INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS
CAMPUS MANAUS-DISTRITO INDUSTRIAL
BACHARELADO EM ENGENHARIA DE CONTROLE E AUTOMAÇÃO

KAMILA BATISTA DE OLIVEIRA

GERENCIAMENTO DE RISCOS ASSOCIADOS A FALHAS DE PROGRAMAÇÃO E INCOMPATIBILIDADE DE EQUIPAMENTOS EM PROJETOS DE AUTOMAÇÃO: UM ESTUDO TEÓRICO/EXPLORATÓRIO

Manaus-AM
2025

KAMILA BATISTA DE OLIVEIRA

GERENCIAMENTO DE RISCOS ASSOCIADOS A FALHAS DE PROGRAMAÇÃO E INCOMPATIBILIDADE DE EQUIPAMENTOS EM PROJETOS DE AUTOMAÇÃO: UM ESTUDO TEÓRICO/EXPLORATÓRIO

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, Campus Manaus - Distrito Industrial, Curso de Bacharelado em Engenharia de Controle e Automação, como requisito parcial para obtenção do título de Bacharel em Engenharia de Controle e Automação.

Orientador: Prof. Dr. Ailton Gonçalves Reis

Manaus-AM

2025

INSTITUTO FEDERAL DO AMAZONAS
CAMPUS MANAUS DISTRITO INDUSTRIAL
DEPARTAMENTO DE ENSINO SUPERIOR

ATA DE DEFESA PÚBLICA DO TRABALHO DE CONCLUSÃO DE CURSO

Aos 21 dias do mês de maio, de 2025, às 18:30 h, por meio do google meet: meet.google.com/zpx-pdwh-iur, a discente **KAMILA BATISTA DE OLIVIERA** apresentou o seu Trabalho de Conclusão de Curso para avaliação da Banca Examinadora constituída pelos seguintes integrantes: Prof. Fr. Ailton Gonçalves Reis (docente-orientador); MSc. Beatriz Machado dos Santos Bandeira (Membro 1-externo) e Prof. MSc. Juan Gabriel de Albuquerque Ramos (Membro 2-interno). A sessão pública de defesa foi aberta pelo presidente da banca, que apresentou a Banca Examinadora e deu continuidade aos trabalhos, fazendo uma breve referência ao TCC, que tem como título: **GERENCIAMENTO DE RISCOS ASSOCIADOS A FALHAS DE PROGRAMAÇÃO E INCOMPATIBILIDADE DE EQUIPAMENTOS EM PROJETOS DE AUTOMAÇÃO**: UM ESTUDO TEÓRICO/EXPLORATÓRIO. Na sequência, a discente teve até 30 minutos para a comunicação oral de seu trabalho. Cada integrante da banca examinadora fez suas arguições após a defesa do mesmo. Ouvidas as explicações da discente, a banca examinadora, reunida em caráter sigiloso, para proceder à avaliação final, deliberou e decidiu pela APROVAÇÃO com média final 8,8 (oito, oito) ao referido trabalho. Foi dada ciência à discente que a versão final do trabalho deverá ser entregue até o dia 20/06/2025, com as devidas alterações sugeridas pela banca. Nada mais havendo a tratar, a sessão foi encerrada às 19h 40min, sendo lavrada a presente ata, que, uma vez aprovada, foi assinada por todos os membros da Banca Examinadora e pela discente.

Prof. Orientador/Presidente: gov.br Documento assinado digitalmente
AILTON GONCALVES REIS
Data: 22/05/2025 12:15:28-0300
Verifique em https://validar.iti.gov.br

Prof.(a) Avaliador 1: gov.br Documento assinado digitalmente
BEATRIZ MACHADO DOS SANTOS BANDEIRA
Data: 24/05/2025 22:42:49-0300
Verifique em https://validar.iti.gov.br

Prof.(a) Avaliador 2 gov.br Documento assinado digitalmente
JUAN GABRIEL DE ALBUQUERQUE RAMOS
Data: 25/05/2025 01:04:12-0300
Verifique em https://validar.iti.gov.br

Discente: gov.br Documento assinado digitalmente
KAMILA BATISTA DE OLIVEIRA
Data: 26/05/2025 21:55:19-0300
Verifique em https://validar.iti.gov.br

Biblioteca do IFAM – Campus Manaus Distrito Industrial

O48g Oliveira, Kamila Batista de.
Gerenciamento de riscos associados a falhas de programação e incompatibilidade de equipamentos em projetos de automação: um estudo teórico/exploratório / Kamila Batista de Oliviera. - Manaus, 2025.
85 f.: il. color.

Trabalho de Conclusão de Curso (Graduação) – Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, Curso de Engenharia de Controle e Automação, Campus Manaus Distrito Industrial, 2025
Orientadora: Prof. Dr. Ailton Gonçalves Reis.

1. Automação. 2. Confiabilidade – sistemas automatizados. 3. Falhas de programação. 4. Gerenciamento de riscos – projetos de automação. 5. Incompatibilidade de equipamentos. I. REIS, Ailton Gonçalves (Orient.) II. Instituto Federal de Educação, Ciência e Tecnologia do Amazonas. III. Título.

CDD 629.895

Elaborada por Luciana Duarte Ferreira da Silva - CRB11/1010

Dedico este trabalho ao Sr. Rivelino, que sempre me apoiou nos estudos e hoje está me apoiando no céu.

AGRADECIMENTOS

A Deus, que cuida de mim em todos os detalhes da minha vida. Sem Ele, nada disso seria possível, nem mesmo o dom da existência.

Aos meus pais, que sempre estiveram ao meu lado, apoiando meus estudos e fazendo o possível para que eu alcançasse os sonhos que eles não puderam realizar. A dedicação e o amor de vocês foram o alicerce para que eu chegasse até aqui.

Ao meu marido, que sempre cuidou de mim com tanto carinho e me inspira a ser uma pessoa melhor a cada dia. Sua força e incentivo foram fundamentais nesta jornada.

Ao meu filho, que mesmo tão pequeno é uma fonte constante de alegria e motivação, ajudando-me a ir além dos meus limites com seu sorriso e amor incondicional.

Aos professores, que ao longo dessa jornada acadêmica compartilharam não apenas seus conhecimentos, mas também seu entusiasmo e dedicação ao ensino. Em especial, ao professor Prof. Dr. Ailton Gonçalves Reis, meu orientador, por sua paciência, disponibilidade, sabedoria e apoio durante a realização deste trabalho. Sua orientação foi essencial para o desenvolvimento deste projeto e para que eu superasse os desafios ao longo do caminho.

Aos meus colegas de curso, com quem compartilhei não apenas aulas, mas também desafios, aprendizados e momentos de descontração que tornaram essa etapa mais leve e significativa. A convivência com vocês foi enriquecedora, e as trocas de ideias e experiências contribuíram imensamente para o meu crescimento acadêmico e pessoal.

A todos vocês, meu sincero e profundo agradecimento.

"É preciso perseverar, porque Deus escreve o final da história com aqueles que não desistem."
(São Josemaría Escrivá)

RESUMO

O presente trabalho aborda o gerenciamento de riscos associados a falhas de programação e incompatibilidade de equipamentos em projetos de automação, destacando sua relevância para a eficiência, confiabilidade e segurança dos sistemas automatizados. A pesquisa explora as principais causas de falhas, como erros no desenvolvimento de software e problemas de integração entre componentes, além de analisar seus impactos nos processos industriais e no desempenho geral dos projetos. Com base em uma revisão bibliográfica e estudos de caso, foram identificadas estratégias e ferramentas eficazes para mitigar riscos, como testes integrados, validações técnicas, uso de normas específicas (IEC 61508, IEC61511 e ISO 31000) e boas práticas de engenharia. O estudo também enfatiza a importância de um planejamento detalhado e do monitoramento contínuo durante todas as etapas do ciclo de vida dos sistemas. Os resultados indicam que o gerenciamento proativo de riscos contribui significativamente para a redução de custos, o aumento da confiabilidade operacional e a prevenção de falhas críticas e, sendo assim, este trabalho oferece diretrizes práticas para engenheiros e gestores de projetos, reforçando a necessidade de uma abordagem integrada e sistemática no desenvolvimento de soluções em automação.

Palavras-chave: Automação; Confiabilidade; Falhas de Programação; Gerenciamento de Riscos; Incompatibilidade de Equipamentos.

ABSTRACT

This paper addresses the risk management associated with programming failures and equipment incompatibility in automation projects, highlighting its relevance to the efficiency, reliability, and safety of automated systems. The research explores the main causes of failures, such as software development errors and integration issues between components, as well as analyzes their impacts on industrial processes and overall project performance. Based on a literature review and case studies, effective strategies and tools for risk mitigation were identified, such as integrated testing, technical validations, the use of specific standards (IEC 61508, IEC 61511, and ISO 31000), and engineering best practices. The study also emphasizes the importance of detailed planning and continuous monitoring throughout all stages of the systems' life cycle. The results indicate that proactive risk management significantly contributes to cost reduction, increased operational reliability, and the prevention of critical failures. Therefore, this paper offers practical guidelines for engineers and project managers, reinforcing the need for an integrated and systematic approach in the development of automation solutions.

Keywords: Equipment Incompatibility; Industrial Automation; Programming Failures; Reliability; Risk Management

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CLP	Controlador Lógico Programável
DNP3	*Distributed Network Protocol version* 3
E/S	Entrada e Saída
FTA	*Fault Tree Analysis*
FMEA	*Failure Mode and Effect Analysis*
IBM	*International Business Machines Corporation*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
MODBUS	Barramento Modicon
PMI	*Project Management Institute*
PROFIBUS	Barramento de Campo de Processo
RTU	Equipamentos remotos
SCADA	*Supervisory Control and Data Acquisition*
SIL	*Safety Integrity Level*
SIS	Sistemas Instrumentados de Segurança
SSDLC	*Secure Software Development Lifecycle*
SWOT	*Strengths, Weaknesses, Opportunities, Threats*

SUMÁRIO

1 **INTRODUÇÃO**

Nos últimos anos, a automação tem assumido um papel cada vez mais significativo em diversos segmentos industriais, impulsionando melhorias de eficiência, redução de custos e ganhos de produtividade.

De acordo com Oliveira (2024), a automação permite que as tarefas sejam realizadas mais rapidamente e com menos recursos, o que reduz o custo por unidade produzida. Esses sistemas, que integram equipamentos e softwares, são fundamentais para viabilizar a operação de processos complexos em setores como manufatura, energia e logística.

Contudo, a implantação bem-sucedida desses sistemas enfrenta desafios relevantes, especialmente no que diz respeito ao gerenciamento de riscos associados a falhas de programação e incompatibilidade de equipamentos. Tais falhas de programação podem ser decorrentes de equívocos humanos, limitações de software ou problemas de comunicação entre os componentes do sistema automatizado.

A Murrelektronik (2024) destaca que a monitoração de falhas em sistemas é crucial para garantir a eficiência e a confiabilidade no processo de automação industrial. Além disso, a incompatibilidade entre equipamentos, frequentemente causada pela combinação de dispositivos de diferentes fabricantes ou versões, pode comprometer a confiabilidade, a segurança e o desempenho global do sistema. Alves (2020) aponta que problemas de compatibilidade podem surgir quando máquinas descontinuadas ou que não dão suporte para o sistema vigente são incluídas na linha de produção.

Esses desafios, quando não gerenciados de maneira eficaz, podem gerar consequências significativas. Riscos mal administrados em sistemas automatizados podem levar a prejuízos financeiros, atrasos na execução dos projetos e, em casos mais graves, falhas catastróficas nos processos industriais. A Murrelektronik (2024) enfatiza que falhas em equipamentos podem levar a paralisações, atrasos na produção, aumento de custos e, em casos extremos, colocar em risco a segurança dos trabalhadores. Assim, torna-se essencial que as organizações adotem práticas robustas de gerenciamento de riscos e implementem soluções que garantam a compatibilidade e a confiabilidade dos sistemas.

O problema central deste estudo está na dificuldade de prever e mitigar riscos técnicos em projetos de automação, sobretudo quando se lida com tecnologias complexas e múltiplas variáveis. Para lidar com esse desafio, propõe-se uma abordagem estruturada que combine teoria e prática, investigando casos reais de falhas e suas consequências, além de analisar por meio de fontes bibliográficas soluções baseadas em ferramentas de análise de risco e boas práticas de engenharia de automação.

Sendo assim, a pergunta que norteia esse Trabalho de Conclusão de Curso (TCC), pode ser assim apresentada: “diante da relevância do gerenciamento de riscos na automação industrial, como a literatura especializada apresenta estratégias para mitigar falhas de programação e incompatibilidades de equipamentos em projetos de automação?”

Para orientar a investigação proposta neste trabalho, foram formuladas hipóteses baseadas em pressupostos teóricos identificados na literatura especializada. A primeira hipótese considera que a adoção de metodologias de gerenciamento de riscos, como Análise dos Modos de Falha e seus Efeitos[1] (FMEA), Análise da Árvore de Falhas[2] (FTA), Gravata Borboleta[3] *e* Matriz *SWOT*[4], contribui para a redução de falhas operacionais. Essas ferramentas possibilitam a identificação antecipada de pontos críticos no sistema, promovendo ações preventivas capazes de evitar falhas significativas durante a operação.

A segunda hipótese sustenta que a conformidade com normas técnicas, como a ISO 31000, a IEC 61508 e a IEC 61511, promove a melhoria da segurança funcional nos sistemas automatizados. A aplicação dessas diretrizes permite o gerenciamento estruturado dos riscos, minimizando os efeitos de falhas de programação e incompatibilidades entre equipamentos.

A terceira hipótese aponta que a integração entre o desenvolvimento de software e os requisitos de hardware pode reduzir problemas de

[1] Do inglês *Failure Mode and Effects Analysis.*
[2] Do inglês *Fault Tree Analysis*.
[3] Do inglês *Bow-Tie*, é uma metodologia de análise de riscos que representa visualmente as causas e consequências de um evento indesejado, juntamente com as barreiras preventivas e mitigadoras.
[4] Ferramenta de análise estratégica que avalia os ambientes interno e externo de um projeto ou organização, identificando *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças).

incompatibilidade. Nesse sentido, a adoção do modelo Ciclo de Vida de Desenvolvimento de Software Seguro[5] (SSDLC) viabiliza uma abordagem sistemática e segura para garantir a compatibilidade e a interoperabilidade entre os componentes de automação.

Por fim, a quarta hipótese propõe que a utilização de práticas ágeis no desenvolvimento e na manutenção de sistemas automatizados contribui para agilizar a resposta a falhas. A estrutura dinâmica das metodologias ágeis facilita a detecção precoce de erros e possibilita intervenções rápidas e eficazes, diminuindo os impactos negativos sobre a operação.

O objetivo geral deste trabalho é analisar, por meio de pesquisa bibliográfica e documental, as estratégias de gerenciamento de riscos apresentadas na literatura especializada para mitigar falhas de programação e incompatibilidades de equipamentos em projetos de automação industrial. Para alcançar tal finalidade, definem-se os seguintes objetivos específicos:

a) Identificar os principais riscos associados a falhas de programação e incompatibilidade de equipamentos em projetos de automação.

b) Analisar o impacto dessas falhas no desempenho, na segurança e na operação dos sistemas automatizados.

c) Estudar metodologias e ferramentas utilizadas no gerenciamento de riscos em projetos de automação.

d) Avaliar o impacto das estratégias estudadas de mitigação de riscos na melhoria da confiabilidade e continuidade dos projetos de automação.

e) Indicar, a partir da análise da literatura, as estratégias e melhores práticas de gerenciamento de riscos mais viáveis para mitigar falhas de programação e incompatibilidades de equipamentos em projetos de automação industrial.

A presente pesquisa justifica-se pela necessidade de aprofundar o conhecimento sobre como gerenciar, de forma sistemática e efetiva, os riscos inerentes a falhas de programação e incompatibilidade de equipamentos em projetos de automação. Ao apresentar métodos e ferramentas que auxiliem engenheiros de controle e automação a identificar, avaliar e reduzir esses riscos,

[5] Do inglês *Secure Software Development Life Cycle*

este estudo busca contribuir para o aprimoramento da qualidade, segurança e eficiência dos sistemas automatizados.

Sendo assim, a relevância dessa investigação torna-se ainda mais evidente em um cenário de rápida evolução tecnológica, em que a automação está cada vez mais inserida em diferentes setores industriais. A adoção de boas práticas no gerenciamento de riscos e a identificação antecipada de potenciais falhas podem garantir não apenas a competitividade e o sucesso dos projetos de automação, mas também a segurança e a continuidade das operações industriais.

No âmbito acadêmico, este trabalho contribui significativamente para a formação de futuros profissionais da área, fornecendo uma base teórica e prática sobre estratégias eficazes de gerenciamento de riscos. Ao explorar abordagens metodológicas e normativas, o estudo proporciona aos alunos um referencial atualizado e aplicado ao contexto industrial, possibilitando a compreensão dos desafios enfrentados no mercado de trabalho. Ademais, a pesquisa incentiva o desenvolvimento de soluções inovadoras e aprimoradas para a gestão de riscos, ampliando o conhecimento acadêmico e fomentando novas investigações dentro da área.

Os referenciais teóricos utilizados neste TCC seguem as contribuições de autores e instituições que abordam a temática central da pesquisa, ou seja, o gerenciamento de riscos em projetos de automação industrial. As diretrizes estabelecidas pelas normas ISO 31000 (ABNT, 2018), IEC 61508 (IEC, 2010) e IEC 61511 (IEC, 2016) fornecem a base para uma abordagem estruturada e funcional no tratamento de riscos em sistemas automatizados. Além disso, metodologias específicas como a FMEA, abordada por Rozenfeld et al. (2013), e a FTA, discutida por autores como Bertuzzi (2023) e Tractian (2024). A técnica Bow-Tie, explorada por Oliveira (2022) e Chaves (2024). No campo do desenvolvimento de software, o modelo SSDLC, conforme apresentado por Bertuzzi (2023) e IBM (2024). Também são considerados autores que discutem os desafios da integração entre hardware e software, como Alves (2020) e *Rockwell Automation* (s.d.), além de fontes técnicas que abordam a aplicação de práticas ágeis no contexto da engenharia de controle e automação, conforme Fernandes e Rabechini Jr. (2023).

Para a realização deste estudo, foi adotada como metodologia a que respeita uma abordagem qualitativa e exploratória, baseada na revisão bibliográfica e na análise de metodologias selecionadas de gerenciamento de riscos. O estudo utilizou artigos científicos, normas técnicas e publicações especializadas obtidas em bases como Google Acadêmico e sites técnicos do setor.

Os resultados mostram que a aplicação de metodologias estruturadas de gerenciamento de riscos, como FMEA, FTA, *Bow-Tie*, Matriz SWOT e SSDLC, aliadas à conformidade com normas técnicas internacionais, contribui significativamente para a redução de falhas operacionais e a melhoria da segurança funcional em projetos de automação. A análise da literatura evidencia que a integração entre software e hardware, bem como a adoção de práticas ágeis, favorece a compatibilidade dos sistemas e agiliza a resposta a incidentes, promovendo maior estabilidade, eficiência e continuidade operacional. Dessa forma, confirma-se a relevância do gerenciamento de riscos como ferramenta estratégica para mitigar falhas de programação e incompatibilidades de equipamentos em ambientes industriais automatizados.

Espera-se que este estudo contribua para o aprimoramento das práticas profissionais na área de automação, oferecendo diretrizes eficazes para o gerenciamento de riscos em projetos e reforçando a importância da identificação prévia de falhas de programação e incompatibilidades de equipamentos. A adoção das melhores práticas apresentadas poderá ampliar a confiabilidade, a segurança e a continuidade dos sistemas automatizados, impactando positivamente a produtividade e a competitividade industrial.

Por fim, este TCC está organizado em seis capítulos, estruturados da seguinte forma:

O primeiro capítulo corresponde à introdução, na qual são apresentados o tema da pesquisa, a delimitação do problema, os objetivos, as hipóteses formuladas e a justificativa da investigação.

O segundo capítulo aborda os principais riscos associados a falhas de programação e à incompatibilidade de equipamentos em projetos de automação, destacando os impactos dessas falhas na operação, na segurança, no

desempenho e no meio ambiente, além de apresentar exemplos reais que ilustram essas ocorrências.

O terceiro capítulo trata da análise e gerenciamento de riscos, abordando conceitos fundamentais, o processo de gestão, bem como as ferramentas utilizadas, como FMEA, FTA, Matriz de Probabilidade e Impacto, SSDLC, Bow-Tie, Matriz SWOT, ISO 31000, IEC 61508, IEC 61511 e Metodologia Ágil.

O quarto capítulo apresenta a metodologia da pesquisa, com ênfase na revisão bibliográfica e documental. São descritos os critérios de inclusão e exclusão, as fontes utilizadas e os procedimentos de organização e análise dos dados coletados.

O quinto capítulo é dedicado à discussão dos resultados, evidenciando os impactos do gerenciamento de riscos na confiabilidade, continuidade operacional e segurança dos sistemas automatizados, além da apresentação de estratégias de mitigação e melhores práticas para prevenir falhas.

Por fim, o sexto capítulo apresenta as considerações finais do trabalho, destacando os principais achados da pesquisa, as limitações enfrentadas e sugestões para estudos futuros que possam ampliar a compreensão sobre o gerenciamento de riscos em projetos de automação industrial.

2 PRINCIPAIS RISCOS ASSOCIADOS A FALHAS DE PROGRAMAÇÃO E INCOMPATIBILIDADE DE EQUIPAMENTOS EM PROJETOS DE AUTOMAÇÃO

Assim, este capítulo tem como objetivo apresentar e analisar os principais riscos associados a falhas de programação e à incompatibilidade de equipamentos em projetos de automação industrial, destacando seus impactos na operação, segurança, desempenho e meio ambiente. Também são abordados exemplos reais que ilustram como esses riscos se manifestam na prática, reforçando a importância de estratégias eficazes de gerenciamento.

2.1 PRINCIPAIS RISCOS ASSOCIADOS A FALHAS DE PROGRAMAÇÃO

Falhas de programação podem gerar erros operacionais, vulnerabilidades de segurança, paradas inesperadas e perda de eficiência. Esses riscos impactam a confiabilidade dos sistemas automatizados, exigindo estratégias eficazes para preveni-los e garantir a continuidade das operações.

- Erros de Lógica Erros de Lógica

Erros de lógica em sistemas de automação ocorrem quando a sequência de instruções programadas não produz o comportamento esperado, resultando em operações incorretas ou inesperadas. Esses erros podem comprometer significativamente a eficiência e a segurança dos processos automatizados.

> Falhas técnicas podem ser causadas por erros de programação, resultando em comportamentos inesperados dos sistemas automatizados, o que evidencia a necessidade de uma análise minuciosa para garantir a segurança e eficiência operacional (FOGAÇA, et al., 2021, p.8).

- Configurações inadequadas

Parâmetros incorretos definidos no software ou nos dispositivos durante a configuração inicial ou atualizada podem resultar em baixa eficiência do sistema, mau funcionamento ou até mesmo danos físicos aos equipamentos. De acordo com a Flexbor (2024), sistemas automatizados mal configurados

ou com falhas podem resultar em acidentes graves, colocando em risco a saúde e a vida dos trabalhadores. Além disso, a Murrelektronik (2024) destaca que falhas em equipamentos podem levar a paralisações, atrasos na produção e aumento de custos, reforçando a importância de uma configuração precisa e monitoramento contínuo dos sistemas de automação industrial.

- Atualizações Problemáticas

Atualizações de software em sistemas de automação industrial são essenciais para manter a eficiência e a segurança operacionais. Contudo, quando mal planejadas ou executadas, podem introduzir falhas significativas, comprometendo a integridade dos processos automatizados.

Um estudo publicado por Aquino (2021, s/p) alerta que "a falta de atualização e manutenção dos sistemas automatizados pode levar a falhas operacionais e perdas financeiras significativas". Além disso, Teixeira (2016, p.3) destaca que " a implementação, em tempo real, no ambiente industrial, é um grande desafio para a automação". Esses fatores podem resultar em atualizações problemáticas, causando interrupções na produção e comprometendo a segurança do ambiente industrial.

- Integração Defeituosa

A integração defeituosa em projetos de automação industrial pode comprometer significativamente a eficiência e a segurança das operações. Erros nesse processo resultam em falhas de comunicação entre sistemas, interrupções na produção e aumento de custos operacionais.

Segundo a Prado Automação Industrial (2023), a falta de planejamento adequado é um dos principais fatores que levam a integrações mal sucedidas. Sem uma análise completa das necessidades, objetivos e recursos disponíveis, o projeto pode enfrentar custos elevados, atrasos e falhas na execução.

Além disso, a negligência na integração de sistemas é apontada como um erro crítico. Muitas empresas, na pressa de modernizar suas operações, cometem erros que podem comprometer não apenas o sucesso do projeto, mas também a saúde financeira da organização.

2.2 RISCOS ASSOCIADOS À INCOMPATIBILIDADE DE EQUIPAMENTOS

A incompatibilidade entre equipamentos pode comprometer a comunicação entre sistemas, resultando em falhas operacionais, retrabalho e aumento de custos. Integrar corretamente hardware e software é essencial para evitar interrupções e garantir eficiência na automação industrial.

- Conflitos de Comunicação

Conflitos de comunicação em projetos de automação industrial frequentemente surgem quando equipamentos utilizam diferentes protocolos ou padrões de comunicação, resultando em desafios significativos para a integração eficiente dos sistemas.

> A diversidade de protocolos de comunicação pode levar a incompatibilidades entre dispositivos de diferentes fabricantes, dificultando a integração e comprometendo a eficiência dos sistemas de automação (CAVALLIN, 2016, p.49).

Segundo o estudo de Quintana et al. (2024, p.2), os protocolos de comunicação são conjuntos de regras que definem como os dados são transmitidos entre dispositivos em uma rede industrial. Sua função é garantir que diferentes equipamentos e máquinas possam se comunicar de forma eficiente e confiável, possibilitando a automação e o controle de processos industriais. O mesmo autor ainda afirma que “os protocolos de comunicação estabelecem as bases para a troca de informações entre dispositivos, assegurando a interoperabilidade e a eficiência operacional". (id. ibid., p. 14)

A diversidade de protocolos, como Modbus[6], Profibus[7], Ethernet/IP[8], entre outros, pode levar a incompatibilidades quando dispositivos que operam com padrões distintos precisam interagir. Essa falta de interoperabilidade pode resultar em falhas de comunicação, comprometendo a eficiência e a segurança das operações industriais.

---

[6] Segundo o Instituto Metrópole Digital da UFRN, o protocolo Modbus foi introduzido pela Modicon (atualmente Schneider Electric) em 1979 como uma especificação aberta, visando facilitar a operação e manutenção de sistemas de automação industrial.

[7] Profibus: (*Process Field Bus*) protocolo de comunicação em rede usado principalmente para conectar equipamentos de automação, como sensores e controladores, em sistemas industriais.

[8] Ethernet/IP: protocolo de rede industrial baseado em Ethernet que permite comunicação entre dispositivos de automação em tempo real, muito usado em ambientes industriais modernos.

Para mitigar esses conflitos, é essencial adotar soluções que promovam a integração entre diferentes protocolos. O uso de *gateways* de comunicação, que atuam como tradutores entre protocolos distintos, permite que dispositivos heterogêneos se comuniquem de maneira harmoniosa. Além disso, a padronização dos protocolos utilizados na planta industrial pode simplificar a integração e reduzir a ocorrência de conflitos. De acordo com Roisenberg (2023, s/p), "a padronização dos protocolos de comunicação é fundamental para garantir a integração eficiente dos sistemas e a interoperabilidade entre dispositivos de diferentes fabricantes".

Dessa forma, entende-se que a escolha criteriosa dos protocolos de comunicação deve considerar fatores como compatibilidade com os dispositivos existentes, requisitos de velocidade e segurança, além da escalabilidade[9] do sistema. Uma análise detalhada das necessidades específicas da aplicação auxiliará na seleção do protocolo mais adequado, minimizando os riscos de incompatibilidade e garantindo a eficiência operacional. Quintana et al. (2024) ressaltam que a seleção adequada do protocolo de comunicação deve levar em conta as particularidades de cada aplicação, visando otimizar o desempenho e assegurar a compatibilidade entre os dispositivos.

Em suma, a integração eficiente de sistemas de automação industrial requer uma abordagem cuidadosa na seleção e padronização dos protocolos de comunicação, visando minimizar conflitos e assegurar a interoperabilidade entre os diversos dispositivos e equipamentos utilizados.

- Especificações Técnicas Divergentes

Especificações técnicas divergentes em projetos de automação industrial podem levar a incompatibilidades entre componentes, resultando em falhas operacionais e aumento de custos. A falta de padronização nos protocolos de comunicação entre dispositivos de diferentes fabricantes é um exemplo comum desse problema. De acordo a Polo Eletrônica (2022, s/p), "a incompatibilidade de protocolos é um problema comum em redes industriais, especialmente

[9] Em termos gerais, refere-se à capacidade de um sistema, seja ele um negócio, um sistema de software ou um processo, de se expandir ou aumentar sua capacidade para atender a uma demanda crescente, sem que isso comprometa a qualidade, a eficiência ou o custo. (WIKIPEDIA)

quando diferentes dispositivos de diferentes fabricantes precisam se comunicar entre si".

Por isso, procurar alternativas para mitigar esses riscos, é essencial que as equipes de projeto compreendam detalhadamente as especificações técnicas dos sistemas de automação, permitindo uma implementação mais precisa e eficiente. Além disso, a elaboração de um projeto executivo detalhado, que inclua todas as especificações técnicas organizadas em etapas lógicas, é fundamental para orientar a implementação correta dos sistemas automatizados. A adoção de normas técnicas e a observância de padrões estabelecidos também são práticas recomendadas para evitar divergências nas especificações e garantir a compatibilidade entre os diversos componentes do sistema. Conforme destacado pelo portal técnico da área de automação Máxima Serviços Industriais (2024, s/p), "as normas e regulamentações em automação industrial são fundamentais para garantir a segurança dos trabalhadores, a qualidade dos produtos e a eficiência dos processos".

- Problemas de Integração Hardware-Software

Problemas de integração entre hardware e software em projetos de automação industrial podem comprometer a eficiência e a confiabilidade dos sistemas implementados. A falta de compatibilidade entre dispositivos físicos e programas de controle pode resultar em falhas operacionais, aumento de custos e atrasos na produção.

Esta constatação é reverberada por Alves (2019, p.19), ao afirmar que “a integração de hardware e software em sistemas automatizados é um desafio significativo. O mesmo autor ainda enfatiza que "a integração de hardware e software dos sistemas que compõem um módulo arrecadador [...] não aconteceu de forma completa", o que evidencia as dificuldades enfrentadas nesse processo” (id. ibid., p. 19).

Além disso, a ausência de padronização e a utilização de protocolos de comunicação distintos entre dispositivos de diferentes fabricantes podem intensificar os problemas de integração. A falta de interoperabilidade dificulta a comunicação eficiente entre componentes, prejudicando o desempenho do sistema como um todo. (id. ibid.)

2.3 IMPACTOS

As falhas de programação e incompatibilidades de equipamentos podem gerar impactos significativos na produção, segurança e eficiência operacional. Compreender essas consequências é fundamental para mitigar riscos e garantir a estabilidade dos sistemas automatizados.

2.3.1 **Análise do Impacto dos principais riscos associados a falhas de programação**

As falhas de programação em sistemas automatizados representam riscos críticos que podem comprometer a segurança, a operação e a confiabilidade dos processos industriais. Erros em algoritmos, configurações inadequadas ou *bugs*[10] no software podem resultar em consequências significativas para as organizações, afetando diretamente a produtividade, a integridade física dos operadores e a eficiência operacional. De acordo com Silveira (2024, s/p), "uma falha de segurança em um sistema de *e-commerce* [11]pode causar perdas de receitas e de clientes para a empresa usuária dele, por exemplo".

2.3.1.1 Impacto na Segurança

Vedan (2025, s/p) destaca que “falhas críticas em equipamentos são incidentes que não apenas prejudicam o funcionamento imediato de uma máquina, mas que também podem desencadear uma série de falhas no processo produtivo”, afetando a escalada de produção e colocando colaboradores em risco. Assim, em sistemas automatizados podem comprometer a segurança dos trabalhadores e dos processos industriais. A

[10] Um bug é um erro ou falha em um programa, sistema ou hardware que impede o seu funcionamento normal. Podem ser problemas pequenos ou graves, como travamentos ou vazamento de informações.

[11] E-commerce é a abreviação de electronic commerce, termo utilizado para se referir a transações comerciais realizadas por meios eletrônicos, especialmente pela internet. Em uma tradução livre, significa “comércio eletrônico”.

implementação de protocolos de segurança e a conformidade com normas técnicas são essenciais para reduzir riscos e prevenir acidentes.

- Comportamento Imprevisível dos Sistemas:

> Falhas de programação podem gerar comportamentos inesperados em sistemas automatizados, como movimentos imprevisíveis de máquinas industriais, colocando operadores e equipamentos em risco (MURRELEKTRONIK, 2024, s/p).

Por exemplo, um erro no código que controla um robô industrial pode resultar em colisões ou movimentos desordenados, aumentando o potencial de acidentes e comprometendo a segurança do ambiente de trabalho.

- Desativação Involuntária de Dispositivos de Segurança:

> Bugs no software podem desativar sistemas de segurança, como sensores de emergência, alarmes ou sistemas de parada automática, elevando significativamente os riscos de acidentes graves (MURRELEKTRONIK, 2024, s/p).

Essa desativação involuntária compromete a capacidade de resposta rápida a situações de emergência, expondo operadores e equipamentos a danos consideráveis.

- Operação Fora dos Parâmetros de Segurança:

De acordo com a Nepin Engenharia (2023, s/p), "a automação industrial desempenha um papel crucial na redução do impacto ambiental por meio da eficiência energética, otimização de processos e monitoramento ambiental".

Falhas em sistemas de controle industrial podem ter impactos ambientais significativos, especialmente quando resultam na operação de equipamentos fora dos parâmetros de segurança estabelecidos. Por exemplo, um controlador mal programado em uma planta química pode não interromper um processo crítico em caso de anomalias, permitindo o vazamento de substâncias tóxicas ou emissões perigosas. No entanto, quando esses sistemas falham, os efeitos podem ser inversos, levando a danos ambientais significativos. Além disso, Alvarez (2021, s/p) destaca que "[...] a produção industrial causa diversos danos ambientais, trazendo poluição ao ar e solo e emissão de gases de efeito estufa".

Portanto, é essencial garantir a integridade e a confiabilidade dos sistemas de controle para prevenir tais incidentes e proteger o meio ambiente.

2.3.1.1.1 Impacto na Operação

Vulnerabilidades no código de sistemas automatizados podem ser exploradas por agentes mal-intencionados, resultando em danos físicos, financeiros e reputacionais.

Nesse quadro, a Rockwell Automation destaca que,

> [...] vulnerabilidades exploradas por hackers mal-intencionados podem levar a vários resultados operacionais negativos que incluem as preocupações típicas centradas em TI, como violações de dados, e vão além (ROCKWELL AUTOMATION, 2022, s/p).

Além disso, o IBM *Guardium Vulnerability Assessment*[12] identifica pontos fracos que podem ser explorados por agentes mal-intencionados, como hackers que usam *malwares* para comprometer sistemas.

Essas vulnerabilidades podem ser exploradas para obter acesso não autorizado ou causar danos aos sistemas.

- Interrupções Operacionais:

Falhas no código de sistemas automatizados podem causar travamentos ou reinicializações inesperadas, resultando em paradas não programadas e perdas de produtividade.

De acordo com a empresa Infraspeak (©2015 - 2023, s/p), "o *downtime*, ou parada não planejada, é um evento imprevisto que interrompe a operação de um negócio, equipamento ou sistema, resultando em perda de produtividade, receita e satisfação do cliente".

Nesta mesma linha de pensamento, Siqueira (2024, s/p) destaca que "a manutenção preventiva em sistemas de automação é crucial para evitar paradas não programadas, otimizando a eficiência e a segurança das operações". Dessa forma, implementar estratégias de manutenção preventiva e preditiva pode

[12] *IBM Guardium Vulnerability Assessment* é uma solução da IBM voltada para a identificação de vulnerabilidades em bancos de dados. Trata-se de uma ferramenta de avaliação de vulnerabilidades, que realiza varreduras automatizadas, compara configurações com padrões de segurança reconhecidos e gera relatórios detalhados, auxiliando na conformidade com normas

ajudar a identificar e corrigir falhas de software antes que causem interrupções operacionais, garantindo a continuidade dos processos industriais.

- Processos Mal Otimizados:

Um algoritmo com lógica inadequada pode levar a um aumento no consumo de energia, na rejeição de produtos ou em tempos de ciclo ineficientes, reduzindo a competitividade da organização. De acordo com França (2024), a combinação de hardwares especializados e algoritmos otimizados pode resultar em uma redução significativa no consumo de energia. Além disso, ele destaca que a implementação de técnicas de otimização energética é crucial para mitigar impactos ambientais e promover a sustentabilidade no desenvolvimento de tecnologias.

- Sobrecarga ou Mau Funcionamento:

Programações incorretas podem causar desgaste prematuro ou danos permanentes a equipamentos críticos, elevando os custos de manutenção e substituição.

> Um dos principais impactos do desgaste nos equipamentos industriais é a redução da vida útil dos ativos, o que pode resultar em paradas não planejadas, retrabalhos de manutenção, baixa produtividade, perda de eficiência operacional, aumento dos custos operacionais e acidentes de trabalho (ABECOM, 2023, s/p).

Também é destacado pela empresa Rolport Rolamentos (s/d) que fatores como lubrificação inadequada, instalação incorreta, exposição a contaminantes e sobrecarga operacional podem levar ao desgaste prematuro de componentes essenciais. Portanto, é fundamental garantir a precisão na programação dos sistemas automatizados e adotar práticas de manutenção preventiva para assegurar o bom funcionamento dos equipamentos e evitar custos adicionais.

- Dados Inconsistentes ou Corrompidos:

Operações incorretas em sistemas automatizados podem comprometer a integridade dos dados gerados, resultando em informações inconsistentes ou corrompidas. Isso dificulta análises precisas e prejudica a tomada de decisões informadas.

Corroborando com o perigo dessas operações incorretas, a Fortinet (© 2025) destaca que,

> [...] o erro humano oferece um grande risco de integridade de dados para as organizações. Isso geralmente é causado por usuários que

> inserem dados duplicados ou incorretos, excluindo dados, não seguindo protocolos ou cometendo erros com procedimentos implementados para proteger informações (FORTINET, © 2025, s/p).

Além disso, falhas no tratamento de transações de banco de dados ou operações de arquivo podem resultar em dados corrompidos ou inconsistentes, conforme destacado pela In-Com (© 2025, s/p), "Falhas no tratamento de transações de banco de dados ou operações de arquivo podem resultar em dados corrompidos ou inconsistentes".

Acrescenta-se também que a baixa qualidade dos dados pode levar a ineficiências operacionais, exigindo intervenções manuais para corrigir erros e aumentando o tempo e o custo das operações. Sendo assim,

> [...] dados de baixa qualidade podem causar ineficiências significativas. Processos automatizados podem falhar ou gerar resultados incorretos, exigindo intervenções manuais para corrigir erros, o que aumenta o tempo e o custo das operações (MAGALHÃES, 2024, s/p).

Portanto, é crucial implementar práticas robustas de validação e tratamento de erros no desenvolvimento de software para garantir a integridade dos dados e apoiar decisões empresariais eficazes.

2.3.1.2 Casos Reais de Falhas de Programação e Incompatibilidade de Equipamentos em Projetos de Automação

A compreensão dos impactos causados por falhas de programação e incompatibilidades entre equipamentos torna-se ainda mais clara quando observada por meio de situações concretas vivenciadas na indústria. Este item apresenta **casos reais** que evidenciam como esses tipos de falhas podem comprometer significativamente a operação, a segurança e o desempenho de sistemas automatizados. A análise desses exemplos permite refletir sobre os riscos envolvidos e reforça a importância da adoção de práticas e ferramentas eficazes de gerenciamento de riscos em projetos de automação.

- Caso do *Worm Stuxnet*

Segundo Fildes (2010), o Stuxnet foi o primeiro *malware*[13] conhecido a visar diretamente infraestrutura física, demonstrando como ataques cibernéticos podem causar danos concretos a equipamentos industriais por meio da manipulação de parâmetros críticos.

O incidente do Stuxnet exemplifica os graves riscos associados a sistemas de automação vulneráveis. Projetado especificamente para atacar sistemas Controle Supervisório e Aquisição de Dados[14] (SCADA), que controlavam centrífugas em instalações nucleares no Irã, o malware explorava vulnerabilidades não corrigidas no sistema operacional Windows e nos softwares de controle utilizados, configurados por meio de controladores lógicos programáveis (CLP's[15])Siemens.

O Stuxnet comprometia configurações críticas e alterava parâmetros operacionais sem ser detectado, causando danos físicos significativos às centrífugas. A exploração de falhas de segurança, como a falta de atualizações e configurações inadequadas, destacou a importância de práticas robustas de gerenciamento de riscos em sistemas automatizados. Este caso reforça a necessidade de medidas preventivas, como atualizações regulares, monitoramento contínuo e validação de configurações, para garantir a segurança e a confiabilidade de infraestruturas críticas.

- Aeroporto de Denver

Segundo Calleam (2008), um exemplo marcante de falha de programação em projetos de automação ocorreu no sistema automatizado de manuseio de bagagens do Aeroporto de Denver, nos Estados Unidos, durante a década de 1990. Projetado para ser um dos mais avançados da época, o sistema enfrentou atrasos significativos devido a configurações incorretas no controle automatizado.

Os problemas incluíram sensores mal configurados, que geravam leituras imprecisas; parâmetros de controle dos atuadores ajustados de forma inadequada, causando engarrafamentos nas esteiras transportadoras; e

[13]Consiste na abreviação em inglês para *malicious software* usada para designar qualquer tipo de software malicioso desenvolvido para causar danos, roubo de dados ou acesso não autorizado a sistemas. Em uma tradução livre, significa "programa malicioso".
[14] Do inglês *Supervisory Control and Data Acquisition*.
[15] Do inglês *Programmable Logic Controllers*

integração deficiente entre o software de controle e os dispositivos de hardware, resultando em falhas na execução de comandos. Essas falhas comprometeram a eficiência do sistema, geraram custos elevados e se tornaram um exemplo clássico de problemas em projetos de automação mal planejados.

Os impactos no sistema automatizado de bagagens do Aeroporto de Denver foram significativos. A inauguração do aeroporto foi adiada por mais de dezesseis meses, devido à necessidade de corrigir problemas no sistema, resultando em atrasos operacionais. Além disso, os custos do projeto, inicialmente estimados em $186 milhões, ultrapassaram $560 milhões, devido às extensas correções necessárias. Durante os testes iniciais, falhas operacionais também foram evidentes, com bagagens frequentemente danificadas ou perdidas, causadas por colisões e quedas devido a configurações incorretas. Esses impactos ressaltam a importância de um planejamento e validação adequados em projetos de automação.

- Estudo de Caso da ASH Cement PLC

Em um estudo de caso publicado na plataforma ResearchGate[16] em 2016, foi documentado um incidente crítico na ASH Cement PLC[17]. A falha foi decorrente de uma incompatibilidade entre o mapeamento de endereços do cartão de Entrada/Saída (E/S) do CLP e a fiação real no campo do forno de clínquer. Esse problema foi identificado após uma manutenção de rotina, durante a qual o software do CLP foi recarregado com uma tabela de E/S desatualizada. Como resultado, uma válvula de alimentação de combustível foi erroneamente configurada como sinal de alarme de sobrepressão.

A consequência direta foi o disparo de uma parada de emergência automática, interrompendo o processo de calcinação por aproximadamente 10 horas. O custo estimado dessa parada foi de US$ 75.000, impactando significativamente a produtividade e as finanças da empresa.

A análise de causa raiz revelou que a principal falha estava na falta de alinhamento entre os esquemas elétricos (hardware) e a configuração do

[16] Plataforma online para pesquisadores, permitindo o compartilhamento e acesso a artigos acadêmicos, estudos e colaborações científicas.
[17] Empresa do setor de cimento, conhecida por suas operações industriais e soluções em materiais de construção, cujo estudo de caso aborda falhas e soluções em processos produtivos.

software do CLP. Ademais, foram apontadas como vulnerabilidades a ausência de procedimentos formais de controle de mudanças e a insuficiente validação cruzada de documentos antes de cada intervenção.

Este caso ilustra a importância de manter atualizadas as configurações de hardware e software, além de implementar rigorosos processos de verificação e validação para garantir a segurança e a eficiência de sistemas industriais.

2.3.2 **Análise do Impacto dos principais riscos associados à Incompatibilidade de Equipamentos**

De acordo com a Polo Eletrônica (2022, s/p), "erros de comunicação em redes industriais são problemas que podem ocorrer durante a transmissão de dados em sistemas de automação industrial", o que pode levar à paralisação da produção e comprometer a eficiência operacional.

A incompatibilidade de equipamentos em sistemas automatizados é um problema crítico que pode gerar uma série de impactos negativos na operação, segurança e desempenho de processos industriais. Esses riscos surgem quando dispositivos de diferentes fabricantes ou com especificações técnicas divergentes não conseguem se comunicar ou operar de maneira integrada, afetando a eficiência e a confiabilidade dos sistemas.

Além disso, a empresa TS Shara (2024, s/p) destaca que erros de software, incluindo *bugs*, incompatibilidade de atualizações e falhas de sistema operacional são causas comuns de tempo de inatividade, resultando em perdas financeiras e prejuízos à reputação da empresa. Portanto, é fundamental que as empresas adotem padrões e protocolos de comunicação compatíveis e realizem uma análise detalhada das especificações técnicas dos equipamentos antes da implementação, visando minimizar os riscos associados à incompatibilidade e assegurar a eficiência operacional.

2.3.2.1 Impactos na Operação

A ocorrência de falhas de incompatibilidades entre equipamentos pode gerar consequências significativas na operação dos sistemas automatizados. Esses impactos afetam diretamente o desempenho, a continuidade e a eficiência dos processos industriais. A seguir, são apresentados os principais efeitos operacionais observados nessas situações.

- Interrupções Operacionais

> A complexidade de integrar novas tecnologias como Inteligência Artificial e Aprendizado de Máquina em sistemas existentes é alta, principalmente porque muitos equipamentos antigos não são compatíveis com essas inovações (CIM AUTOMAÇÃO, © 2017 – 2024, s/p).

De acordo com a CIM Automação (2024), a incompatibilidade entre equipamentos em sistemas automatizados pode ocasionar falhas de comunicação e interrupções não programadas, comprometendo diretamente a continuidade do processo produtivo. Tais falhas podem levar à paralisação inesperada das operações, reduzindo a eficiência operacional e aumentando o risco de atrasos, perdas produtivas e custos adicionais para a retomada do funcionamento normal dos sistemas.

- Baixa Eficiência

A incompatibilidade entre dispositivos em sistemas automatizados pode impedir que as operações alcancem seu desempenho ideal, resultando em tempos de resposta mais lentos e redução da produtividade. De acordo com Avetis (2024), "uma incompatibilidade pode levar a perdas de produtividade em vez de ganhos".

Além disso, a Psico Smart (©2025, s/p) destaca que "a automação tem se mostrado uma aliada indispensável na busca por produtividade em diversas organizações". Portanto, garantir a compatibilidade entre dispositivos é essencial para otimizar os processos e manter a competitividade no mercado.

- Aumento de Custos Operacionais

De acordo Dexyi (2023, s/p), "erros e falhas na detecção podem gerar desperdícios de materiais e aumento dos custos operacionais devido à necessidade de correção". A necessidade de soluções de integração, como

gateways[18] ou adaptadores, eleva os custos do projeto. Além disso, retrabalhos[19] e paradas frequentes geram despesas adicionais. Portanto, é fundamental garantir a compatibilidade entre os equipamentos e sistemas utilizados para minimizar esses custos adicionais.

2.3.2.2 Impactos na Segurança

A segurança é um dos pilares mais críticos em ambientes industriais automatizados. Falhas de incompatibilidades entre equipamentos podem comprometer diretamente a integridade física dos trabalhadores, além de gerar riscos significativos às instalações e ao meio ambiente. Este tópico aborda os principais impactos que essas falhas podem causar sob a perspectiva da segurança, evidenciando a necessidade de sistemas confiáveis, conformidade com normas técnicas e a adoção de medidas preventivas para evitar acidentes e danos severos.

- Comprometimento dos Sistemas de Segurança

Roisenberg (2024, s/p) destaca que "a escolha de hardware com suporte oficial ao Linux minimiza o risco de incompatibilidade e assegura um melhor desempenho e confiabilidade do sistema". Portanto, garantir a compatibilidade entre os componentes é essencial para manter a eficácia dos sistemas de segurança e proteger os operadores de possíveis perigos.

- Riscos à Integridade Física

A incompatibilidade entre dispositivos em sistemas automatizados pode resultar em falhas operacionais que comprometem a integridade física dos operadores. Por exemplo, a falta de integração adequada entre componentes de diferentes fabricantes pode levar ao funcionamento inadequado de

[18] *Gateways* são dispositivos ou softwares que atuam como pontos de entrada e saída entre duas redes distintas, possibilitando a comunicação entre diferentes protocolos. Em uma tradução livre, podem ser compreendidos como “portões de acesso” ou “concentradores de comunicação”, que permitem a integração entre sistemas que, de outra forma, não se comunicariam diretamente.

[19] Refere-se à necessidade de refazer um trabalho ou parte dele que já foi realizado anteriormente, devido a erros, falhas ou não conformidade com os padrões estabelecidos. É a repetição de atividades em um processo para que o resultado atenda às expectativas de qualidade. Em outras palavras, é fazer algo novamente porque a primeira tentativa não foi satisfatória.

equipamentos pesados, aumentando o risco de acidentes no ambiente de trabalho.

A Norma Regulamentadora nº 12 (NR-12) enfatiza a importância de garantir que máquinas e equipamentos possuam sistemas de segurança eficazes para proteger a saúde e a integridade física dos trabalhadores. O item 12.4.9 da norma estabelece que:

> [...] máquinas e equipamentos que possam representar risco à saúde ou à integridade física, caso sejam acionados por pessoas não autorizadas, devem contar com um sistema que permita o bloqueio dos dispositivos de acionamento. (ABNT, 2022).

Portanto, assegurar a compatibilidade entre dispositivos é essencial para manter a segurança operacional e prevenir acidentes decorrentes de falhas em equipamentos incompatíveis.

2.3.2.3 Impactos Ambientais

De acordo com Filtroil (2025, s/p) a ausência de manutenção preditiva pode resultar em riscos de acidentes de trabalho e danos ao meio ambiente. A incompatibilidade entre equipamentos em sistemas automatizados pode resultar em falhas operacionais que comprometem processos críticos, levando a danos ambientais significativos. Por exemplo, falhas em equipamentos industriais podem causar vazamentos de substâncias perigosas, poluição do solo e da água, além de emissões atmosféricas nocivas. Portanto, é essencial garantir a compatibilidade entre os equipamentos e implementar programas de manutenção preventiva para mitigar esses riscos e proteger o meio ambiente.

2.3.2.4 Impactos no Desempenho

As incompatibilidades entre equipamentos não afetam apenas a segurança e a operação dos sistemas automatizados, mas também exercem influência direta sobre o seu desempenho. Esses impactos comprometem indicadores essenciais como confiabilidade, qualidade e dificuldade em expandir ou atualizar sistemas. A seguir, são apresentados os principais efeitos negativos

no desempenho dos sistemas, com base na literatura técnica e em estudos de caso.

- Perda de Confiabilidade

A incompatibilidade entre equipamentos em sistemas automatizados pode aumentar a probabilidade de falhas, comprometendo a confiabilidade geral das operações. Segundo publicação técnica da Elite Soluções em Corte e Solda (2024, s/p), empresa especializada em automação industrial, “[...] as empresas precisam desenvolver estratégias eficientes para garantir a disponibilidade e confiabilidade dos sistemas automatizados, minimizando tempo de inatividade e perdas de produção.”

Portanto, garantir a compatibilidade entre os equipamentos é essencial para manter a confiabilidade e eficiência dos sistemas automatizados.

- Redução da Qualidade do Produto

A falta de integração eficiente entre sistemas e processos produtivos pode levar a inconsistências que prejudicam a qualidade final dos produtos.

> A falta de integração de sistemas é um dos maiores obstáculos para uma comunicação eficaz dentro das empresas. Em ambientes onde cada departamento opera com sistemas isolados, o fluxo de informações é interrompido, e a troca de dados entre setores se torna lenta e ineficiente. (SKYONE, 2023, s/p).

Essa desconexão resulta em silos de informação, dificultando a colaboração e aumentando o retrabalho, o que impacta diretamente na consistência e qualidade dos produtos finais.

> Quando os sistemas não são integrados, os dados gerados por cada sistema do seu negócio ficam parados ali, surgindo a necessidade de transferi-los manualmente sempre que outro sistema precise acessá-los ou um relatório precise ser feito. (COSTA, 2023, s/p).

Esse processo manual aumenta o risco de erros e inconsistências, comprometendo a qualidade do produto. Portanto, a integração eficiente é essencial para assegurar processos produtivos consistentes e a excelência na qualidade dos produtos.

- Dificuldade em Expandir ou Atualizar Sistemas

Sistemas compostos por componentes incompatíveis enfrentam desafios significativos ao serem atualizados ou expandidos, limitando sua capacidade de adaptação a novas demandas tecnológicas.

> A falta de atualizações de software e a obsolescência das linguagens utilizadas deixam esses sistemas vulneráveis a ataques cibernéticos e dificultam a implementação de novas funcionalidades, o que compromete a eficiência operacional e a competitividade da empresa. (COSTA, 2024, s/p).

Logo, garantir a compatibilidade entre os componentes é essencial para facilitar upgrades e expansões, permitindo que os sistemas acompanhem as evoluções tecnológicas e atendam às novas demandas do mercado.

2.3.2.5 Exemplos Reais

Na modernização de uma subestação elétrica no Brasil, o projeto enfrentou falhas operacionais devido à incompatibilidade entre equipamentos de diferentes fabricantes. O objetivo era integrar novos sistemas de supervisão e controle com dispositivos de proteção existentes, mas o processo foi comprometido por diferenças técnicas.

Os principais problemas incluíram a utilização de diferentes protocolos de comunicação entre os sistemas, como os relés de proteção operando com o protocolo IEC 61850 (um padrão internacional para comunicação em subestações elétricas) e o sistema SCADA, utilizando a versão 3 do Protocolo de Rede Distribuídora[20] (DNP3) e o Modbus. Essa diversidade de padrões impossibilitou a comunicação direta entre os equipamentos. Além disso, o hardware incompatível exigia adaptações, como a transição de cabos de cobre para conexões de fibra óptica. Por fim, falhas no mapeamento de dados entre dispositivos causaram erros de monitoramento e alarmes falsos.

> Com diferentes fabricantes, diferentes protocolos de comunicação foram criados, gerando dificuldades no projeto de subestações e na

[20] Do inglês *Distributed Network Protocol version* 3, consiste em um protocolo de comunicação utilizado principalmente em sistemas de automação de serviços públicos, como redes elétricas, estações de tratamento de água e gás. Projetado para comunicação confiável e eficiente entre equipamentos remotos (RTU's) e centros de controle, mesmo em ambientes com baixa largura de banda ou conexões instáveis.

> posterior modernização das mesmas, já que equipamentos de fabricantes distintos não 'falavam a mesma língua'. (RODRIGUES, 2013, s/p).

Esse problema se reflete diretamente na necessidade de adaptações que elevam os custos e aumentam a complexidade da integração.

Dessa forma, observa-se que os riscos associados a falhas de programação e incompatibilidades de equipamentos podem gerar impactos significativos em diversas dimensões, como operação, segurança, desempenho e custos.

Casos como o citado demonstram que a ausência de padronização, planejamento e integração entre sistemas pode comprometer severamente os resultados esperados em projetos de automação industrial. Compreender esses riscos é essencial para que se possam adotar medidas preventivas eficazes.

Nesse contexto, o próximo capítulo abordará os fundamentos do gerenciamento de riscos, suas etapas, metodologias e ferramentas aplicáveis, com o objetivo de demonstrar como esses instrumentos podem ser utilizados para minimizar falhas e promover maior confiabilidade e segurança nos sistemas automatizados.

3 **ANÁLISE E GERENCIAMENTO DE RISCOS**

Esse capítulo tem como objetivo apresentar os fundamentos do gerenciamento de riscos em projetos de automação industrial, abordando sua definição, importância, etapas do processo e as principais ferramentas e normas utilizadas. Busca-se evidenciar como essas estratégias podem contribuir para a identificação, avaliação e mitigação de falhas de programação e incompatibilidades de equipamentos, promovendo maior segurança, eficiência e confiabilidade nos sistemas automatizados.

A análise e o gerenciamento de riscos são disciplinas essenciais para o sucesso de qualquer projeto, especialmente em setores como a automação. Nessa área, a incerteza e a imprevisibilidade têm o potencial de gerar impactos significativos na execução e nos resultados do projeto.

Como afirma Drucker (1980, p.12), "O maior perigo em tempos de turbulência não é a turbulência em si, mas agir com a lógica do passado." Essa reflexão ressalta a necessidade de adaptação e atualização constante na gestão de riscos, garantindo que estratégias ultrapassadas não comprometam a eficácia do projeto.

O mesmo autor ainda salienta que um gerenciamento de riscos eficiente não se limita à mitigação de possíveis danos; ele também permite identificar e explorar oportunidades que podem surgir ao longo do processo, contribuindo para a otimização dos recursos e o alcance dos objetivos estabelecidos.

3.1 DEFINIÇÃO DE RISCO E IMPORTÂNCIA DO GERENCIAMENTO

A gestão de riscos é definida por Pritchard (1996) como "o processo de identificar, avaliar e controlar riscos, com o objetivo de minimizar ou maximizar suas implicações em um projeto".

Nesse sentido, o mesmo autor preconiza que o autor o risco é descrito como qualquer evento ou condição incerta que, se ocorrer, pode afetar negativamente os objetivos de um projeto, como escopo, cronograma, custo ou qualidade.

Esse conceito é de vital importância para a construção de um planejamento robusto, que minimize falhas, especialmente em sistemas de automação onde os erros podem resultar em sérios prejuízos.

De acordo com o Centro de Formação de Servidores de Pernambuco (CEFOSPE, 2020), o gerenciamento de riscos é indispensável para assegurar o sucesso de projetos, especialmente em contextos de alta complexidade, como os projetos de automação. Nesse sentido, a gestão de riscos deve ser uma prática contínua, não restrita à fase de planejamento, mas integrada a todas as etapas do ciclo de vida do projeto. Além disso, destaca que o êxito de um projeto está intrinsecamente relacionado à capacidade de identificar e mitigar riscos desde as fases iniciais.

3.2 PROCESSO DE GERENCIAMENTO DE RISCOS

O processo de gerenciamento de riscos envolve várias etapas, conforme descrito pelo Pritchard (1996), que delineia a abordagem de cinco fases: identificação dos riscos, análise dos riscos, planejamento das respostas aos riscos, implementação das respostas e monitoramento e controle dos riscos.

A figura 1 a seguir apresenta um fluxograma cíclico de gestão de riscos, composto pelas cinco etapas principais,

Figura 1 — Gestão de risco

Fonte: UDS (2025).

1. Identificação dos Riscos: O primeiro passo é identificar os riscos potenciais que podem impactar o projeto. Segundo Hillson (2009), a identificação de riscos é uma atividade colaborativa e dinâmica, que envolve a análise de toda a documentação do projeto e entrevistas com a equipe envolvida. Nesse sentido, a identificação de riscos deve ser realizada ao longo de todo o ciclo de vida do projeto, à medida que novos fatores podem surgir e impactar os objetivos do projeto.

2. Análise de Riscos: Após a identificação, os riscos devem ser analisados para avaliar a probabilidade de sua ocorrência e o impacto que teriam caso se materializassem. Pritchard (1996) descreve a análise de riscos como uma etapa crítica, que deve ser dividida em análise qualitativa e quantitativa. A análise qualitativa envolve a avaliação do risco com base em sua probabilidade e impacto, enquanto a análise quantitativa, utilizando ferramentas como simulações ou modelos matemáticos, permite estimar os efeitos financeiros e operacionais dos riscos identificados.

3. Planejamento de Respostas aos Riscos: Esta fase envolve a elaboração de estratégias para lidar com os riscos identificados. De acordo com Schwalbe (2006), as respostas podem ser classificadas em estratégias para evitar, mitigar, transferir ou aceitar os riscos. Logo, a escolha da estratégia depende da natureza do risco e do impacto potencial no projeto.

Por exemplo: em projetos de automação, é comum adotar medidas de mitigação para reduzir o impacto de falhas de programação e incompatibilidade de equipamentos, como o uso de redundância e testes de integração.

4. Implementação das Respostas: após o planejamento das respostas, é crucial garantir que as ações sejam implementadas de forma eficiente. Kerzner (2006) observa que a implementação efetiva requer um acompanhamento contínuo das ações planejadas, o que pode ser facilitado por ferramentas de controle de projetos e relatórios de progresso.

5. Monitoramento e Controle dos Riscos: A última fase envolve o monitoramento contínuo dos riscos identificados e a adaptação das estratégias de resposta quando necessário. Segundo Müller e Turner (2010), o monitoramento eficaz dos riscos envolve não apenas o acompanhamento dos

riscos conhecidos, mas também a identificação de novos riscos que possam surgir ao longo da execução do projeto.

3.3 FERRAMENTAS PARA GERENCIAMENTO DE RISCO

A aplicação de ferramentas adequadas é essencial para garantir um gerenciamento de riscos eficiente em projetos de automação industrial. Cada método possui abordagens específicas que auxiliam na identificação, análise e tratamento dos riscos em diferentes etapas do projeto. Nesta seção, serão apresentadas algumas das principais ferramentas utilizadas nesse contexto, como a Análise de Modos de Falha e FMEA, FTA, a Matriz de Probabilidade e Impacto, os SSDLC e suas contribuições para a confiabilidade dos sistemas. Cada uma dessas ferramentas será detalhada nos próximos subitens, destacando sua aplicação, metodologia e benefícios no contexto da automação.

3.3.1 **Análise de Modos de Falha e Efeitos (FMEA)**

A FMEA é uma metodologia sistemática utilizada para identificar, avaliar e prevenir falhas potenciais em produtos, processos ou sistemas, analisando seus modos de falha e os efeitos correspondentes.

De acordo com o *Institute for Healthcare Improvement* [21](IHI, 2023), a FMEA "é uma ferramenta para conduzir uma análise sistemática e proativa de um processo no qual podem ocorrer danos".

Embora originada no setor da saúde, essa definição é amplamente aplicável ao contexto industrial, onde a FMEA se destaca como uma metodologia eficaz para antecipar modos de falha potenciais e evitar suas consequências em sistemas automatizados. O IHI (2023) certifica ainda que essa abordagem permite que equipes multidisciplinares antecipem possíveis falhas e implementem ações preventivas para mitigar riscos, garantindo maior confiabilidade e segurança nas operações.

[21] *Institute for Healthcare Improvement* (IHI) é uma organização sem fins lucrativos, sediada nos Estados Unidos, voltada para a melhoria da qualidade dos serviços de saúde em âmbito global. Em uma tradução livre, seu nome significa “Instituto para a Melhoria dos Cuidados em Saúde”. O IHI é conhecido por desenvolver e disseminar metodologias de melhoria contínua.

3.3.1.1 Aplicação da FMEA em Projetos De Automação

A FMEA tem sido amplamente utilizada para aprimorar a confiabilidade e a qualidade em processos industriais. Silva e Gagno Júnior (2011) aplicaram as técnicas FTA e FMEA na análise de falhas em ativos de automação de processos na siderúrgica ArcelorMittal Tubarão, visando aumentar a confiabilidade e disponibilidade operacional.

Em outro estudo, Laurenti, Rozenfeld et al. (2012) avaliaram a aplicação dos métodos FMEA e Revisão de Projeto Baseada em Modos de Falha[22] (DRBFM) no processo de desenvolvimento de produtos em uma empresa de autopeças, destacando a importância da combinação de recursos, trabalho em equipe multidisciplinar e formação de competências para o sucesso da aplicação desses métodos. O DRBFM é uma abordagem complementar à FMEA que enfatiza a revisão detalhada das mudanças realizadas em um projeto, com foco especial na prevenção de falhas decorrentes dessas alterações.

3.3.1.2 Metodologia da FMEA

De acordo com Rodrigues (2004, p.189), a implementação da FMEA envolve etapas como a identificação dos modos de falha potenciais, análise de seus efeitos, determinação das causas, avaliação da severidade, ocorrência e detecção, e a priorização dos riscos para a definição de ações corretivas. Essa abordagem permite uma análise qualitativa dos riscos, auxiliando na tomada de decisões para a melhoria contínua dos processos.

De acordo com o mesmo autor, "a Análise de Modos de Falhas e Efeitos é uma ferramenta que auxilia as organizações a identificar, priorizar e tratar riscos, proporcionando maior confiabilidade e eficiência nos processos produtivos" (id. ibid., p. 189).

[22] Do inglês *Design Review Based on Failure Mode* (DRBFM) consiste numa metodologia desenvolvida pela Toyota, voltada para a análise detalhada de projetos com foco na identificação e prevenção de falhas. O DRBFM é utilizado principalmente para avaliar modificações em projetos já existentes, concentrando-se em mudanças e seus possíveis impactos nos modos de falha.

Dessa forma, essa metodologia ajuda a identificar as falhas mais críticas e a implementar ações corretivas de forma proativa, garantindo a continuidade e a eficácia das operações.

3.3.1.3 Benefícios da FMEA

A aplicação da FMEA em projetos de automação proporciona diversos benefícios, tais como:

- Prevenção de Falhas: A FMEA permite identificar modos de falha potenciais antes que eles ocorram, possibilitando a implementação de ações preventivas. Segundo a Siembra (s/d), "a FMEA é uma ferramenta eficaz para antecipar falhas potenciais e tomar medidas preventivas que garantam a continuidade e segurança dos processos".
- Melhoria da Qualidade: A metodologia contribui para a melhoria contínua dos processos, aumentando a satisfação dos clientes. De acordo com a Tagout (© 2020; s/p), "a FMEA ajuda a identificar falhas críticas que comprometem a qualidade, permitindo que as empresas se concentrem em ações corretivas e preventivas".
- Redução de Custos: Prevenir falhas potenciais evita custos elevados de reparo ou substituição. O Instituto Kaizen (s/d) afirma que ao mapear os modos de falha possíveis e as respectivas causas, as organizações conseguem reduzir os custos a erros associados e fortalecer a segurança, a qualidade e a eficiência das suas operações.

3.3.2 **Análise de Árvore de Falhas (FTA)**

A FTA é uma metodologia dedutiva e sistemática utilizada para identificar as causas potenciais de falhas em sistemas complexos. Por meio de diagramas lógicos, a FTA permite mapear as combinações de eventos que podem levar a um evento indesejado, facilitando a compreensão das interações entre componentes e a adoção de medidas preventivas. De acordo com a Corporação Internacional de Máquinas de Negócios[23] (IBM) (IBM, 2024), uma das maiores empresas globais de tecnologia e inovação em soluções de software e sistemas, a FTA é definida como "uma metodologia dedutiva que parte do topo para identificar a causa de um evento indesejado em um sistema complexo" (IBM, 2024, s/p).

[23] Do inglês *International Business Machines Corporation*

Essa abordagem permite visualizar a relação entre falhas em subsistemas e o evento principal, contribuindo para a identificação de causas-raiz e a elaboração de estratégias de mitigação eficazes. Essa abordagem auxilia gestores e engenheiros a identificar modos potenciais de falha e a probabilidade de cada um, contribuindo para análises de segurança e confiabilidade.

3.3.2.1 Aplicação da FTA em Projetos de Automação

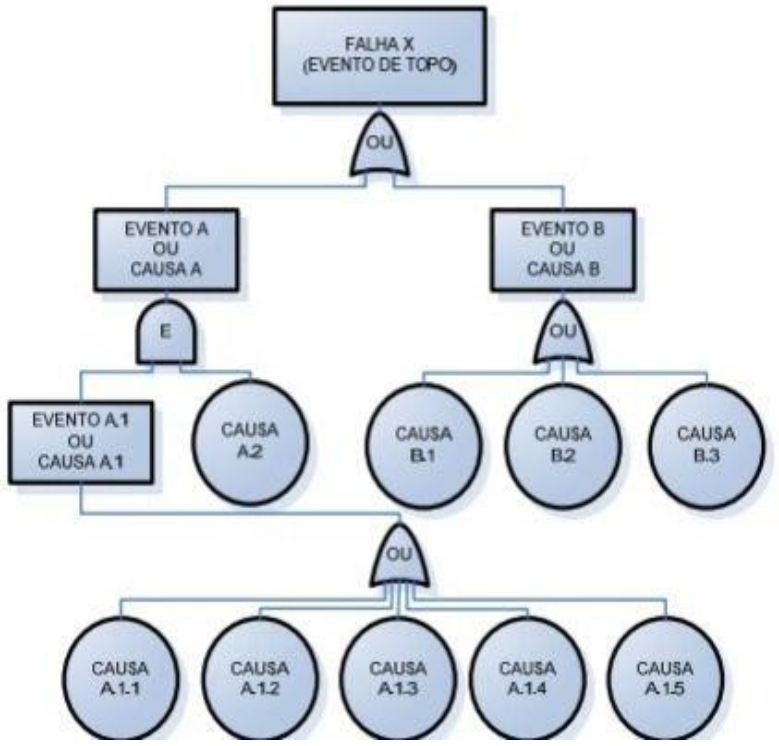
Em projetos de automação, a FTA é particularmente valiosa para analisar falhas de programação e incompatibilidades de equipamentos. Silva e Gagno Júnior (2011) destacam a aplicação integrada das técnicas FTA na análise de falhas em ativos de automação de processos. Para os mesmos autores, a partir da aplicação das técnicas FTA e FMEA, foram definidos pontos de maior relevância e criticidade, resultando em planos de ação para mitigação das falhas potenciais.

3.3.2.2 Metodologia da FTA

Segundo a IBM a FTA é uma metodologia dedutiva e sistemática utilizada para identificar as causas potenciais de falhas em sistemas complexos. Por meio de diagramas lógicos, permite mapear as combinações de eventos que podem levar a um evento indesejado, facilitando a compreensão das interações entre componentes e a adoção de medidas preventivas.

Sendo assim, a construção de uma árvore de falhas inicia-se com a definição do evento indesejado (evento de topo) e, subsequentemente, identifica-se os eventos intermediários e básicos que podem levar a esse evento, utilizando portas lógicas como "E" e "OU" para representar as interações entre as causas. O Diagrama 1 ilustra essa análise, evidenciando a estrutura lógica e hierárquica descrita.

Diagrama 1 — Exemplo de estrutura de FTA



Fonte: Silva e Gagno Jr (2011).

Conforme descrito por Vedan (2025), o método consiste em um processo gráfico, lógico e dedutivo que tem início em um evento indesejado previamente definido (evento topo) e, a partir dele, explora-se sistematicamente as possíveis causas em nível de sistema.

A FTA é amplamente utilizada em diversas indústrias, incluindo aeroespacial, nuclear, química e petroquímica, devido à sua eficácia na identificação de falhas potenciais e na melhoria da confiabilidade dos sistemas. Segundo o Infraspeak (2023, s/p), "uma análise de árvore de falhas é uma abordagem sistemática que permite identificar a causa raiz de uma falha através de um diagrama".

Ao aplicar a FTA, as organizações podem antecipar problemas potenciais e implementar medidas preventivas, garantindo operações mais seguras e eficientes.

3.3.2.3 Benefícios da FTA

A aplicação da FTA em projetos de automação proporciona diversos benefícios, tais como:

- Identificação de Causas-Raiz: A FTA permite uma compreensão aprofundada das causas fundamentais das falhas, facilitando a implementação de soluções eficazes.

> O FTA fornece uma representação visual dos fatores e eventos contribuintes que podem levar a uma falha do sistema, facilitando a compreensão das interações complexas entre os componentes do sistema (IBM, 2023, s/p).

- Prevenção de Falhas: o mapear as combinações de eventos que levam a falhas, a FTA auxilia na adoção de medidas preventivas que aumentam a confiabilidade do sistema.

> Ao decompor sistematicamente sistemas complexos nos seus componentes individuais, a FTA permite que os gestores de manutenção identifiquem e priorizem os potenciais modos de falha de forma mais eficaz (IBM, 2023, s/p).

- Melhoria Contínua: A análise sistemática das falhas contribui para o aprimoramento contínuo dos processos e sistemas de automação. A Infraspeak (2023) observa que uma árvore de falhas permite analisar uma única ocorrência indesejada, mas também pode ser usada sistematicamente para avaliar o funcionamento de um conjunto de componentes, o que torna essa ferramenta muito versátil.

A Análise da Árvore de Falhas é uma ferramenta poderosa no gerenciamento de riscos em projetos de automação, especialmente no que tange a falhas de programação e incompatibilidade de equipamentos. Sua aplicação, conforme mostrado por Silva e Gagno Júnior (2011), pode resultar em aumentos significativos na confiabilidade e disponibilidade operacional dos sistemas automatizados.

3.3.3 **Matriz de Probabilidade e Impacto**

Minetto (2019) afirma que a Matriz de Probabilidade e Impacto é uma ferramenta amplamente utilizada no gerenciamento de riscos para avaliar e priorizar potenciais problemas em projetos. Ela permite classificar os riscos com base na probabilidade de ocorrência e no impacto que podem causar, facilitando a tomada de decisões sobre quais riscos necessitam de maior atenção.

3.3.3.1 Aplicação da Matriz de Probabilidade e Impacto em Projetos de Automação

Em projetos de automação, a identificação e mitigação de riscos associados a falhas de programação e incompatibilidade de equipamentos são cruciais. A Matriz de Probabilidade e Impacto auxilia na priorização desses riscos, permitindo que a equipe de projeto direcione esforços para as áreas mais críticas.

Sendo assim,

> [...] a Matriz de Riscos ou Matriz de Probabilidade e Impacto é uma ferramenta de gerenciamento de riscos que permite de forma visual identificar quais são os riscos que devem receber mais atenção. (MINETTO, 2019, s/p).

Essa visualização facilita a tomada de decisões e a implementação de medidas preventivas para tratar os riscos identificados.

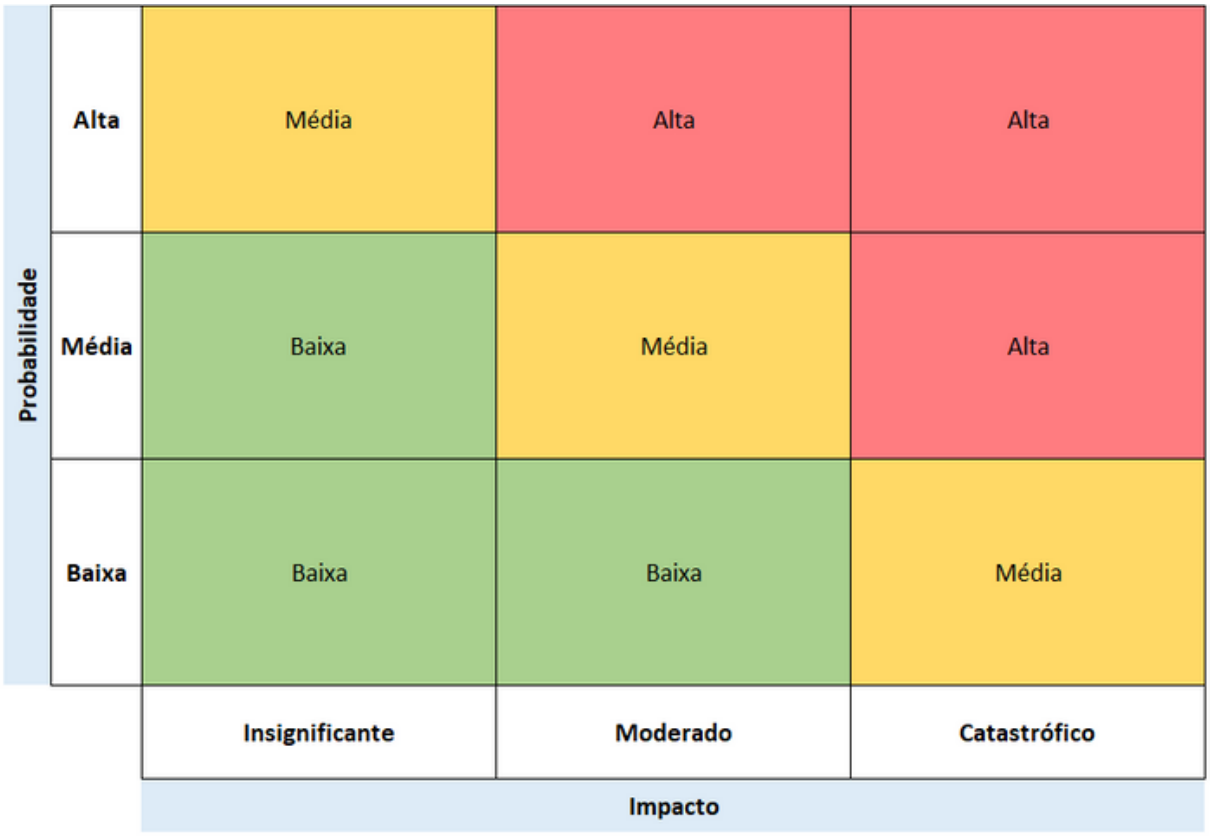
3.3.3.2 Metodologia De Aplicação

Minetto (2019) também afirma que a aplicação da Matriz de Probabilidade e Impacto envolve os seguintes passos:

- Identificação dos Riscos: Listar todos os possíveis riscos que podem afetar o projeto ou operação. Por exemplo, risco de falha no fornecimento de materiais.
- Avaliação da Probabilidade: Estimar a chance de cada risco ocorrer, classificando-a em níveis como baixa, média ou alta.
- Avaliação do Impacto: Determinar as consequências de cada risco caso ele ocorra, também classificando em níveis.
- Construção da Matriz: Posicionar cada risco na matriz de acordo com sua probabilidade e impacto, resultando em uma visualização que auxilia na priorização dos riscos.
- Planejamento de Respostas: Desenvolver estratégias para mitigar ou eliminar os riscos identificados, focando principalmente naqueles com alta probabilidade e alto impacto.

O quadro 1 facilita a visualização dos níveis de risco e a priorização de ações preventivas ou corretivas.

Quadro 1 — Exemplo de matriz de risco



Fonte: Minetto (2019).

A matriz de risco apresentada no Quadro 1 cruza a probabilidade de ocorrência de um evento (eixo vertical) com o impacto que esse evento pode causar (eixo horizontal). A combinação desses dois fatores classifica os riscos em três níveis: baixo (verde), médio (amarelo) e alto (vermelho). Essa categorização orienta a tomada de decisão, permitindo que eventos com alta probabilidade e impacto catastrófico, por exemplo, sejam tratados com prioridade máxima, enquanto riscos de baixa probabilidade e impacto insignificante demandam menor atenção.

3.3.3.3 Benefícios Da Utilização Da Matriz

A utilização da Matriz de Probabilidade e Impacto oferece diversos benefícios, tais como:

- Priorização de Riscos: Facilita a identificação dos riscos mais críticos que necessitam de ações imediatas. Segundo Minetto (2019), a Matriz de Riscos é

uma ferramenta que auxilia na classificação e priorização dos riscos, permitindo identificar quais exigem tratamento imediato e quais podem ser apenas monitorados, sem necessidade de ações corretivas imediatas.

- Alocação Eficiente de Recursos: Minetto (2019) afirma ainda que essa ferramenta contribui para o uso mais racional dos recursos disponíveis, permitindo que sejam direcionados aos riscos mais críticos. Nesse sentido, a autora destaca que a Matriz de Probabilidade e Impacto possibilita à equipe de gestão priorizar ameaças com maior chance de ocorrência e consequências mais severas, otimizando a tomada de decisão.
- Melhoria na Comunicação: Fornece uma representação visual que facilita o entendimento e a comunicação dos riscos entre os membros da equipe e *stakeholders*[24]. Conforme enfatiza a autora a matriz também serve como um instrumento de comunicação eficaz, permitindo que todas as partes interessadas compreendam rapidamente os riscos e participem ativamente da sua gestão.

3.3.4 **Hábitos de Desenvolvimento Seguros (SSDLC)**

Segundo Bertuzzi (2023) o Ciclo de Vida de Desenvolvimento de Software Seguro (SSDLC)[25] é uma abordagem que integra práticas de segurança em todas as fases do desenvolvimento de software, desde a concepção até a manutenção.

De acordo com o autor o SSDLC tem como principal objetivo garantir que a segurança seja incorporada desde o início do processo de desenvolvimento, reduzindo vulnerabilidades e melhorando a confiabilidade do software.

3.3.4.1 Importância do SSDLC em Projetos de Automação

Em projetos de automação, a incorporação de práticas de segurança no ciclo de desenvolvimento é vital para garantir a confiabilidade e a integridade dos sistemas. O autor ainda destaca que o SSDLC foi desenvolvido como uma extensão do SDLC tradicional, incorporando um foco mais aprofundado em aspectos de segurança e conformidade ao longo de todas as etapas do ciclo de

[24] Termo em inglês que significa "partes interessadas", referindo-se a todos os indivíduos ou grupos que têm interesse ou são afetados por um projeto, organização ou processo.
[25] Do inglês *Secure Software Development Lifecycle*

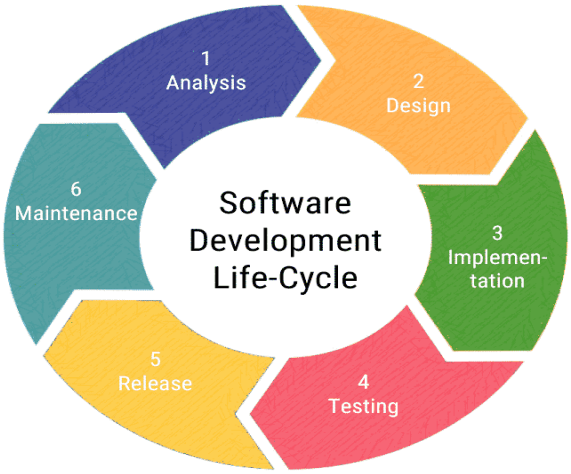
desenvolvimento. Essa integração é crucial para prevenir vulnerabilidades que possam comprometer o funcionamento de sistemas automatizados.

3.3.4.2 Fases do SSDLC

O SSDLC é uma abordagem que integra práticas de segurança em todas as fases do desenvolvimento de software, desde a concepção até a manutenção. Também de acordo com Bertuzzi (2023, s/p), o SSDLC "envolve uma abordagem cíclica para o desenvolvimento de software. O processo começa com a análise de requisitos, seguida de design, implementação, verificação, liberação e resposta".

Na figura 2 é possível verificar todas as fases do SSDLC.

Figura 2 — Fases do SSDLC



Fonte: Platform Simplifier.

As fases do SSDLC incluem:

- Planejamento e Análise de Requisitos: Identificação dos requisitos de segurança e definição de políticas que serão aplicadas durante o desenvolvimento. Segundo Bertuzzi (2023, s/p), "nesta etapa, são levantados os requisitos de segurança e as normas que o sistema deve atender para garantir a proteção contra ameaças".
- *Design*: Arquitetura do sistema com foco em segurança, incluindo a modelagem de ameaças e a definição de controles de segurança. Ainda destacado pelo mesmo autor, "o *design* seguro é essencial para mitigar

vulnerabilidades desde o início, permitindo a adoção de práticas como modelagem de ameaças e definição de mecanismos de controle" (id. ibid., s/p).

- Implementação: Codificação seguindo práticas seguras, como validação de entradas e uso de bibliotecas confiáveis. Bertuzzi (2023) também afirma que, durante a fase de implementação, é fundamental adotar boas práticas de codificação segura — como a validação criteriosa dos dados de entrada — a fim de minimizar vulnerabilidades no sistema.
- Testes: Realização de testes de segurança, como análise estática e dinâmica de código, para identificar vulnerabilidades. O mesmo autor afirma ainda que a realização de testes de segurança, incluindo testes de penetração e análise de código, é essencial para garantir que vulnerabilidades sejam identificadas e corrigidas antes da implantação.
- Implantação: Essa etapa busca garantir que o ambiente de produção esteja devidamente protegido, com configurações alinhadas aos requisitos de segurança. De acordo com Bertuzzi (2023), a implantação envolve a configuração cuidadosa do ambiente, assegurando que todas as medidas de proteção estejam aplicadas antes da liberação do software.
- Monitoramento contínuo: Após a implantação, a segurança do software depende do monitoramento constante e de atualizações periódicas para corrigir novas vulnerabilidades. Conforme observa o mesmo autor (2023), é fundamental manter uma rotina de manutenção para mitigar possíveis ameaças que possam surgir ao longo do tempo.

3.3.4.3 Benefícios do SSDLC

A adoção do SSDLC em projetos de automação oferece diversos benefícios:

- Redução de Vulnerabilidades: A integração da segurança desde as etapas iniciais do desenvolvimento de software contribui significativamente para a prevenção de falhas de programação passíveis de exploração. De acordo com especialistas da área de cibersegurança da empresa Check Point (2024), a adoção do modelo SSDLC permite a identificação antecipada de vulnerabilidades e a aplicação de controles de segurança desde a fase de planejamento, o que reforça a proteção dos sistemas e reduz os riscos de ataques.
- Conformidade com Normas: O SSDLC atende a requisitos de conformidade e regulamentações de segurança, evitando penalidades. Conforme destaca os mesmos especialistas, "a aplicação do SSDLC facilita a aderência às regulamentações de segurança, como GDPR, ISO 27001 e NIST,

garantindo que os softwares estejam alinhados com as normas do setor" (CHECK POINT, 2024, s/p).

- Eficiência Operacional: Sistemas mais seguros tendem a apresentar menor incidência de falhas, aumentando a eficiência e a confiabilidade. Ainda de acordo com os especialistas, "o SSDLC melhora a resiliência do software ao integrar práticas de segurança contínuas, minimizando interrupções operacionais e reduzindo custos com correções emergenciais" (CHECK POINT, 2024, s/p).

A implementação de hábitos de desenvolvimento seguros por meio do SSDLC é vital para o sucesso de projetos de automação. Conforme enfatizado por Bertuzzi (2023, s/p), "a ideia é a readequação de processos existentes, a implementação de novas ferramentas e, claro, uma mudança cultural nas equipes envolvidas". Essa mudança de paradigma é fundamental para enfrentar os desafios de segurança em sistemas cada vez mais complexos e interconectados.

3.4 MODELOS DE GERENCIAMENTO DE RISCOS

O gerenciamento de riscos em projetos de automação industrial exige a aplicação de modelos consolidados, que ofereçam estrutura, diretrizes e métodos eficazes para lidar com as incertezas. Esses modelos fornecem uma base teórica e prática para identificar, avaliar, tratar, monitorar e comunicar riscos de maneira sistemática, garantindo maior segurança, confiabilidade e desempenho nas operações.

A seguir, são apresentados os principais modelos adotados na área, com destaque para a ISO 31000, as normas IEC 61508 e IEC 61511, o modelo Bow-Tie e a Metodologia Ágil, todos amplamente reconhecidos e aplicados em contextos industriais diversos.

3.4.1 **ISO 31000**

A IS0 31000 é uma norma internacional que fornece diretrizes para o gerenciamento de riscos, aplicável a qualquer organização, independentemente de seu porte ou setor.

A Associação Brasileira de Normas Técnicas (ABNT), por meio da NBR ISO 31000:2018, apresenta os princípios, a estrutura e o processo para o

gerenciamento de riscos, com o objetivo de promover a melhoria contínua, a criação e a proteção de valor nas organizações (ABNT, 2018). Essa abordagem sistemática contribui para a identificação, avaliação e mitigação de riscos, além de favorecer a tomada de decisões mais informadas e o aperfeiçoamento contínuo dos processos organizacionais.

3.4.1.1 Aplicação da ISO 31000 em Projetos de Automação

Em projetos de automação, especialmente no campo da engenharia de controle, a aplicação da norma ISO 31000 é considerada essencial para a estruturação de um sistema eficaz de gerenciamento de riscos. Essa norma orienta as organizações na identificação, avaliação e tratamento de riscos, com foco na prevenção de falhas e na proteção do desempenho e da segurança dos sistemas automatizados, conforme estabelecido pela Associação Brasileira de Normas Técnicas (ABNT, 2018).

A ABNT, ainda por meio da mesma NBR "fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A aplicação destas diretrizes pode ser personalizada para qualquer organização e seu contexto" (ABNT, 2018). Essa flexibilidade é crucial para adaptar as práticas de gestão de riscos às especificidades de projetos de automação.

3.4.1.2 Princípios da ISO 31000

A ISO 31000 estabelece princípios fundamentais para uma gestão de riscos eficaz, garantindo que as organizações possam identificar, avaliar e tratar riscos de forma estruturada e eficiente. Segundo Maluf (2023, s/p), "a norma estabelece princípios essenciais que devem ser seguidos para garantir que a gestão de riscos seja eficaz e adaptada à realidade de cada organização". Esses princípios incluem:

- Integração: A gestão de riscos deve ser parte integrante dos processos organizacionais. Segundo o autor (2023), a gestão de riscos só é realmente eficaz quando está integrada a todas as atividades da organização, deixando de ser um processo isolado e tornando-se parte da cultura empresarial.
- Estrutura e Abrangência: Deve ser conduzida de forma estruturada e abrangente para gerar resultados consistentes e comparáveis. Também para o mesmo autor, "a abordagem estruturada da ISO 31000 permite que os riscos sejam identificados, avaliados e tratados de maneira consistente, garantindo a confiabilidade e eficiência do processo" (id. ibid., s/p).
- Personalização: A gestão de riscos deve ser adaptada ao contexto externo e interno da organização, bem como ao perfil de riscos. Ainda segundo o mesmo autor, "cada organização enfrenta desafios e riscos específicos, e a personalização da abordagem de gestão de riscos é essencial para que o processo seja eficaz e relevante" (id. ibid., s/p).
- Inclusão: Deve envolver as partes interessadas apropriadas para assegurar que a gestão de riscos considere todos os pontos de vista relevantes. Sendo assim, "a participação ativa das partes interessadas no processo de gestão de riscos aumenta a compreensão e aceitação das medidas adotadas, garantindo uma abordagem mais colaborativa e eficaz" (id. ibid., s/p).
- Dinâmica: A gestão de riscos deve antecipar, detectar, reconhecer e reagir a mudanças e eventos de forma oportuna e apropriada. O autor (2023) também ressalta que, "o ambiente organizacional está sempre evoluindo, e a gestão de riscos precisa ser dinâmica, adaptando-se rapidamente às mudanças internas e externas".
- Melhoria Contínua: O processo de gestão de riscos deve ser continuamente aprimorado por meio de aprendizado e experiência. Para tanto, "a ISO 31000 enfatiza a necessidade de revisão constante do processo de gestão de riscos, garantindo que ele permaneça eficiente e alinhado às melhores práticas". (MALUF, 2023, s/p).

Dessa forma, então, a adoção desses princípios permite que as organizações gerenciem riscos de maneira estruturada e proativa, fortalecendo sua resiliência e sustentabilidade no longo prazo.

3.4.1.3 Processo de Gestão de Riscos Segundo a ISO 31000

A ISO 31000 define um processo estruturado para a gestão de riscos, composto pelas seguintes etapas:

- Comunicação e Consulta: Envolver as partes interessadas para compreender o risco e as medidas adotadas.

> Já que a gestão de riscos deve ser inclusiva, este é o momento onde as partes interessadas apropriadas serão conscientizadas para

> entenderem os riscos (comunicação) e retornarão com informações que auxiliarão a tomada de decisão (consulta) (MARTINS, 2022, s/p).

- Estabelecimento do Contexto: Definir os parâmetros externos e internos a serem considerados ao gerenciar riscos. Martins (op. cit.), também explica que, nessa etapa, o processo de gestão de riscos deve ser personalizado, com a definição clara das atividades abrangidas pelo escopo e a consideração do contexto interno e externo dessas atividades.
- Avaliação de Riscos: Identificar, analisar e avaliar os riscos. Ainda segundo a mesma autora, essa fase engloba as etapas de identificação, análise e avaliação dos riscos, sendo essencial para a compreensão das ameaças que podem impactar os objetivos organizacionais.
- Tratamento de Riscos: Selecionar e implementar opções para abordar os riscos. Martins (2022) observa que as organizações devem escolher e aplicar estratégias adequadas de tratamento, avaliando a eficácia das ações adotadas e decidindo sobre a aceitabilidade do risco remanescente ou a necessidade de medidas adicionais.
- Monitoramento e Análise Crítica: Acompanhar e revisar o desempenho do processo de gestão de riscos. A autora ainda destaca que é necessário assegurar, de forma contínua, a qualidade e eficácia da concepção, implementação e resultados do processo de gestão de riscos em todas as suas etapas.
- Registro e Relato: Documentar e relatar os resultados do processo de gestão de riscos. Segundo Martins (2022), a norma ISO 31000 ressalta a importância da documentação adequada do processo e dos resultados, considerando as necessidades das partes interessadas.

3.4.1.4 Benefícios Da Implementação Da ISO 31000

A implementação da ISO 31000 em projetos de automação oferece diversos benefícios significativos. Conforme aponta Martins (2022), essa norma proporciona uma abordagem estruturada para a identificação, avaliação e tratamento de riscos, o que resulta em maior segurança e confiabilidade para as organizações.

- Melhoria na Identificação de Riscos: A mesma norma estimula uma abordagem proativa na identificação de ameaças, favorecendo uma detecção mais abrangente e precisa. De acordo com Martins (2022), essa antecipação possibilita um preparo mais eficaz das empresas para enfrentar desafios antes que eles se agravem.

- Tomada de Decisões Informadas: A ISO 31000 oferece suporte à tomada de decisões estratégicas ao estruturar o processo de avaliação de riscos com base em dados. Martins (op. cit.) destaca que isso permite que os líderes empresariais adotem ações mais assertivas.
- Aumento da Confiabilidade dos Sistemas: Martins (2022) ainda afirma que a norma contribui diretamente para a segurança e confiabilidade dos sistemas automatizados, ao fornecer diretrizes claras para mitigação de riscos. Como ressalta a autora, isso resulta em maior estabilidade e eficiência operacional.
- Conformidade com Normas e Regulamentações: Por fim, Martins (2022) observa que a adoção da ISO 31000 facilita o atendimento aos requisitos legais e normativos, reduzindo os riscos jurídicos e fortalecendo a governança e a reputação da organização no mercado.

A implementação da ISO 31000 em projetos de automação é uma prática recomendada para gerenciar eficazmente os riscos associados a falhas de programação e incompatibilidades de equipamentos. Conforme a ABNT NBR ISO 31000:2018, a norma fornece uma abordagem comum para gerenciar qualquer tipo de risco e não é específica para qualquer indústria ou setor. Essa universalidade facilita sua aplicação em diversos contextos, incluindo a automação.

3.4.2 **IEC 61508 e IEC 61511**

A *International Electrotechnical Commission* [26] (IEC), possuem duas normas, IEC 61508 e IEC 61511 que são referências internacionais fundamentais para a segurança funcional de sistemas elétricos, eletrônicos e programáveis eletronicamente, especialmente em indústrias de processos. A IEC 61508 estabelece os requisitos gerais para garantir que sistemas relacionados à segurança funcionem de maneira confiável (IEC, 2010), enquanto a IEC 61511 adapta esses princípios ao setor de processos industriais,

[26] Em tradução livre: Comissão Eletrotécnica Internacional. É uma organização internacional de normalização responsável por elaborar e publicar normas para todas as tecnologias elétricas, eletrônicas e correlatas. Fundada em 1906, a IEC atua na padronização de áreas como segurança funcional, automação industrial e sistemas de energia, com o objetivo de promover a interoperabilidade entre tecnologias e garantir maior eficiência, segurança e sustentabilidade em escala global.

fornecendo diretrizes específicas para o desenvolvimento, implementação e manutenção de Sistemas Instrumentados de Segurança (SIS) (IEC, 2016).

3.4.2.1 Aplicação Das Normas Em Projetos De Automação

Em projetos de automação, de acordo com Ferrarezi et al. (2015, p.1) a conformidade com as normas IEC 61508 e IEC 61511 é crucial para gerenciar riscos associados a falhas de programação e incompatibilidades de equipamentos. A adoção dessas normas assegura que os sistemas de controle sejam projetados e operados com níveis adequados de integridade de segurança, minimizando a probabilidade de falhas que possam comprometer a operação segura dos processos automatizados.

Ferrarezi et al. (2015, p.1) ainda afirma que, "uma forma de se desenvolver sistemas mais seguros e confiáveis é o uso dos Sistemas Instrumentados de Segurança (SIS) de acordo com as normas IEC 61508 e IEC 61511". Essa abordagem é essencial para garantir que os sistemas automatizados atendam aos requisitos de segurança funcional necessários.

3.4.2.2 Estrutura das Normas

. Para que as normas técnicas sejam efetivamente aplicadas no gerenciamento de riscos em projetos de automação industrial, é essencial compreender sua estrutura e organização interna. A IEC 61508 e a IEC 61511 são compostas por partes distintas, cada uma abordando aspectos específicos da segurança funcional de sistemas elétricos, eletrônicos e programáveis. A seguir, será apresentada a estrutura de cada uma dessas normas, destacando suas divisões, objetivos e o foco de cada parte, com o intuito de facilitar sua compreensão e aplicação prática no contexto industrial.

3.4.2.2.1 *IEC 61508*

A norma IEC 61508 é composta por sete partes, abrangendo desde os requisitos gerais de segurança funcional até orientações específicas para a aplicação de sistemas elétricos, eletrônicos e programáveis eletronicamente. Ela

define os Níveis de Integridade de Segurança (SILs[27]) e estabelece um ciclo de vida de segurança para o desenvolvimento de sistemas relacionados à segurança (IEC, 2010).

3.4.2.2.2 *IEC 61511*

Adaptada para a indústria de processos, a norma IEC 61511 detalha os requisitos para o projeto, implementação, operação e manutenção de SIS. Ela enfatiza a importância de uma abordagem sistemática para a gestão de segurança funcional ao longo de todo o ciclo de vida do sistema (IEC, 2016).

3.4.2.3 Benefícios da Implementação das Normas

A adoção das normas IEC 61508 e IEC 61511 em projetos de automação oferece diversos benefícios:

- Redução de Riscos: aplicação rigorosa das normas permite identificar e mitigar riscos potenciais associados a falhas de programação e incompatibilidades de equipamentos (IEC, 2010; IEC, 2016).
- Conformidade Regulatória: As normas fornecem uma base para atender a requisitos legais e regulatórios relacionados à segurança funcional (IEC, 2016).
- Melhoria da Confiabilidade: Sistemas desenvolvidos conforme essas normas tendem a apresentar maior confiabilidade e disponibilidade operacional (IEC, 2010).

O respeito às normas IEC 61508 e IEC 61511 é essencial para o sucesso de projetos de automação. Uma vez que elas fornecem uma estrutura robusta para o gerenciamento de riscos, assegurando que os sistemas sejam projetados e operados com os mais altos padrões de segurança funcional.

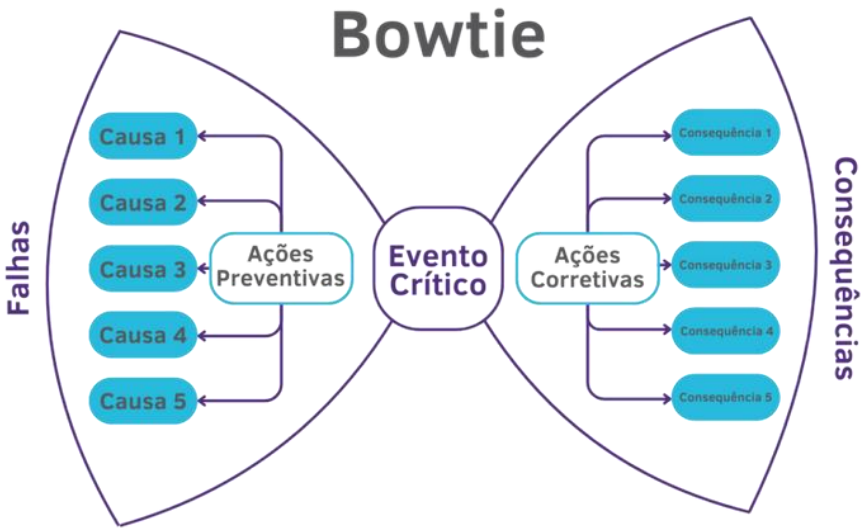
3.4.3 ***Bow-Tie***

[27] Do inglês *Safety Integrity Levels* consiste em níveis que classificam a integridade de segurança de sistemas instrumentados, conforme definido pela norma IEC 61508. Em uma tradução livre, significam “Níveis de Integridade de Segurança”, e variam de SIL 1 (nível mais baixo) a SIL 4 (nível mais alto), de acordo com a probabilidade de falha aceitável em função do risco controlado.

Conforme Oliveira (2022, s/p), "o *Bowtie* é uma ferramenta valiosa na gestão de riscos, permitindo uma análise minuciosa dos controles críticos e dos eventos indesejados".

O autor afirma ainda que o modelo *BowTie* é uma ferramenta gráfica que combina elementos FTA e da Análise de Árvores de Eventos (ETA). Conforme observado na figura 3, sua estrutura lembra o formato de uma gravata borboleta, dividida em três partes principais: causas, evento crítico e consequências.

Figura 3 — Modelo *Bow-Tie*



Fonte: Chaves (2024).

3.4.3.1 Aplicação do Modelo Bow-Tie em Projetos de Automação

Oliveira (2022) afirma que o modelo Bow-Tie é essencial para gerenciar riscos associados a falhas de programação e incompatibilidades de equipamentos. Ao mapear visualmente as causas potenciais de falhas (como erros de software ou incompatibilidade de hardware) e suas possíveis consequências (como interrupções operacionais ou acidentes), a ferramenta auxilia na identificação de medidas preventivas e mitigatórias eficazes.

Nessas características,

> [...] o bow-tie é uma ferramenta valiosa na gestão de riscos, permitindo uma análise minuciosa dos controles críticos e dos eventos indesejados. Sua representação gráfica facilita a comunicação e

> promove uma compreensão clara dos riscos e medidas de controle (OLIVEIRA, 2023, s/p).

3.4.3.2 Estrutura do Modelo *Bow-Tie*

O diagrama *Bow-Tie* é composto por diferentes elementos que estruturam a análise de riscos, permitindo uma compreensão clara das relações entre causas, eventos e consequências. Segundo Oliveira (2023, s/p), sua estrutura inclui:

- Evento Central (Nó): Representa o evento indesejado ou falha principal que se deseja evitar.
- Causas (Lado Esquerdo): Fatores que podem levar ao evento central, como falhas de programação ou incompatibilidade de equipamentos.
- Consequências (Lado Direito): Resultados potenciais decorrentes do evento central, como paralisações ou danos materiais.
- Barreiras Preventivas: Medidas implementadas para impedir que as causas resultem no evento central.
- Barreiras de Mitigação: Ações destinadas a reduzir o impacto das consequências após a ocorrência do evento central.

3.4.3.3 Benefícios do Modelo *Bow-Tie*

A adoção do Modelo *Bow-Tie* em projetos de automação oferece diversos benefícios para a gestão de riscos e segurança operacional. Ainda para Oliveira (2023, p.42), os principais benefícios incluem:

- Clareza Visual: A representação gráfica facilita a compreensão das relações causais e das medidas de controle.
- Identificação de Lacunas: Auxilia na detecção de áreas onde faltam medidas preventivas ou mitigatórias.
- Comunicação Eficaz: Facilita o entendimento entre membros da equipe e partes interessadas, promovendo uma cultura de segurança.

A implementação do Modelo *Bow-Tie* em projetos de automação é uma prática recomendada para gerenciar riscos de forma eficaz. Consoante a Oliveira (2023, p.35), "os *bow-tie* podem contribuir para favorecer um ambiente de trabalho mais protegido e confiável, melhorando a segurança e a eficácia das atividades industriais". Sendo assim, sua aplicação sistemática permite uma

abordagem proativa na identificação e mitigação de riscos, assegurando a continuidade e a segurança das operações automatizadas.

3.4.4 **Metodologia Ágil**

Segundo Fernandes e Rabechini Jr. (2021), a Metodologia Ágil representa um conjunto de práticas e princípios voltados para o desenvolvimento iterativo e incremental de projetos, enfatizando a flexibilidade, a colaboração contínua com o cliente e a capacidade de adaptação a mudanças. No contexto da automação, a aplicação de metodologias ágeis, como o Scrum, tem se mostrado eficaz no gerenciamento de riscos associados a falhas de programação e incompatibilidades de equipamentos.

Ainda segundo os autores, a adoção de metodologias ágeis permite uma resposta rápida às incertezas do projeto, promovendo maior eficiência na entrega de valor e na mitigação de riscos tecnológicos.

De acordo com os mesmos autores (2021, p.2), "os resultados dos testes estatísticos confirmaram a influência do gerenciamento de riscos no sucesso de projetos gerenciados por abordagens ágeis".

Essa afirmação destaca a relevância de incorporar práticas ágeis para aprimorar a gestão de riscos em projetos complexos.

3.4.4.1 Princípios da Metodologia Ágil Aplicados ao Gerenciamento de Riscos

- Detecção Precoce de Problemas: Por meio de revisões frequentes, falhas de programação e incompatibilidades de equipamentos são identificadas rapidamente. Conforme Fernandes e Rabechini Jr. (2021, p.6), essa abordagem permite mitigar riscos ao longo do desenvolvimento, garantindo maior confiabilidade dos sistemas.
- Redução de Incertezas: A abordagem iterativa permite a validação contínua de hipóteses, diminuindo a incerteza associada ao desenvolvimento. Ainda para os autores (2021, p.7) destacam ainda que a adaptabilidade das metodologias ágeis possibilita ajustes rápidos diante de mudanças de requisitos e desafios técnicos.
- Melhoria Contínua: As retrospectivas ao final de cada ciclo incentivam a reflexão e o aprimoramento constante dos processos e, sendo assim, “esse princípio fomenta um ambiente colaborativo e orientado à inovação, otimizando a gestão de riscos” (id. ibid., p. 7).

A adoção de metodologias ágeis, como o Scrum, no gerenciamento de projetos de automação, oferece uma abordagem eficaz para lidar com os riscos inerentes a falhas de programação e incompatibilidades de equipamentos. Também observado por Fernandes e Rabechini Jr. (2023, p.8), a gestão de riscos em ambientes ágeis contribui significativamente para o sucesso dos projetos, tornando-se uma prática recomendada para engenheiros de controle e automação que buscam aumentar a eficiência e a confiabilidade de seus sistemas.

Diante do exposto, é possível compreender que a análise e o gerenciamento de riscos desempenham um papel essencial na prevenção de falhas de programação e na mitigação de incompatibilidades de equipamentos em projetos de automação industrial. A aplicação de ferramentas como FMEA, FTA, Matriz de Riscos, SSDLC e modelos consolidados como a ISO 31000, IEC 61508, IEC 61511, Bow-Tie e a Metodologia Ágil oferece uma abordagem estruturada e eficaz para lidar com incertezas. Esses métodos auxiliam na tomada de decisões mais seguras, na definição de prioridades e na construção de sistemas mais confiáveis, seguros e resilientes. O conhecimento e a aplicação dessas estratégias fortalecem não apenas a prevenção de falhas, mas também a cultura organizacional voltada à melhoria contínua e à excelência operacional.

3.4.5 **Matriz SWOT**

Segundo Hill e Westbrook (1997) a aplicação da Matriz SWOT tem se consolidado como uma estratégia eficaz para mitigar os riscos inerentes aos projetos de automação, principalmente aqueles associados a falhas de programação e à incompatibilidade de equipamentos. Essa ferramenta possibilita uma análise abrangente dos fatores internos e externos que podem afetar o desempenho do sistema, organizando-os em quatro categorias: Forças (Strengths), Fraquezas (Weaknesses), Oportunidades (Opportunities) e Ameaças (Threats).

No ambiente interno dos projetos, as forças podem incluir aspectos como a experiência técnica da equipe, a qualidade dos processos de desenvolvimento e a robustez dos sistemas já implantados. Por outro lado, as fraquezas podem estar relacionadas a deficiências na integração entre sistemas e equipamentos,

processos de atualização de software pouco dinâmicos ou mesmo lacunas no treinamento dos operadores. Já no cenário externo, as oportunidades podem surgir a partir do constante avanço tecnológico e da possibilidade de parcerias estratégicas, enquanto as ameaças podem envolver a rápida obsolescência dos equipamentos e a volatilidade dos fornecedores de tecnologia.

Conforme evidenciado por Hill e Westbrook (1997), a análise SWOT oferece uma visão sistêmica que facilita a identificação dos pontos críticos a serem corrigidos, bem como a exploração de situações favoráveis para a melhoria contínua dos processos. Além disso, o Project Management Institute (PMI, 2017) ressalta que a integração de métodos sistemáticos de análise de riscos — como a Matriz SWOT — contribui significativamente para a elaboração de planos de ação que visam minimizar impactos adversos e potencializar os acertos nos projetos.

A figura 4 apresenta uma Matriz SWOT, dividida em quatro quadrantes que ajudam a identificar os fatores internos e externos em um projeto de automação. A parte superior inclui as Forças, que representam os pontos positivos da organização, como a experiência da equipe e processos consolidados, e as Fraquezas, que são os aspectos que prejudicam o desempenho, como a falta de testes adequados e manutenção de código. Na parte inferior, as Oportunidades referem-se a condições externas favoráveis, como avanços tecnológicos, enquanto as Ameaças abordam os riscos que podem impactar negativamente o projeto, como obsolescência de equipamentos.

Figura 4 — Matriz SWOT

Fonte: Runrun.it

Portanto, a inclusão da Matriz SWOT no gerenciamento de riscos em projetos de automação não só favorece uma compreensão mais detalhada das vulnerabilidades e potencialidades do sistema, mas também serve de base para a implementação de estratégias que promovam a resiliência e a sustentabilidade dos processos tecnológicos. Essa abordagem integrada é fundamental para a tomada de decisões estratégicas que assegurem a continuidade e a eficiência das operações em ambientes cada vez mais complexos e dinâmicos.

4 METODOLOGIA

Este capítulo apresenta a metodologia utilizada para o desenvolvimento da pesquisa, de natureza qualitativa e quantitativa, com enfoque exploratório. O estudo baseia-se em uma revisão bibliográfica e documental, com a análise de normas técnicas, artigos científicos e materiais especializados que abordam o gerenciamento de riscos em projetos de automação industrial.

4.1 CARACTERISTICAS METODOLOGICAS

A presente pesquisa caracteriza-se como bibliográfica, documental e de abordagem mista, combinando aspectos qualitativos e quantitativos.

A pesquisa bibliográfica, conforme Gil (2008), fundamenta-se na análise de obras já publicadas — como livros, artigos científicos, normas técnicas e publicações especializadas — com o objetivo de aprofundar o conhecimento sobre determinado tema. A escolha por essa abordagem visa compreender, por meio da literatura, estratégias eficazes para mitigar falhas de programação e incompatibilidades de equipamentos, contribuindo para a melhoria da confiabilidade e segurança dos sistemas automatizados.

A pesquisa documental, segundo Lakatos e Marconi (2003), baseia-se em documentos que, embora não tenham sido analisados ainda sob uma abordagem científica, contêm informações relevantes para o estudo, como normas regulamentadoras, relatórios técnicos e legislações.

Quanto à abordagem, esta pesquisa é predominantemente qualitativa, buscando compreender de forma interpretativa os riscos associados a falhas de programação e incompatibilidades de equipamentos em projetos de automação industrial. De acordo com Creswell (2010), a abordagem qualitativa permite analisar fenômenos em profundidade, considerando seus contextos e significados.

No entanto, também se incorpora uma abordagem quantitativa, uma vez que foi realizado um levantamento inicial de trabalhos acadêmicos e documentos técnicos relacionados ao tema. Aplicaram-se critérios objetivos de inclusão e exclusão para selecionar os materiais mais relevantes, e os resultados dessa triagem foram organizados em forma de quadro quantitativo, permitindo

visualizar o volume de publicações encontradas e as que foram efetivamente analisadas. Essa etapa contribuiu para garantir maior rigor e transparência ao processo de seleção das fontes utilizadas.

4.2 PROCEDIMENTOS METODOLÓGICOS

Este trabalho adota uma abordagem mista, combinando elementos qualitativos e quantitativos, com caráter exploratório. A abordagem qualitativa permite uma análise interpretativa e aprofundada dos fenômenos relacionados aos riscos em projetos de automação, especialmente no que se refere a falhas de programação e incompatibilidades de equipamentos. Já o aspecto quantitativo está presente na etapa de levantamento e triagem dos materiais, em que se procedeu à quantificação dos estudos identificados e à seleção dos mais relevantes com base em critérios previamente estabelecidos.

O caráter exploratório da pesquisa refere-se ao objetivo de ampliar a compreensão sobre o tema, investigando e organizando o conhecimento disponível, uma vez que se trata de uma área que, embora técnica, ainda carece de estudos sistematizados que integrem riscos técnicos e estratégicos de forma conjunta.

A pesquisa fundamenta-se em uma revisão bibliográfica, que consiste na análise de livros, artigos científicos, normas técnicas e demais publicações já existentes, além da análise documental de estudos de caso e registros técnicos, fornecendo uma base teórica consistente para sustentar as discussões e conclusões apresentadas.

4.2.1 **Fontes**

A pesquisa fundamenta-se em fontes técnicas e científicas obtidas em bases de dados reconhecidas, priorizando materiais relevantes e atualizados sobre gestão de riscos, falhas em projetos de automação, protocolos de comunicação e compatibilidade de hardware/software. As principais fontes incluem:

- Google Acadêmico, para busca de artigos científicos e dissertações relacionadas ao tema.
- Sites especializados em automação industrial, incluindo blogs técnicos, portais de engenharia e fabricantes de equipamentos.
- Normas técnicas internacionais e nacionais, comov ISO 31000 (Gestão de Riscos), IEC 61508 (Segurança Funcional de Sistemas Elétricos, Eletrônicos e Programáveis) IEC 61511 (Segurança funcional — Sistemas instrumentados de segurança para o setor da indústria de processo) e documentos técnicos de fabricantes sobre compatibilidade de equipamentos e boas práticas de programação.
- Trabalhos acadêmicos disponíveis em repositórios de universidades, que tratam de gerenciamento de riscos na automação industrial.

4.2.2 **Critérios de inclusão e exclusão**

Para garantir a relevância e aplicabilidade da pesquisa, foram estabelecidos os seguintes critérios:

1. Inclusão:

- Materiais disponíveis em português e inglês.
- Conteúdos que abordam especificamente falhas de programação (erros de lógica, bugs, falhas de comunicação entre sistemas) e incompatibilidades de equipamentos (integração de dispositivos de diferentes fabricantes, conflitos de protocolos de comunicação, falhas de configuração em CLPs e sensores).

2. Exclusão:

- Publicações que tratam de riscos industriais de forma genérica, sem foco na automação.

Trabalhos que não apresentem embasamento técnico sólido ou não sejam reconhecidos academicamente.

5 **APRESENTACAO E DISCUSSÃO DOS RESULTADOS**

Este capítulo apresenta os resultados obtidos por meio da análise bibliográfica e documental realizada, estruturada em torno dos principais riscos associados a falhas de programação e incompatibilidade de equipamentos em projetos de automação industrial. A discussão dos achados tem como objetivo verificar a eficácia das metodologias de gerenciamento de riscos identificadas, confrontando os dados coletados com os pressupostos teóricos e hipóteses formuladas na introdução deste trabalho.

5.1 ORGANIZAÇÃO E ANÁLISE DOS DADOS

Os dados coletados foram sistematizados em fichas de leitura e organizados em categorias temáticas. A estrutura analítica adotada incluiu:

Classificação dos riscos:

- Falhas de programação, como erros de lógica, bugs em scripts de controle e inconsistências em sistemas SCADA.
- Incompatibilidades de equipamentos, com destaque para dificuldades de integração entre CLP’s, sensores, atuadores e softwares de diferentes fabricantes.
- Análise das causas-raiz: Utilização das ferramentas FMEA, Árvore de Falhas (FTA), Matriz de Probabilidade e Impacto e SSDLC, que permitiram identificar pontos críticos e estabelecer ações preventivas.
- Estratégias de mitigação: Adoção de boas práticas de programação, uso de protocolos padronizados de comunicação, redundância em sistemas críticos, validação de segurança e testes automatizados.

5.2 RESULTADOS DA REVISÃO BIBLIOGRÁFICA E LITERÁRIA

A revisão bibliográfica e documental deste trabalho foi conduzida a partir de um conjunto amplo e diversificado de fontes. Foram utilizadas 72 referências, entre artigos científicos, trabalhos acadêmicos, normas técnicas, manuais de empresas, blogs especializados e sites institucionais do setor de automação.

5.2.1 **Artigos Científicos e Trabalhos Acadêmicos**

Durante a pesquisa, foram analisados aproximadamente 25 artigos e TCCs. Destes, 10 foram lidos integralmente por apresentarem relação direta com o tema. Após triagem qualitativa, 4 foram selecionados para compor a base teórica do trabalho, por reunirem os seguintes critérios:

- Aplicação direta de ferramentas como FMEA, FTA, Bow-Tie, Matriz SWOT e SSDLC;
- Estudos de caso práticos relacionados a falhas em sistemas de automação;
- Discussão consistente sobre integração de hardware e software;
- Fundamentação baseada em normas técnicas e melhores práticas da engenharia.

Os demais foram excluídos por tratarem de abordagens genéricas ou por não aprofundarem os tópicos de falhas técnicas e riscos operacionais.

5.2.2 **Normas Técnicas**

Foram levantadas 6 normas técnicas relevantes, sendo 3 normas selecionadas e aplicadas diretamente na fundamentação das estratégias de mitigação:

- ISO 31000 – Diretrizes para gestão de riscos;
- IEC 61508 – Segurança funcional de sistemas elétricos e eletrônicos programáveis;
- IEC 61511 – Segurança funcional para sistemas instrumentados na indústria de processos.

As demais normas foram consideradas complementares ou pouco aderentes ao escopo específico deste estudo.

5.2.3 **Sites Técnicos e Materiais Online**

Foram consultados mais de 40 sites especializados e portais institucionais de empresas líderes no setor, como Rockwell Automation, Siemens, Schneider Electric, Tractian, entre outros. Destes, cerca de 25 foram utilizados efetivamente por conterem:

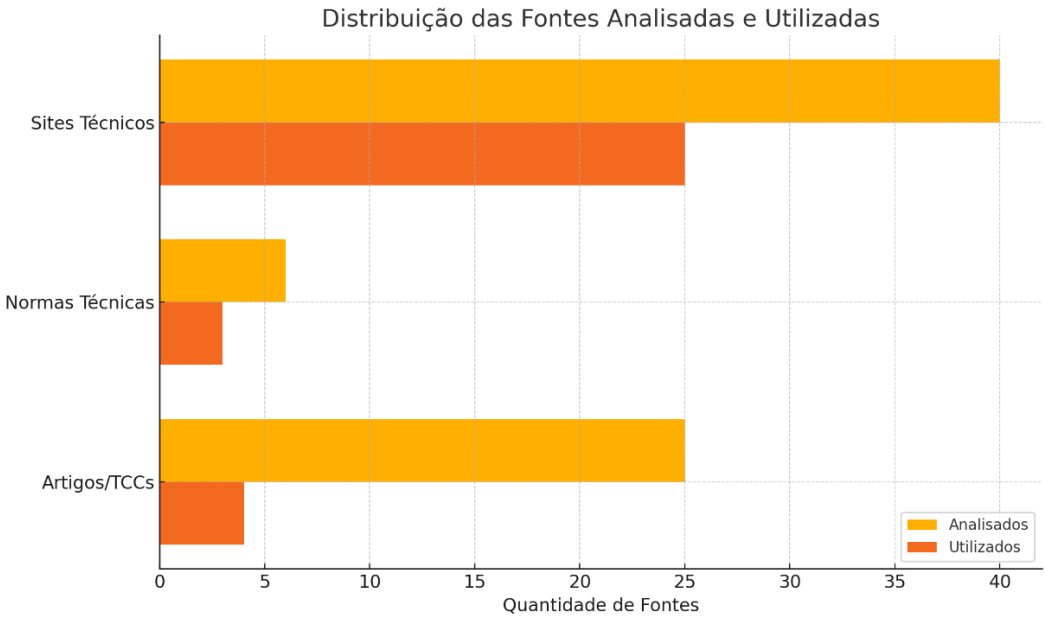
- Informações técnicas atualizadas;
- Estudos de caso sobre falhas reais e soluções implementadas;

- Explicações didáticas sobre ferramentas como FMEA, Bow-Tie, SSDLC e protocolos industriais;
- Discussões práticas sobre manutenção, integração de sistemas, desenvolvimento seguro e riscos operacionais.

Os demais foram descartados por apresentarem conteúdos superficiais, repetitivos ou fora do escopo técnico necessário.

O gráfico 1 apresenta a distribuição das fontes pesquisadas e efetivamente utilizadas neste trabalho. Observa-se que, embora uma quantidade significativa de materiais tenha sido analisada, apenas uma parte foi selecionada com base na aderência ao tema e na profundidade técnica necessária para sustentar as estratégias discutidas.

Gráfico 1 — Quantitativo de Trabalhos



Fonte: Dados da Pesquisa (2025)

Essa ampla revisão possibilitou reunir tanto a profundidade teórica quanto a aplicabilidade prática necessária para o desenvolvimento do modelo de gerenciamento de riscos proposto neste trabalho.

5.3 ESTRUTURAÇÃO E APLICAÇÃO DO MODELO DE GERENCIAMENTO DE RISCOS

Com base na revisão da literatura e na categorização dos riscos, foi proposto um modelo metodológico estruturado em três fases:

1. Identificação de vulnerabilidades nos códigos, na configuração dos softwares e na interoperabilidade dos dispositivos.
2. Implementação de estratégias preventivas, com foco na validação sistemática de códigos e na escolha adequada de protocolos de comunicação.
3. Ações corretivas e planos de resposta rápida para mitigar falhas já ocorridas, reduzindo o tempo de inatividade e os impactos operacionais.

Esse modelo foi embasado em normas como ISO 31000, IEC 61508 e IEC 61511, proporcionando uma abordagem confiável e padronizada.

5.4 MELHORES PRÁTICAS IDENTIFICADAS

Com base na análise dos estudos consultados, foram identificadas as principais estratégias e melhores práticas para mitigar falhas de programação e incompatibilidades de equipamentos. A seleção baseou-se em sua eficácia comprovada na literatura técnica e na aplicação prática em ambientes industriais complexos:

- Identificação e Análise de Riscos: ferramentas como FMEA, FTA, matriz de risco e matriz SWOT oferecem suporte sistemático para identificação, classificação e tratamento de riscos.
- SSDLC: promove prevenção desde a concepção do software e reforça a cultura de segurança.
- Conformidade com normas ISO e IEC: garante estrutura robusta para gestão de riscos e aumenta a confiabilidade dos sistemas.
- Planejamento Ágil e Integração Contínua: aceleram o desenvolvimento e reduzem falhas na integração de sistemas.
- Monitoramento e Validação Contínua: asseguram padrões de desempenho e permitem resposta rápida a falhas.
- Capacitação e Documentação: fortalecem a competência técnica das equipes e facilitam o rastreamento de falhas e correções.
- Revisão e Melhoria Contínua: possibilitam adaptação constante frente às inovações tecnológicas e desafios operacionais.

Essas práticas, quando aplicadas em conjunto, formam a base de uma abordagem proativa e eficiente para garantir segurança e confiabilidade em projetos de automação industrial.

5.5 DISCUSSÃO DOS CASOS PRÁTICOS

Estudos de caso selecionados da literatura foram analisados para validar a aplicabilidade do modelo proposto. Os critérios de seleção incluíram:

- Relevância técnica dos incidentes documentados.
- Complexidade dos desafios enfrentados (falhas de lógica, incompatibilidade entre dispositivos, problemas de comunicação em protocolos industriais).
- Impactos operacionais observados (interrupções, perdas de produtividade, retrabalho).

A análise dos casos evidenciou que as organizações que adotaram práticas padronizadas e metodologias formais de análise de riscos conseguiram reduzir significativamente o número e a gravidade das falhas.

5.6 AVALIAÇÃO DA EFETIVIDADE DAS ESTRATÉGIAS

A avaliação dos resultados foi conduzida em três etapas:

1. Verificação da eficácia das metodologias de identificação de riscos: confirmou-se que ferramentas como FMEA, FTA e a Matriz de Risco são eficazes para antecipar e classificar riscos críticos.
2. Avaliação das estratégias de mitigação: constatou-se que metodologias como SSDLC, conformidade normativa e práticas ágeis resultam em maior controle e adaptabilidade dos sistemas.
3. Monitoramento e revisão contínua: evidenciou-se a importância de manter o ciclo de melhoria contínua, promovendo ajustes constantes frente às mudanças tecnológicas e operacionais.

5.7 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Os dados obtidos reforçam as hipóteses iniciais deste trabalho, comprovando que a aplicação sistemática de ferramentas de análise de risco, aliada ao desenvolvimento seguro, conformidade normativa e práticas de gestão ágeis, contribui significativamente para a mitigação de falhas em projetos de automação. Os desafios persistem, especialmente em relação à integração entre sistemas heterogêneos e à comunicação entre áreas técnicas, mas os

resultados apontam para um avanço importante na padronização e na confiabilidade dos processos industriais.

CONSIDERAÇÕES FINAIS

Este trabalho abordou o gerenciamento de riscos associados a falhas de programação e incompatibilidade de equipamentos em projetos de automação, destacando as ferramentas e estratégias para garantir a eficiência, segurança e confiabilidade dos sistemas automatizados. A partir da revisão bibliográfica e análise de ferramentas aplicadas, foi possível identificar os principais fatores de risco e propor estratégias para mitigá-los.

Os resultados indicam que o sucesso de um projeto de automação depende de um planejamento detalhado que integre todas as etapas do ciclo de vida do sistema, desde a escolha de equipamentos até o desenvolvimento e a validação do software. Ferramentas como FTA, FMA e outras provaram ser essenciais para minimizar falhas.

Adicionalmente, a implementação de práticas robustas de gerenciamento de riscos, incluindo a adoção de normas técnicas e frameworks, como a IEC 61508, IEC 61511 e a ISO 31000, foi destacada como uma abordagem eficaz para lidar com incertezas e aumentar a resiliência dos sistemas.

Embora o estudo tenha atingido seus objetivos ao analisar as estratégias de gerenciamento de riscos apresentadas na literatura especializada para mitigar falhas de programação e incompatibilidades de equipamentos em projetos de automação industrial, é importante reconhecer que limitações, como a falta de acesso a dados operacionais reais, podem ter influenciado a abrangência das análises realizadas.

Em resumo, este trabalho contribui para o entendimento dos desafios associados ao gerenciamento de riscos em projetos de automação e oferece diretrizes práticas para profissionais da área, promovendo um avanço na confiabilidade e eficiência dos sistemas automatizados.

Recomenda-se que trabalhos futuros explorem estudos empíricos e ampliem a integração de ferramentas de inteligência artificial para diagnóstico e previsão de falhas.

REFERÊNCIAS

ABECOM. **Qual o impacto do desgaste nos equipamentos industriais?** ABECOM. 2023. Disponível em: https://www.abecom.com.br/impacto-do-desgaste-nos-equipamentos. Acesso em: 27 jan. 2025.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000:2018: Gestão de Riscos - Diretrizes**, 28 mar. 2018.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR IEC 61511-1: Segurança funcional — Sistemas instrumentados de segurança para o setor da indústria de processo — Parte 1: Estrutura, definições, sistema, hardware e requisitos de programação do aplicativo**, 14 mar. 2024.

ALVAREZ, Jesús. **Conheça os principais impactos da indústria no meio ambiente**. Checklist Fácil. 2021. Disponível em: https://checklistfacil.com/blog/impactos-da-industria-no-meio-ambiente/. Acesso em: 27 jan. 2025.

ALVES, José. **INTEGRAÇÃO DE HARDWARE E SOFTWARE EM UM SISTEMA AUTOMATIZADO PARA ARRECADAR DOAÇÕES**. Cajazeiras Trabalho de Conclusão de Curso (TECNOLOGIA EM AUTOMAÇÃO INDUSTRIAL) - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, 2020.

AQUINO, Fagner. **Plataforma de baixo custo utilizada como ferramenta para análise de viabilidade na automação indústria**. In: Revista Científica Multidisciplinar, Maio 2021.

ROCKWELL AUTOMATION**. Gerenciamento de riscos na automação industrial** . Rockwell Automation, 2022. Disponível em: https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/gmsn-wp004_-pt-p.pdf. Acesso em: 27 jan. 2025.

BERTUZZI, Thiago. **Desenvolvimento Seguro, S-SDLC**. DEV. 2023. Disponível em: https://dev.to/tbertuzzi/desenvolvimento-seguro-s-sdlc-1n4f. Acesso em: 30 jan. 2025.

BRASIL**.** Ministério do Trabalho e Previdência. **Norma Regulamentadora nº 12 – Segurança no Trabalho em Máquinas e Equipamentos.** Atualizada em 2022. Disponível em: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-

tripartite-partitaria-permanente/arquivos/normas-regulamentadoras/nr-12-atualizada-2022-1.pdf. Acesso em: 22 abril. 2025.

CALLEAM CONSULTING. **Case Study – Denver International Airport Baggage Handling System – An illustration of ineffectual decision making**. Calleam Consulting. 2008. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://calleam.com/WTPF/wp-content/uploads/articles/DIABaggage.pdf?utm_source. Acesso em: 30 jan. 2025.

CAVALLIN, Fernando. **ESTUDO SOBRE REDES DE COMUNICAÇÃO PARA AUTOMAÇÃO INDUSTRIAL**. CURITIBA, 2016 Monografia - Universidade Tecnológica Federal do Paraná.

CEFOSPE - CENTRO DE FORMAÇÃO DOS SERVIDORES E EMPREGADOS PÚBLICOS DO ESTADO DE PERNAMBUCO. **Gerenciamento de Riscos em Projetos**. Recife, 2020. Disponível em: https://www.cefospe.pe.gov.br/images/media/1665419818_Apostila%20Gerenciamento%20de%20Riscos%20em%20Projetos.pdf. Acesso em: 19 dez. 2024.

CHAVES, Amanda. **Bowtie: Gestão de riscos visual e eficaz**. Docnix. 2024. Disponível em: https://docnix.com.br/ferramentas-metodos/bowtie-gestao-de-riscos-visual-e-eficaz/. Acesso em: 30 jan. 2025.

CHECKPOINT. **What is Secure SDLC?** Disponível em: https://www.checkpoint.com/pt/cyber-hub/cloud-security/what-is-secure-sdlc. Acesso em: 30 jan. 2025.

CIM AUTOMAÇÃO. **6 principais desafios da automação industrial. CIM Automação**, 2022. Disponível em: https://blog.cimautomacao.com.br/6-principais-desafios-da-automacao-industrial/. Acesso em: 28 jan. 2025.

COSTA, Rebeca. **Problemas causados pela falta de integração**. FIQON, 2023. Disponível em: https://fiqon.com.br/problemas-causados-pela-falta-de-integracao. Acesso em: 30 jan. 2025.

COSTA, Silvio. **Sistema Legado: principais características**. Lyncas, 2024. Disponível em: https://lyncas.net/blog/sistema-legado-principais-caracteristicas/. Acesso em: 30 jan. 2025.

CRESWELL, John W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 3. ed. Porto Alegre: Artmed, 2010.

CYRINO, Luis. **Análise da Árvore de Falhas**. 2025. Disponível em: https://tractian.com/blog/analise-da-arvore-de-falhas. Acesso em: 30 jan. 2025.

DEXYI. **Sensores Ópticos Balluff: Elevando a Precisão e Eficiência na Indústria**. DEXYI. Disponível em: https://dexyi.com.br/tipo/automacao-industrial/. Acesso em: 28 jan. 2025.

DRUCKER, Peter. **Gerenciando em tempos turbulentos**. Nova York: Harper & Row, 1980.

ELITE SOLDAS E ROBÓTICA. **Desafios na automação industrial**. Disponível em: https://www.elitesoldaserobotica.com.br/blog/desafios-na-automacao-industrial. Acesso em: 30 jan. 2025.

FERNANDES, Pedro; RABECHINI JR, Roque. **GESTÃO DE RISCOS NA ABORDAGEM ÁGIL E O SUCESSO DE PROJETOS**. In: Revista Gestão e Tecnologia, v. 23, n. 1, p. 138-16, 2023.

FERRAREZI, Rodrigo Cesar *et al*. **Framework para o desenvolvimento de programas de controles de SIS baseado na norma IEC 61511**. São Paulo, 2014 - Escola Politécnica da Universidade de São Paulo.

FILDES, Jonathan. **O worm Stuxnet 'tinha como alvo ativos iranianos de alto valor'**. BBC News. 2010. Disponível em: https://www.bbc.com/news/technology-11388018. Acesso em: 30 jan. 2025.

FLEXBOR. **Importância da segurança na automação industrial**. 2024. Disponível em: https://flexbor.com/importancia-da-seguranca-na-automacao-industrial/. Acesso em: 24 fev. 2025.

FOGAÇA, Frederson; DIAS, Andre; SILVA, Frederico. **A importância da análise de falhas para o ensino técnico em automação industrial**. 2021. Disponível em: https://publicacoes.ifc.edu.br/index.php/metapre/article/download/2261/1796/7894#:~:text=A%20import%C3%A2ncia%20desse%20tipo%20de,produ%C3%A7%C3%A3o%20ou%20inefici%C3%AAncias%20no%20processo. Acesso em: 30 jan. 2025.

FORTINET. **O que é integridade de dados?** Fortinet, 2025. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/data-integrity. Acesso em: 27 jan. 2025.

FRANÇA, Vitor. **DESAFIOS ENERGÉTICOS EM TREINAMENTO DE MODELOS DE IA**. GOIÂNIA Trabalho de Conclusão de Curso (Ciência da

Computação) - Escola Politécnica e de Artes da Pontifícia Universidade Católica de Goiás, 2024.

AVETIS, Grigoryan. **Workflow Automation**. LATENODE, 2024. Disponível em: https://latenode.com/pt-br/blog/workflow-automation. Acesso em: 28 jan. 2025.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

GRUPO FILTROIL. **Falhas em equipamentos industriais mais comuns**. FILTROIL, 2025. Disponível em: https://grupofiltroil.com.br/oleos-industriais/falhas-em-equipamentos-industriais-mais-comuns/. Acesso em: 30 jan. 2025.

HILLSON, David. **Managing Risk in Projects**: Fundamentals of Project Management. Routledge, 2016.

Hill, T. & Westbrook, R. (1997). **SWOT analysis: It's time for a product recall**.

IBM. **Fault Tree Analysis**. Disponível em: https://www.ibm.com/br-pt/topics/fault-tree-analysis. Acesso em: 30 jan. 2025.

IHI. **FMEA (Análise de Modos de Falhas e Efeitos)**. Disponível em: https://www.ihi.org/sites/default/files/202309/FMEA_Portugu%C3%AAs.pdf? Acesso em: 30 jan. 2025.

IN-COM. **Abordando as consequências da falta de tratamento adequado de erros no desenvolvimento de software**. IN-COM, 2024. Disponível em: https://www.in-com.com/pt/blog/proper-error-handling-software-development/. Acesso em: 27 jan. 2025.

NEPIN ENGENHARIA. **Indústria e meio ambiente: O que a indústria tem feito para minimizar os impactos no planeta**. Nepin. 2023. Disponível em: https://www.nepin.com.br/blog/industria/industria-e-meio-ambiente-o-que-a-industria-tem-feito-para-minimizar-os-impactos-no-planeta/. Acesso em: 27 jan. 2025.

INFRASPEAK. **Tempo de parada não planejado: causas, consequências e soluções**. Infraspeak. 2023. Disponível em: https://blog.infraspeak.com/pt-br/tempo-de-parada-nao-planejado. Acesso em: 27 jan. 2025.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems**. Geneva: IEC, 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61511: Functional safety – Safety instrumented systems for the process industry sector**. Geneva: IEC, 2016.

KAIZEN®. **Análise FMEA: gestão de riscos eficiente**. Disponível em: https://kaizen.com/pt/insights-pt/analise-fmea-gestao-riscos-eficiente. Acesso em: 30 jan. 2025.

KERZNER, Harold. **Project Management: A Systems Approach to Planning Scheduling and Controlling, 2e**, f. 469. 2006. 937 p.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, 2003.

LOCHBAUM, Dave. **Nuclear Plant Accidents: Browns Ferry Fire**. Union of Concerned Scientists. 2016. Disponível em: https://blog.ucsusa.org/dlochbaum/nuclear-plant-accidents-browns-ferry-fire/#:~:text=The%20March%2022%2C%201975%2C%20fire,1%20reactor%20close%20to%20meltdown. Acesso em: 30 jan. 2025.

MAGALHÃES, Carlos. **Os problemas da Baixa Qualidade de Dados**. Dio. 2024. Disponível em: https://www.dio.me/articles/os-problemas-da-baixa-qualidade-de-dados. Acesso em: 27 jan. 2025.

MARTINS**,** Aryana. **Diretrizes para gestão de riscos com base na ISO 31000**. Blog da Qualidade, 2022. Disponível em: https://blogdaqualidade.com.br/diretrizes-para-gestao-de-riscos-com-base-na-iso-31000. Acesso em: 30 jan. 2025.

MÁXIMA. **Desenvolvimento Industrial: A Importância das Normas Técnicas na Garantia de Qualidade e Segurança**. Máxima. 2024. Disponível em: https://maximasi.com.br/blog/ler/96? Acesso em: 27 jan. 2025.

MINETTO, Bianca. **Matriz de Riscos (Matriz de Probabilidade e Impacto)**. 2019. Disponível em: https://ferramentasdaqualidade.org/matriz-de-riscos-matriz-de-probabilidade-e-impacto/. Acesso em: 3 jan. 2025.

MÜLLER, Ralf; TURNER, Rodney. The Influence of Project Managers on Project Success Criteria and Project Success by Type of Project. **European Management Journal**, 04 agosto 2007.

MURRELEKTRONIK. **Passos para otimizar a monitoração de falhas em sistemas de automação industrial**. Murrelektronik. 2023. Disponível em: https://blog.murrelektronik.com.br/falhas-em-sistemas-de-automacao/?utm_source. Acesso em: 27 jan. 2025.

MURRELEKTRONIK. **Sistemas Automatizados: passos para uma segurança eficaz**. Murrelektronik. 2024. Disponível em: https://blog.murrelektronik.com.br/sistemas-automatizados/? Acesso em: 27 jan. 2025.

OLIVEIRA, Diego. **Como a Automação Reduz Custos e Aumenta a Eficiência na Produção**. DF Robótica. 2024. Disponível em: https://dfrobotica.com/como-a-automacao-reduz-custos-e-aumenta-a-eficiencia-na-producao/?utm_source. Acesso em: 27 jan. 2025.

OLIVEIRA, Helton Luiz Santana. **Implementação do Bowtie como Ferramenta de Gestão de Riscos em uma Termoelétrica**. 2022. Trabalho de Conclusão de Curso (Graduação em Engenharia de Produção) – Universidade Federal Fluminense, Niterói, 2022. Disponível em: https://app.uff.br/riuff/handle/1/29754. Acesso em: 30 jan. 2025.

PLANAS, Oriol. **Acidente nuclear de Three Mile Island, Estados Unidos**. Energia Nuclear. 2010. Disponível em: https://pt.energia-nuclear.net/acidentes-nucleares/three-mile-island?utm_source. Acesso em: 30 jan. 2025.

POLO ELETRÔNICA. **Como resolver problemas de conexão com redes industriais em IHMs?** Polo Eletrônica, 2022. Disponível em: https://poloeletronica.com.br/glossario/como-resolver-problemas-de-conexao-com-redes-industriais-em-ihms/? Acesso em: 27 jan. 2025.

POLO ELETRÔNICA. **O que é erros de Comunicação em Redes Industriais?** Polo Eletrônica, 2022. Disponível em: https://poloeletronica.com.br/glossario/o-que-e-erros-de-comunicacao-em-redes-industriais/. Acesso em: 28 jan. 2025.

PRADO. **Os principais erros na implementação de projetos de automação na indústria**. Prado Automação Industrial. Disponível em: https://pradoautomacaoindustrial.com.br/blog/erros-automacao-industria/. Acesso em: 30 jan. 2025.

PRITCHARD, Carl L. **Risk Management**: Concepts and Guidance, f. 122. 1996. 244 p. PROJECT MANAGEMENT INSTITUTE. **A Guide to the Project**

Management Body of Knowledge (PMBOK® Guide). 6 ed. Project Management, 2017.

PSICO-SMART. **Impacto da automação na produtividade das empresas**. Vorecol. 2025. Disponível em: https://psico-smart.com/pt/blogs/blog-impacto-da-automacao-na-produtividade-das-empresas-147667. Acesso em: 28 jan. 2025.c

QUINTANA, Anderson; FLORIAN, Fabiana; FIGUEIRA, Ronaldo. **ESTUDO COMPARATIVO DOS PROTOCOLOS DE COMUNICAÇÃO UTILIZADOS NA AUTOMAÇÃO RESIDENCIAL**. In: Revista Científica Multidisciplinar, v. 5, n. 11, novembro 2024.

RESEARCHGATE. **Investigation of Critical Failures Using Root Cause Analysis Methods: Case Study of ASH Cement PLC**. 2016. Disponível em: https://www.researchgate.net/publication/311652023_Investigation_of_critical_failures_using_root_cause_analysis_methods_Case_study_of_ASH_Cement_PLC. Acesso em: 27 jan. 2025.

RODRIGUES, Marcus Vinicius**. Ações para a qualidade: GEIQ gestão integrada para a qualidade: padrões seis sigma - classe mundial**. 2. ed. Rio de Janeiro: Qualitymark, 2004. ISBN 978-85-7303-473-8.

ROISENBERG, Leandro. **A Importância dos Protocolos de Comunicação na Indústria 4.0**. LDI. 2024. Disponível em: https://blog.lri.com.br/protocolos-de-comunicacao-na-industria-4-0/. Acesso em: 27 jan. 2025.

ROISENBERG, Leandro. **Linux em Sistemas de Controle Industrial: Vantagens, Desafios e Impacto na Inovação**. LRI. 2023. Disponível em: https://blog.lri.com.br/linux-em-sistemas-de-controle-industrial-vantagens-desafios-e-impacto-na-inovacao. Acesso em: 28 jan. 2025.

ROLPORT. **Desgaste prematuro de rolamentos: causas e como evitar**. Rolport. Disponível em: https://www.rolport.com.br/faq/desgaste-prematuro-de-rolamentos--causas-e-como-evitar-. Acesso em: 27 jan. 2025.

ROZENFELD, H; FRANIECK, E. K; ROZENFELD, H. **Avaliação da aplicação dos métodos FMEA e DRBFM no processo de desenvolvimento de produtos em uma empresa de autopeças**. Disponível em: <http://www.scielo.br/pdf/gp/v19n4/a13v19n4.pdf. Acesso em: 27 dez. 2024.

SCHWALBE, Kathy. **Information Technology Project Management**, f. 354. 2006. 708 p.

SIEMBRA. **FMEA: entenda o que é e suas vantagens**. Disponível em: https://www.siembra.com.br/noticias/fmea-entenda-o-que-e-e-suas-vantagens/. Acesso em: 30 jan. 2025.

SILVA, Hugo. **Perguntas e Respostas Sobre Projetos de Automação Industrial**. TNM Automations. 2023. Disponível em:

SILVA, Patrick; GAGNO JR, Antônio. **ANÁLISE DE FALHAS EM ATIVOS DE AUTOMAÇÃO COM AS TÉCNICAS FTA E FMEA**. 2011.

SILVEIRA, Samara. **A Importância da Dependabilidade em Sistemas de Software**. Casa do Desenvolvedor. 2024. Disponível em: https://blog.casadodesenvolvedor.com.br/dependabilidade-sotware/? Acesso em: 27 jan. 2025.

SIQUEIRA, Guilherme. **Manutenção Preventiva em Sistemas de Automação: Dicas para Evitar Paradas Não Programadas**. Polimaq. 2024. Disponível em: https://polimaqautomacao.com.br/manutencao-preventiva-em-sistemas-de-automacao-dicas-para-evitar-paradas-nao-programadas. Acesso em: 27 jan. 2025.

RICCE, Adeliana. **Qual é a importância da manutenção e seu impacto na qualidade de produtos e serviços?** SISMETRO, 2023**.** Disponível em: https://blog.sismetro.com/post/17/qual-e-a-importancia-da-manutencao-e-seu-impacto-na-qualidade-de-produtos-e-servicos. Acesso em: 30 jan. 2025.

SIMPLIFIER. **The 6 stages of Software Development – Part 1**. Simplifier. Disponível em: https://simplifier.io/en/the-6-stages-of-software-development/. Acesso em: 30 jan. 2025.

SKYONE. **Falta de integração de sistemas afeta equipe**. SKYONE, 2024. Disponível em: https://skyone.solutions/blog/falta-de-integracao-de-sistemas-afeta-equipe/. Acesso em: 30 jan. 2025.

SOUZA, Eric. **AUTOMAÇÃO DE SUBESTAÇÕES COM O PROTOCOLO IEC-61850: estudo de caso.** Monografia - Universidade Tecnológica Federal do Paraná, Curitiba, 2016.

TAGOUT. **FMEA: entenda o que é e quais são suas vantagens**. Disponível em: https://www.tagout.com.br/blog/fmea-entenda-o-que-e-e-quais-sao-suas-vantagens/. Acesso em: 30 jan. 2025.

TEIXEIRA, Ana Flávia; VISOTO, Nayanne; PAULISTA, Paulo Henrique. **AUTOMAÇÃO INDUSTRIAL: SEUS DESAFIOS E PERSPECTIVAS**. **FEPI**, v. 3, n. 2, 2016.

TS SHARA. **Downtime: Saiba o que é e como evitar na sua empresa**. Ts shara. 2024. Disponível em: https://tsshara.com.br/blog/falta-de-energia/downtime-saiba-o-que-e-e-como-evitar-na-sua-empresa/. Acesso em: 28 jan. 2025.

MALUF, Gabriela. **ISO 31000: o que é e qual o seu impacto?** UPLEXIS, 2023. Disponível em: https://uplexis.com.br/blog/artigos/iso-31000-o-que-e-e-qual-o-seu-impacto/. Acesso em: 30 jan. 2025.

VEDAN, Alex. **Prevenção de Falhas em Equipamentos: Guia para Alta Gestão**. 2025. Disponível em: https://tractian.com/blog/analise-da-arvore-de-falhas. Acesso em: 30 jan. 2025.