessidades dinâmicas da indústria. O estudo não apenas ajuda a esclarecer o caminho para o futuro da indústria, como contribui para a construir um

setor mais seguro, proporcionando informações para futuras pesquisas e implementações.

Referências

ACHOUCH, M. et al. **On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges.** *Applied Sciences*, v. 12, p. 8081, 2022. DOI: 10.3390/app12168081.

AVED, Muhammad Atif; MURAM, Faiz Ul; PUNNEKKAT, Sasikumar; HANSSON, Hans. **Safe and secure platooning of automated guided vehicles in Industry 4.0**.**Journal of Systems Architecture**, v. 121, p. 102309, 2021. ISSN 1383-7621.

CAVALIERI, S. **A proposal to improve interoperability in the Industry 4.0 based on the Open Platform Communications Unified Architecture standard. Computers**, v. 10, n. 6, p. 70, 2021.

COSTA, Andrieli Cristina Aparecida; BUENO, Stefan Antônio.**Proposta de implantação de um sistema automatizado de carregamento em uma multinacional. Anais da Engenharia de Produção**, v. 5, n. 1, p. 281–307, 2024.

DE SORDI, José Osvaldo.**Design Science Research Methodology: Theory Development from Artifacts.**Cham: Springer Nature, 2021. 146 p. ISBN 9783030821562.

HAJDA, Janusz; JAKUSZEWSKI, Ryszard; OGONOWSKI, Szymon.**Security Challenges in Industry 4.0 PLC Systems. Applied Sciences**, v. 11, n. 21, p. 9785, 2021.

JAVED, M. A.; MURAM, F. U.; PUNNEKKAT, S.; HANSSON, H.**Safe and secure platooning of Automated Guided Vehicles in Industry 4.0**.**Journal of Manufacturing Systems**, v. 58, p. 434-448, 2021.

JIANG, Y.; YIN, S.; KAYNAK, O.**Monitoramento de processo de toda a planta supervisionado por desempenho na Indústria 4.0: Um roteiro**. **IEEE Open Journal of the Industrial Electronics Society**, v. 2, p. 21-35, 2021. DOI: 10.1109/OJIES.2020.3046044.

KIFOR, Claudiu Vasile; POPESCU, Aurelian. **Automotive cybersecurity: a survey on frameworks, standards, and testing and monitoring technologies. Sensors**, v. 24, n. 18, p. 6139, 2024.

KRAUS, S.; BREIER, M.; LIM, W. M. **Literature reviews as independent studies: guidelines for academic practice.Review of Managerial Science**, v. 16, p. 2577–2595, 2022. DOI: 10.1007/s11846-022-00588-8.

KUBASAKOVA, Iveta; KUBANOVA, Jaroslava; BENCO, Dominik; KADLECOVÁ, Dominika. **Implementation of Automated Guided Vehicles for the Automation of Selected Processes and Elimination of Collisions between Handling Equipment and Humans in the Warehouse. Sensors**, v. 24, n. 3, p. 1029, 2024.

KUMAR, M.; GUPTA, H. **A review of cyber security challenges and mitigation strategies in Industry 4.0 technologies.**In: **2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)**, Greater Noida, India, 2023. p. 1676-1682. DOI: 10.1109/ICAC3N60023.2023.10541435.

MASIP-BRUIN, X. et al. **Cibersegurança nas cadeias de fornecimento de TIC: principais desafios e uma arquitetura relevante. Sensors**, v. 21, n. 18, p. 6057, 2021.

MENDES, David; GASPAR, Pedro D.; CHARRUA-SANTOS, Fernando; et al. **Synergies between Lean and Industry 4.0 for enhanced maintenance management in sustainable operations: A model proposal. Processes**, v. 11, n. 9, p. 2691, 2023.

MEKALA, S. H.; BAIG, Z.; ANWAR, A.; ZEADALLY, S. **Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications**, v. 208, p. 294-320, 2023. ISSN 0140-3664. DOI: 10.1016/j.comcom.2023.06.020.

PAPADOPOULOS, T. et al.**Towards the next generation of manufacturing: implications of big data and digitalization in the context of Industry 4.0. Production Planning & Control**, v. 33, n. 2-3, p. 101–104, 2021. DOI: 10.1080/09537287.2020.1810767.

PECH, M.; VRCHOTA, J.; BEDNÁŘ, J.**Predictive maintenance and intelligent sensors in smart factory: Review. Sensors**, v. 21, n. 4, p. 1470, 2021. DOI: 10.3390/s21041470.

PEFFERS, K.; TUUNANEN, T.; ROTHENBERGER, M. A.; CHATTERJEE, S. **A design science research methodology for information systems research.Journal of Management Information Systems**, v. 24, n. 3, p. 45–77, 2007. DOI: 10.2753/MIS0742-1222240302.

STÓJ, Jacek et al. **Industrial shared wireless communication systems—Use case of autonomous guided vehicles with collaborative robot**. **Sensors**, v. 23, n. 1, p. 158, 2023.

TUPTUK, N.; HAILES, S.**Security of smart manufacturing systems.Journal of Manufacturing Systems**, v. 47, p. 93-106, 2018. ISSN 0278-6125. DOI: 10.1016/j.jmsy.2018.04.007.

UYSAL, M. P.; MERGEN, A. E.**Smart manufacturing in intelligent digital mesh: Integration of enterprise architecture and software product line engineering. Journal of Industrial Information Integration**, v. 22, p. 100202, 2021. DOI: 10.1016/j.jii.2021.100202.

WAI, Eric; LEE, C. K. M. **Seamless Industry 4.0 integration: A multilayered cyber-security framework for resilient SCADA deployments in CPPS. Applied Sciences**, v. 13, n. 21, p. 12008, 2023.

XU, K. et al. **Advanced data collection and analysis in data-driven manufacturing process. Chinese Journal of Mechanical Engineering**, v. 33, p. 43, 2020. DOI: 10.1186/s10033-020-00459-x.

ZHANG, W.; YANG, D.; WANG, H. **Data-driven methods for predictive maintenance of industrial equipment: A survey. IEEE Systems Journal**, v. 13, n. 3, p. 2213-2227, set. 2019. DOI: 10.1109/JSYST.2019.2905565.