UNIVERSIDADE DE SÃO PAULO
ESCOLA POLITÉCNICA

ACÁSSIO MATHEUS ROQUE

Considerações sobre avaliação de risco e resiliência eletromagnética em sistemas elétricos e eletrônicos

São Paulo
2023

ACÁSSIO MATHEUS ROQUE

Considerações sobre avaliação de risco e resiliência eletromagnética em sistemas elétricos e eletrônicos

Versão Corrigida

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre de Ciências.

Área de Concentração: Sistemas de Potência

Orientador: Prof. Dr. Carlos Antonio França Sartori

São Paulo
2023

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 08 de Janeiro de 2023

Assinatura do autor: Acássio M. Roque

Assinatura do orientador: 

Catalogação-na-publicação

Roque, Acássio Matheus
Considerações sobre avaliação de risco e resiliência eletromagnética em sistemas elétricos e eletrônicos / A. M. Roque -- versão corr. -- São Paulo, 2023.
198 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Energia e Automação Elétricas.

1.Compatibilidade Eletromagnética 2.Resiliência Eletromagnética 3.Segurança Funcional 4.Gerenciamento de Risco 5.Sistemas Elétricos e Eletrônicos I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Energia e Automação Elétricas II.t.

Dissertação de autoria de Acássio Matheus Roque, sob o título "**Considerações sobre avaliação de risco e resiliência eletromagnética em sistemas elétricos e eletrônicos**", apresentada à Escola Politécnica da Universidade de São Paulo, para obtenção do título de Mestre em Ciências do Programa de Pós-Graduação em Engenharia Elétrica, na área de concentração Sistemas de Potência, aprovada em 23 de novembro de 2022 pela comissão julgadora constituída pelos doutores:

Prof. Dr.: Carlos Antonio França Sartori

Instituição: Programa de Pós-graduação em Engenharia Elétrica – PEA/EPUSP

Presidente

Prof. Dr.: Mário Leite Pereira Filho

Instituição: Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A. – IPT

Prof. Dr.: Jamilson Ramos Evangelista

Instituição: Agência Nacional de Telecomunicações – ANATEL

Agradecimentos

Primeiramente, agradeço à dádiva da vida que me foi concedida. Agradeço ao meu orientador, Prof. Dr. Carlos Antonio França Sartori, pela coordenação deste trabalho, pela amizade e pelas conversas semanais.

À Universidade de São Paulo e ao Programa de Pós-graduação em Engenharia Elétrica (PPGEE) da Escola Politécnica pela oportunidade.

À minha família, em especial aos meus pais e irmãos, por todo o amor e disponibilidade concedidas.

À minha esposa Barbara Macedo, pelo carinho, paciência e momentos compartilhados.

Aos colegas de trabalho do CTMSP e Amazul, por dividirem boa parte dos meus dias e pelo conhecimento compartilhado.

Aos meus sinceros amigos, por tornarem minha vida melhor.

Á todos que, direta ou indiretamente, colaboraram durante o desenvolvimento deste trabalho.

Resumo

ROQUE, Acássio Matheus. **Considerações sobre avaliação de risco e resiliência eletromagnética em sistemas elétricos e eletrônicos**. 2023. 198 p. Dissertação (Mestrado em Ciências) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2023.

O crescente uso de tecnologias elétricas e eletrônicas tem ampliado o ambiente eletromagnético, ao mesmo tempo que as novas tecnologias podem ser suscetíveis à interferência eletromagnética (EMI). Isso representa uma grande preocupação para a aplicação de equipamentos elétricos e eletrônicos em sistemas de segurança, já que falhas e mau funcionamento causados por EMI nesses sistemas podem afetar, além dos aspectos operacionais, a segurança humana e ambiental. Neste contexto, a obtenção de segurança funcional em relação às perturbações eletromagnéticas, conhecida como resiliência eletromagnética, é obrigatória para prevenir a ocorrência de incidentes e acidentes. O processo para alcançar a resiliência eletromagnética é constituído de diversas etapas, sendo a avaliação de risco, uma das mais importantes. Embora muitas técnicas de determinação de risco tenham sido estudadas e regras gerais para sua seleção tenham sido desenvolvidas, poucos resultados são observados, no que tange ao estabelecimento de metodologias para avaliar técnicas de determinação de risco adequadas ao conceito de resiliência eletromagnética. Este trabalho apresenta uma proposta de estrutura para selecionar técnicas de determinação de risco adequadas à obtenção de resiliência eletromagnética de sistemas elétricos e eletrônicos. A definição dos critérios específicos tem como consideração inicial as dificuldades fundamentais encontradas no campo de resiliência eletromagnética relatadas na literatura. Neste trabalho, a formulação do problema de seleção e análise comparativa entre os métodos de avaliação de risco selecionados são realizadas usando o *Analytical Network Process* – ANP. A pré-seleção das técnicas de determinação de risco é realizada a partir de uma revisão sistemática de mais de 80 técnicas, tendo como base mais de 1400 artigos científicos pré-selecionados. Para ilustrar a metodologia de seleção, apresenta-se, como exemplo, resultados obtidos a partir de uma aplicação em um sistema de cadeira de rodas motorizada, onde comparam-se três métodos de avaliação de risco: a Análise de Modo de Falha e Efeito (FMEA), Análise de Árvore de Falha (FTA) e o *Systems Theoretic Accident Model and Process* (STAMP).

Palavras-chave: Compatibilidade Eletromagnética, Resiliência Eletromagnética, Segurança Funcional, Gerenciamento de Risco, Sistemas Elétricos e Eletrônicos.

Abstract

ROQUE, Acássio Matheus. **Considerations of risk assessment and electromagnetic resilience for electrical and electronic systems**. 2023. 198 p. Dissertation (Master of Science) – Polytechnic School, University of São Paulo, São Paulo, 2023.

The growing use of electrical and electronic technologies has amplified the electromagnetic environment at the same time as modern technologies can be susceptible to electromagnetic interference (EMI). This represents a major concern for the application of electrical and electronic equipment in safety-related systems since faults and malfunctioning caused by EMI in these systems can affect, besides the operational aspects, human and environmental safety. In this context, the achievement of functional safety regarding electromagnetic disturbances, known as electromagnetic resilience, is mandatory to prevent the occurrence of incidents and accidents. The process to reach electromagnetic resilience is based on many steps, in which the risk assessment is one of high importance. Although many risk assessment techniques have been studied and general rules for their selection have been developed, few results have been obtained in relation to the establishment of methodologies to evaluate the relevance of risk assessment techniques for electromagnetic resilience. This work introduces a proposal for a framework to select suitable risk assessment techniques for achieving electromagnetic resilience of electrical and electronic systems. The definition of specific criteria has initially considered the fundamental difficulties encountered in the electromagnetic resilience field and described in literature. In this work, the formulation of the selection problem and the comparison analysis between the selected risk assessment are performed using the Analytical Network Process (ANP) method. A pre-selection of risk assessment techniques is performed by means of a systematic revision of literature which considered more than eighty techniques analyzed in more than 1400 papers previously selected. To illustrate the proposed selection methodology, it is presented, as an example, the results of an application with a motorized wheelchair comparing three well-known risk assessment methods: Failure Mode and Effect Analysis (FMEA), Failure Tree Analysis (FTA) and Systems Theoretic Accident Model and Process (STAMP).

Keywords: Electromagnetic Compatibility, Electromagnetic Resilience, Functional Safety, Risk Management, Electrical and Electronic Systems.

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

AAF	Análise de Árvore de Falhas
ACEC	*Advisory Committee on Electromagnetic Compatibility*
ACH	Avaliação de Confiabilidade Humana
AEA	*Action Error Analysis*
AFD	*Anticipatory Failure Determination*
AHI	*Accident Hazard Index*
AHP	*Analytic Hierarchy Process*
ALARA	*As Low As Reasonably Achievable*
ALARP	*As Low As Reasonably Practicable*
AMD	Apoio Multicritério à Decisão
ANP	*Analitycal Network Process*
ANSI	*American National Standards Institute*
APJ	*Absolute Probability Judgment*
APPCC	Análise de Perigos e Pontos Críticos de Controle
APR	Análise Probabilística de Riscos
APS	Avaliação Preliminar de Segurança
ASEP	*Accident Sequence Evaluation Program*
ASME	*American Society of Mechanical Engineers*
ASP	*Accident Sequences Precursor*
ASSP	*American Society of Safety Professionals*
ATHEANA	*Technique for Human Event Analysis*
ATSB	*Australian Transport Safety Bureau*
BASI	*Bureau of Air Safety Investigation*
BIA	*Business Impact Analysis*
BORA	*Barrier and Operational Risk Analysis*
CARA	*Controller Action Reliability Assessment*
CAST	*Causal Analysis based on System Theory*
CCA	*Cause-and-Consequence Analysis*
CCF	*Common Cause Failure*
CEM	Compatibilidade Eletromagnética
CHA	*Concept Hazard Analysis*
CISPR	*International Special Committee on Radio Interference*
CORA	*Cost-Of-Risk Analysis*
CREA	*Clinical Risk and Error Analysis*
CREAM	*Cognitive Reliability and Error Analysis Method*
CSR	*Concept Safety Review*
DFMEA	*Design Failure Mode and Effect Analysis*
DMRA	*Decision Matrix Risk-Assessment*
EFT	*Electrical Fast Transients*
ELECTRE	*Elimination Et Choix Traduisant la Realité*

EM	Eletromagnética
EMC	*Electromagnetic Compatibility*
EMI	*Electromagnetic Interference*
ESD	*Electrostatic Discharge*
ETA	*Event Tree Analysis*
ETE	*Estimate-Talk-Estimate*
FCC	*Federal Communication Comission*
FDA	*US Food and Drug Agency*
FHA	*Functional Hazard Analysis*
FIT	*Fault Insertion Testing*
FMEA	*Failure Mode and Effect Analysis*
FMECA	*Failure Mode, Effects, and Criticality Analysis*
FRAAP	*Facilitated Risk Analysis and Assessment Process*
FRAM	*Functional Resonance Analysis Method*
FRAP	*Facilitated risk analysis process*
FTA	*Failure Tree Analysis*
GOFA	*Goal-Oriented Failure Analysis*
HACCP	*Hazard Analyzis and Critical Control Points*
HAZID	*Hazard Identification*
HAZOP	*Hazard and Operability Studies*
HAZSCAN	*Hazardous Scenario Analysis*
HCR	*Human Cognitive Reliability Correlation*
HEART	*Human Error Assessment and Reduction Technique*
HEMP	*High-amplitude nuclear electromagnetic pulse*
HEP	*Human Error Potential*
HFACS	*Human Factors Analysis and Classification System*
HFEA	*Human Factor Event Analysis*
HIRA	*Hazard Identification and Ranking*
HPEM	*High Power Electromagnetics*
HRA	*Human Reliability Assessment*
HSE	*Health Service Executive*
HTA	*Hierarchical Task Analysis*
HTN	*Hierarchical Task Network*
ICI	*Imperial Chemical Industries*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IEICE	*Institute of Electronics, Information and Communication Engineers*
IEM	Interferência Eletromagnética
IEMI	Interferência Eletromagnética Intencional
IET	*Institution of Engineering and Technology*
ISA	*International Society of Automation*
ISO	*International Organization for Standardization*
ISS	*Injury Severity Score*
JHEDI	*Justified Human Error Data Information*

LOPA	*Layer of Protection Analysis*
MACBETH	*Measuring Attractiveness by a Categorical Based Evaluation Technique*
MAUT	*Multi-Attribute Utility Theory*
MCAA	*Maximum Credible Accident Analysis*
MCDA	*Multi-Criteria Decision Analysis*
MCDM	*Multi-Criteria Decision Making*
MLD	*Master Logic Diagram*
MOSAR	*Méthode Organisée et Systémique d'Analyse de Risques*
MTTF	*Mean Time To Failure*
NARA	*Nuclear Action Reliability Assessment*
NASA	*National Aeronautics and Space Administration*
NAT	*Normal Accident Theory*
NRC	*Nuclear Regulatory Comission*
OCTAVE	*Operationally Critical Threat, Asset and Vulnerability Evaluation*
OHS	*Occupational Health and Safety*
ORA	*Optimal Risk Assessment*
PEA	*Predictive, Epistemic Approach*
PFH	*Probability of Failure on Demand per Hour*
PFMEA	*Product Failure Mode and Effect Analysis*
PGR	Programa de Gerenciamento de Riscos
PHA	*Preliminary Hazard Analysis*
PRA	*Probabilistic Risk Assessment*
PROMETHEE	*Preference Ranking Organization METHod for Enrichment Evaluations*
PSA	*Probabilistic Safety Assessment*
RBD	*Reliability Block Diagrams*
RBM	*Risk-Based Maintenance*
RCM	*Reliability Centred Maintenance*
RFI	*Radio Frequency Interference*
RLI	*Risk Level Indicators*
RPN	*Risk Priority Number*
RRA	*Rapid Risk Assessment*
RRABD	*Rapid Risk Analysis Based Design*
RVA	*Risk and Vulnerability Analysis*
SCM	*Swiss Cheese Model*
SFAIRP	*So Far as is Reasonably Practicable*
SFMEA	*Software Failure Mode and Effect Analysis*
SGD	*Signed Directed Graph*
SHERPA	*Systematic Human Error Reduction and Prediction Analysis*
SHIPP	*System Hazard Identification, Prediction and Preventio*
SIL	*Safety Integrity Level*
SIS	Sistemas Instrumentados de Segurança
SLIM	*Success Likelihood Index Method*

SOD	*Severity, Occurence and Detection*
STAMP	*Systems-Theoretic Accident Model and Processes*
STEP	*Sequentially Timed Event Plotting*
STPA	*System Theoretic Process Analysis*
SWC	*Surge Withstand Capability*
SWIFT	*Structure « What if? »*
THERP	*Technique for Human Error Rate Prediction*
TOPSIS	*Technique for Order of Preference by Similarity to Ideal Solution*
TSECA	*Threat Scenario, Effect, and Criticality Analysis*
UPS	*Uninterruptible Power Systems*
WRA	*Weighted Risk Analysis*

Sumário

1 Introdução

1.1 Motivação

Os sistemas elétricos e eletrônicos desempenham, cada vez mais, papéis de grande relevância na sociedade atual. Eles estão presentes nas mais diversas aplicações, incluindo áreas sensíveis, como plantas nucleares, equipamentos eletromédicos, processos industriais etc., onde desempenham funções vitais relacionadas à segurança.

Sistemas como os mencionados acima seguem rígidos requisitos de operação e segurança recomendados por instituições nacionais e internacionais. Nota-se que grande parte das funções de segurança são executadas com o auxílio de sistemas elétricos e eletrônicos, que, por meio de equipamentos, tais como, controladores, atuadores e sensores, são responsáveis pelo processamento e controle de variáveis de processo, pela realização de acionamentos (como bombas, válvulas, motores, e outros equipamentos eletromecânicos), etc.

Nota-se, no entanto, que estes sistemas utilizam tecnologias que podem apresentar mau funcionamento e falhas que tendem a afetar suas funções primárias. Um dos aspectos peculiares a todas as tecnologias elétricas e eletrônicas é o nível de imunidade destes às interferências eletromagnéticas (IEM). As perturbações relacionadas as IEM têm sido observados desde o início do século XX, cujos eventos associados se intensificaram, principalmente, após a invenção dos componentes eletrônicos de alta densidade, como os circuitos integrados (PAUL, 2006). Atualmente, menciona-se que a aplicação, em ampla escala, de determinadas tecnologias, tais como comunicações sem fios, conversores de frequência etc., contribui significativamente para alterar o ambiente eletromagnético das instalações relacionadas (INSTITUTION OF ENGINEERING AND TECHNOLOGY, 2013). Assim, a necessidade de avaliações de sistemas e equipamentos elétricos, com o objetivo de se minimizar contribuições das perturbações conduzidas e radiadas, visando-se adequar os ambientes eletromagnéticos resultantes aos níveis de imunidade destas, passa a assumir uma importância primordial para garantir o funcionamento adequado e seguro destes. Desta forma, a busca pela garantia da imunidade dos equipamentos nos ambientes eletromagnéticos nos quais estão instalados, é fundamental para o correto funcionamento de sistemas relacionados e importantes para segurança.

Diversos guias e normas internacionais apresentam diretrizes, recomendações e requisitos para testes e avaliação de compatibilidade eletromagnética (CEM)

(INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2022) (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019) (US DEPARTMENT OF DEFENSE, 2015). Nota-se, porém, que estes testes avaliam o desempenho de sistemas considerando-se eventos e perturbações isoladas, diferente dos diversos ambientes onde eventos combinados, tanto os resultantes de ação de seres humanos, bem como de eventos físicos mecânicos, térmicos e eletromagnéticos, podem ocorrer. Deve-se observar que a magnitude e distribuição das possíveis fontes de perturbações são difíceis de serem previstas com precisão. Menciona-se, também, que falhas e maus funcionamentos causados por IEM são geralmente transitórios, não deixando claras evidências de sua ocorrência, causando dificuldades na sua identificação.

Neste contexto, a análise de segurança, dita funcional, de sistemas elétricos e eletrônicos, em particular quando associado aos eventos de IEM, assume grande interesse e importância atual. Os sistemas relacionados à segurança necessitam ser robustos, com níveis de imunidade adequados durante toda o seu ciclo de vida, mesmo quando consideradas diferentes perturbações EM, que possam ocorrer simultaneamente, ou como a combinação de perturbações EM com outros eventos físicos, tais como, corrosão, envelhecimento, má utilização dos equipamentos e operações indevidas, etc.

A segurança funcional pode ser entendida como uma parte da segurança geral, sendo relacionada a sistemas que apresentam atuação ou realizam controle de processos que dependem do correto funcionamento do sistema elétrico de segurança e de outras camadas de proteção. Deste modo, a segurança funcional está relacionada aos sistemas ativos, tendo como objetivo obter sistemas de segurança capazes de prevenir falhas perigosas ou formas de controlá-las, caso ocorram. Enfatiza-se que meios, que alcançam segurança por meio de sistemas passivos, não são classificados como de segurança funcional (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010).

Os princípios e requisitos básicos da segurança funcional para sistemas elétricos e eletrônicos podem ser encontrados na norma IEC 61508, “Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related System” (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010). Menciona-se que os aspectos de segurança funcional específicos relacionados à compatibilidade eletromagnética (CEM) encontram-se na norma IEC 61000-1-2, “Electromagnetic compatibility (EMC): General - Methodology for the Achievement of Functional Safety of Electrical and Electronic Systems Including Equipment with Regard to Electromagnetic Phenomena” (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016), que apresenta um guia para a avaliação dos efeitos dos ambientes eletromagnéticos nos sistemas elétricos relacionados à segurança, introduzindo diversos

requisitos e recomendações técnicas para alcançar os níveis de segurança funcional desejados, quando da ocorrência de perturbações EM. Esta abordagem implica na adoção de técnicas e métodos, desde o projeto até o momento do comissionamento (incluindo gestão, especificação etc.), para alcançar níveis desejados de segurança, ressaltando-se aquelas relacionadas à obtenção de CEM.

O conceito da consideração do gerenciamento de riscos funcionais em relação às perturbações eletromagnéticas pode ser chamado, de forma mais sucinta, de resiliência eletromagnética (ARMSTRONG e DUFFY, 2020). Esse conceito foi apresentado no guia prático da *Institution of Engineering and Technology* (IET) (INSTITUTION OF ENGINEERING AND TECHNOLOGY, 2017) que apresenta uma abordagem com os passos recomendados para cumprir os requisitos impostos na norma acima-citada IEC 61000-1-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016), tendo sido a inspiração para a recém-publicada norma IEEE 1848 (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 2020). Esta relaciona um conjunto de métodos práticos para auxiliar no gerenciamento dos níveis de risco devido às perturbações eletromagnéticas considerando-se todo o ciclo de vida dos equipamentos e sistemas eletrônicos.

Uma das etapas indicadas na base normativa para obtenção de segurança funcional está fundamentada na determinação de riscos. Essa etapa deve ser iniciada nas primeiras fases do projeto, sendo passo essencial para a posterior determinação das especificações de requisitos de segurança. Atualmente, as ferramentas tradicionais mais utilizadas para avaliação de riscos tem como base o conceito de cadeia de eventos. Ou seja, considera-se que os acidentes ocorrem devido a uma sequência de múltiplos eventos, que culminam em uma falha. Essas análises, que incluem avaliações diretas (como nas Árvores de Eventos ou nas Análises de Modos de Falha e Efeitos) ou inversas (Árvores de Falha), possuem grande aplicação, tendo, entretanto, limitações quando aplicadas a sistemas muito complexos ou na consideração de riscos decorrentes de interações de subsistemas. Entretanto, diversos outros métodos de avaliação de risco com abordagens adaptativas de gerenciamento de risco têm sido introduzidos, onde menciona-se, por exemplo, os métodos com base na engenharia de resiliência, tais como, o método FRAM (*Functional Ressonance Analysis Method*), o método STAMP (*System-Theoretic Accident Model and Processes*) e o método AcciMap, etc. (UNDERWOOD e WATERSON, 2012).

Ressalta-se, assim, a importância da busca de metodologias adequadas, que possam ser aplicadas na análise e avaliação de segurança funcional e de compatibilidade eletromagnética

dos sistemas elétricos e eletrônicos atuais, de modo que as dificuldades existentes e apontadas em literatura possam ser superadas.

1.2 Objetivos

Este trabalho tem como objetivo apresentar uma análise sobre as técnicas de determinação de risco a serem utilizadas nas avaliações de segurança funcional de sistemas elétricos e eletrônicos, abordando-se as metodologias tradicionais e atuais. Em particular, devido à importância atual dos tópicos de compatibilidade eletromagnética, ênfase será dada para as metodologias que possam se adequar a consideração dos aspectos de resiliência eletromagnética na análise de segurança destes sistemas. A partir de uma análise preliminar das principais técnicas de avaliação de risco e das dificuldades na área de resiliência eletromagnética apontadas em literatura, um procedimento para seleção de técnicas de determinação de risco adequadas para as avaliações de resiliência eletromagnética é apresentado, sendo utilizado, de maneira ilustrativa, em uma aplicação prática em um sistema elétrico ou eletrônico.

Entre os objetivos específicos e suas respectivas etapas de estudo, destacam-se os seguintes:

1. Análise de métodos para a determinação de riscos aplicáveis à segurança funcional abordando-se:
    - Revisão bibliográfica dos principais métodos descritos em literatura;
    - Revisão sistemática das técnicas de determinação de risco;
2. Definição de critérios para classificação das técnicas de determinação de risco, incluindo-se:
    - Critérios gerais relacionados à avaliação de risco;
    - Critérios específicos relacionados à resiliência eletromagnética;
3. Identificação de métodos de apoio multicritério à decisão para seleção ou hierarquização das técnicas da determinação de risco com base nos critérios específicos definidos;
4. Aplicação do procedimento proposto de seleção de técnicas de determinação de risco em uma aplicação de um sistema elétrico ou eletrônico.

1.3 Estrutura do Texto

Este trabalho divide-se em 5 capítulos. No primeiro capítulo, apresenta-se a motivação e importância dos tópicos considerados nesta dissertação, definindo-se os principais objetivos e tópicos a serem avaliados.

O capítulo 2 apresenta a revisão bibliográfica dos temas abordados neste trabalho. Apresenta-se uma breve evolução dos temas de compatibilidade eletromagnética, segurança funcional e resiliência eletromagnética. São descritos os aspectos históricos e principais normas destes tópicos, sendo estabelecido a relação entre eles. Algumas técnicas reconhecidas aplicáveis na determinação de risco são brevemente discutidas.

O capítulo 3 apresenta a metodologia a ser aplicada na avaliação de técnicas para a determinação de riscos em relação à tópicos de compatibilidade eletromagnética, úteis na análise de segurança funcional de sistemas elétricos e eletrônicos. Um procedimento de seleção de técnicas de determinação de risco para resiliência eletromagnética é proposto, sendo definidos os critérios gerais e específicos para utilização na seleção. Ainda são apresentados métodos de apoio multicritério à decisão para utilização no procedimento proposto.

O capítulo 4 apresenta um exemplo ilustrativo considerando-se uma avaliação de risco para o sistema elétrico e eletrônico de uma cadeira de rodas motorizada, sendo a aplicação e seus resultados discutidos na sequência. Posteriormente, são exibidos os resultados da revisão sistemática das técnicas de determinação de risco e é realizada a aplicação do procedimento proposto de seleção de técnicas de determinação de risco em relação a sua adequação para a análise de segurança funcional e compatibilidade eletromagnética, a partir de critérios específicos relacionados à resiliência eletromagnética.

O capítulo 5 destaca os principais resultados obtidos e avalia as principais contribuições deste trabalho, sendo consideradas ainda sugestões de trabalhos futuros relacionados à continuação do desenvolvimento do tema proposto.

As referências bibliográficas utilizadas no texto são então apresentadas, seguidas dos anexos.

2 Revisão Bibliográfica

Este capítulo apresenta uma revisão das principais publicações científicas relacionadas ao tema em estudo neste trabalho, iniciando-se com um histórico da área de compatibilidade eletromagnética e identificando-se suas bases normativas. A segurança funcional é, então, avaliada, estabelecendo-se uma relação com o tema de CEM: a resiliência eletromagnética.

Enfatiza-se, na sequência, a evolução histórica, o estágio atual e as perspectivas futuras das metodologias de análise de risco aplicáveis aos sistemas elétricos e eletrônicos para a avaliação de segurança funcional e os aspectos de resiliência eletromagnética. São descritos, ainda, a origem e as principais publicações das técnicas de determinação de risco consideradas nas seções anteriores.

Ao final, apresenta-se os princípios metodológicos com uma breve explanação sobre os conceitos fundamentais de CEM e os seus principais aspectos. Posteriormente, ressaltam-se os procedimentos recomendados para a avaliação de segurança funcional de sistemas elétricos e eletrônicos em relação aos aspectos eletromagnético, ou seja, para obtenção de resiliência eletromagnética, sendo, em particular, ressaltada uma de suas etapas: a determinação de risco. Na sequência,

2.1 Histórico e Evolução da Área de Compatibilidade Eletromagnética

Embora relatos de interferência eletromagnética (IEM) existam desde os primórdios das comunicações de rádio e telégrafo, os primeiros artigos abordando perturbações eletromagnéticas surgiram na década de 1920 e apresentavam os principais aspectos relacionados ao aumento dos eventos, como principais fontes de IEM (a própria indústria do rádio, equipamentos, linhas de transmissão, cargas comerciais conectadas à rede, circuitos residenciais, etc.), operações indevidas, questões financeiras decorrentes e discussões sobre medidas de mitigação (MARRIOTT, 1923) (CORBETT, 1925) (ALLEN, 1929). O surgimento da preocupação com a IEM pode ainda ser verificada na apresentação das primeiras patentes sobre métodos para garantir a continuidade metálica e a integridade de blindagens (OLAF, 1928).

Durante a Segunda Guerra Mundial, o uso de equipamentos de rádio, navegação e radar aumentou de forma expressiva. Casos de interferência eletromagnética entre estes dispositivos eram geralmente corrigidos com a readequação da banda de frequência para operação, afastamento de cabos das possíveis fontes emissoras, etc. Essas soluções pontuais eram

possíveis devido à baixa densidade de equipamentos. Após a invenção dos transistores nos anos de 1950 e dos componentes eletrônicos de alta densidade, tais como os circuitos integrados, nos anos de 1960, observou-se um aumento significativo dos problemas de interferência e verificou-se a necessidade de um planejamento do uso de espectros específicos de frequência, da utilização de medidas de controle para as emissões eletromagnéticas e das características de operações, tais como faixas de frequências de operação (PAUL, 2006).

Nota-se que já em 1934, a *International Electrotechnical Comission* (IEC) criou um comitê especial para abordar problemas emergentes de EMI, chamado de *International Special Committee on Radio Interference* (CISPR). A CISPR elaborou diversos documentos específicos sobre requisitos, técnicas de medição e limites de emissão de sinais conduzidos e radiados que passaram a ser utilizados por diversos países na Europa. Da mesma forma, a *Federal Communications Commission* (FCC), a agência independente do Governo dos Estados Unidos que regula as comunicações nesse país, publicou em 1979, uma regulamentação geral para todos os dispositivos eletrônicos, seguindo os limites recomendados pela CISPR.

Ressalta-se que antes mesmo das publicações anteriores, a indústria já aplicava normas e limites, de maneira voluntária, para evitar problemas de IEM. As instituições militares americanas adotavam limites de emissão eletromagnética para os sistemas eletrônicos desde o início da década de 60, através das primeiras versões das normas MIL-STD (US DEPARTMENT OF DEFENSE, 2015). É oportuno destacar que a norma militar já abordava a adoção de níveis de imunidade eletromagnética, indo além da adoção de medidas de controle de emissões ao ambiente eletromagnético.

Tendo como base o histórico apresentado, pode-se compreender a utilização do termo de interferência de rádio frequência (do inglês, *radio frequency interference* – RFI) dada pelos engenheiros nas primeiras observações. Atualmente, o termo interferência eletromagnética é mais adequado para se referir ao fato de os sistemas elétricos e eletrônicos sofrerem degradação e causar perturbações em uma faixa de frequência muito abrangente (0Hz a alguns GHz).

A compatibilidade eletromagnética possui um longo histórico de estudos que abrangem diversos campos de aplicação, realizados através de artigos científicos publicados nas principais revistas científicas relacionadas, tais como IEEE Transactions on Electromagnetic Compatibility, IEEE Electromagnetic Compatibility Magazine, IEICE Transaction on Communications, IEEE Transactions on Power Electronics, entre outras. Além dos artigos científicos, consideração especial deve ser dada aos livros publicados por Henry Ott, que ainda nos anos 70 publicou uma das principais referências da área (OTT, 1976), sendo sua versão mais atualizada (OTT, 2009) considerada por muitos a bíblia da CEM; e por Clayton R. Paul,

que em 1992 publicou a primeira versão de *"Introduction to Electromagnetic Compatibility"* (PAUL, 2006). Embora esses livros possam ser considerados as obras mais acessadas e utilizadas como texto-base em universidade e como referência para engenheiros atualmente, abordando diversos temas relacionados, como conceitos básicos, normas e requisitos técnicos visando obter CEM, outras importantes publicações podem ser também destacadas (CHATTERTON e HOULDEN, 1991) (PEREZ, 1995).

Atualmente, a área de compatibilidade eletromagnética assume uma importância especial, sendo considerada já na etapa de concepção de sistemas elétricos e eletrônicos, visando garantir os aspectos operacionais e de segurança a estes relacionados. A fim de ilustrar a dimensão dos eventos de IEM, pode se citar, por exemplo, a publicação realizada por Keith Armstrong (ARMSTRONG, 2014). Nesta publicação são compilados mais de 500 casos de IEM de diversos níveis de complexidade, tais como eventos de atrasos ocasionados em trens causados pelas IEM de linhas de potência que afetavam a indicação luminosa dos sinais de via, exemplos de EMI com sistemas de controle e instrumentação afetando tanto os aspectos operacionais como os de segurança de sistemas complexos. Sabe-se que a preocupação com interferências eletromagnéticas para estes sistemas é crescente devido ao seu uso em diversas aplicações que requerem alto nível de segurança, considerando-se que o ambiente eletromagnético das instalações atuais está em constante alteração devido ao uso de novas aplicações e tecnologias, como conexões sem-fio, conversores de frequência, etc.

Percebe-se, portanto, que a evolução de eventos de IEM com a introdução de inovações tecnológicas e popularização de equipamentos eletrônicos demandou o desenvolvimento de normas e diretivas de diversas fontes no sentido de controlar a emissão de equipamentos e o ambiente eletromagnético para garantir o bom funcionamento de equipamentos nos meios eletromagnéticos nos quais eles estão inseridos. A evolução dos tópicos de CEM se confundem em muitos casos com o próprio desenvolvimento dos guias técnicos e normas internacionais para a adequação dos projetos em relação aos requisitos legais impostos pelas agências governamentais, regulamentações comerciais ou boas práticas exigidas.

2.2 Normas Aplicáveis à Compatibilidade Eletromagnética (CEM)

Dentre as organizações internacionais, a IEC se destaca por possuir diversos comitês e manter relações ou parcerias com associações profissionais e organizações regionais, nacionais e internacionais. Estes comitês são: o Comitê Técnico 77 (TC77) e a CISPR (Comitê Internacional Especial de Perturbações Radioelétricas), ambos responsáveis por elaboração de

normas gerais de CEM; e o Comitê Consultivo em Compatibilidade eletromagnética (ACEC), que garante a coordenação entre os comitês especiais de CEM com outras organizações externas e guia outros comitês de produtos no desenvolvimento de normas específicas (IEC EMC Players).

As normas de CEM estão divididas em grandes famílias. Ressalta-se, como exemplo, a série IEC 61000 e a série CISPR 16 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019), cujas estruturas básicas das duas séries são apresentadas na Tabela 1 e na Tabela 2, respectivamente.

Tabela 1 – Estrutura da família de normas IEC 61000.

Parte	Tópico	Descrição
1	Geral	Conceitos fundamentais, segurança funcional e incertezas nas medições.
2	Ambiente EM	Descrição, classificação do ambiente EM e níveis de compatibilidade.
3	Limites	Limites de emissões e limites de imunidade
4	Método de testes e técnicas de medição	Métodos de testes e de medidas, associados as perturbações eletromagnéticas.
5	Guias de Instalação e Mitigação	Guias de instalação; dispositivos e métodos de mitigação.
6	Normas Gerais	Requisitos gerais de emissão e imunidade em vários ambientes EM.
7	Ainda em definição	Ainda em definição
8	Ainda em definição	Ainda em definição
9	Miscelânea	Ainda em definição

Tabela 2 – Estrutura da família de normas CISPR (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

Parte	Tópico	Descrição
1	Aparatos e locais de testes	São seis partes que descrevem os aparatos para medição (corrente, tensão e campos), incluindo calibração e verificação destes.
2	Métodos de medição	São cinco partes e especificam métodos de avaliação de perturbações EM.
3	Relatórios técnicos	Apresenta o relatório técnico IEC contendo diversos relatórios da CISPR (história da CISPR, circuitos para simular interferências, etc.).

4	Incertezas e considerações estatísticas	São cinco partes e contêm informações sobre avaliações de incertezas nos testes e medições, considerações estatísticas de reclamações e fontes de interferência, modelo para cálculo de limites e condições de uso de métodos de testes alternativos.

Consideração especial deve ser realizada à ampla variedade de perturbações consideradas na avaliação de imunidade de equipamentos e sistemas elétricos e eletrônicos pelas normas da família IEC 61000-4, sendo que a norma IEC 61000-4-1 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016) apresenta um panorama da abrangência dos documentos pertencentes a essa família. Devem ser destacados as perturbações, métodos e protocolos para testes ou simulações apresentados na Tabela 3.

Tabela 3 – Perturbações e métodos avaliados pelas normas da família IEC 61000-4.

Perturbações – Métodos	**Norma Relacionadas**
Descarga eletroestática (*ESD*)	IEC 61000-4-2:2008
Campo eletromagnético radiado	IEC 61000-4-3:2020
Transientes elétricos rápidos (*EFT/Burst)*	IEC 61000-4-4:2012
Surtos elétricos	IEC 61000-4-5:2014
Perturbações conduzidas por campos de rádio frequência	IEC 61000-4-6:2013
Harmônicos e Inter harmônicos	IEC 61000-4-7:2002 IEC 61000-4-13:2002 IEC TR 61000-4-37:2016
Campos Magnéticos 50/60Hz	IEC 61000-4-8:2009
Campo Magnético Pulsado	IEC 61000-4-9:2016
Campo magnético oscilatório amortecido	IEC 61000-4-10:2016
Quedas de tensão e interrupções	IEC 61000-4-11:2020 IEC 61000-4-29:2000 IEC 61000-4-34:2005
Ondas amortecidas (*Ring wave*)	IEC 61000-4-12:2017 IEC 61000-4-18:2019
Flutuações de tensão	IEC 61000-4-14:1999 IEC 61000-4-15:2010 IEC TR 61000-4-38:2015
Perturbações conduzidas de modo comum na faixa entre 0 Hz e 150 kHz	IEC 61000-4-16:2015
Ondulação em fontes de potência de corrente contínua	IEC 61000-4-17:1999

Perturbações – Métodos	Norma Relacionadas
Perturbações conduzidas de modo diferencial na faixa de frequência entre 2 kHz a 150 kHz para portas de energia de corrente alternada	IEC 61000-4-19:2014
Guias de Ondas (Transversal Eletromagnético)	IEC 61000-4-20:2010
Câmaras de reverberação	IEC 61000-4-21:2011
Perturbação conduzida	IEC 61000-4-22:2010
Pulso eletromagnético de grande amplitude (*HEMP*) Radiado / Conduzido	IEC 61000-4-23:2016 IEC 61000-4-24:2015 IEC 61000-4-25:2001 IEC TR 61000-4-35:2009
Desequilíbrio em redes trifásicas	IEC 61000-4-27:2000
Variações de frequência	IEC 61000-4-28:1999
Medição de parâmetros de qualidade de energia	IEC 61000-4-30:2015
Teste de imunidade de perturbação conduzida de banda larga para portas de corrente alternada	IEC 61000-4-31:2016
Compêndio de simulador de pulso eletromagnético de grande amplitude	IEC TR 61000-4-32:2002
Transientes de alta potência (HPEM)	IEC 61000-4-33:2005
Interferência Eletromagnética Intencional (IEMI)	IEC 61000-4-36:2020
Campos radiados em aplicações de proximidade	IEC 61000-4-39:2017
Métodos digitais para medição de potência para sinais distorcidos ou modulados	IEC TR 61000-4-40:2020

A Tabela 4 apresenta os diversos comitês especiais responsáveis pela definição dos requisitos e abordagem das normas para equipamentos ou aplicações específicas que utilizam sistemas elétricos e eletrônicos.

Tabela 4 – Comitês especiais da IEC e respectivas normas associadas a sistemas de controle e instrumentação.

Comitê	Norma ou Família de Normas	Título da Norma
TC 9	IEC 62236	*Railway applications - Electromagnetic compatibility*
TC 18	IEC 60533	*Electrical and electronic installations in ships - Electromagnetic compatibility*
SC 22E	IEC 61204-3	*Low-voltage power supplies, d.c. output - Part 3: Electromagnetic compatibility (EMC)*
SC 22G	IEC 61800-3	*Adjustable speed electrical power drive systems - Part 3: EMC requirements and specific test methods*

Comitê	Norma ou Família de Normas	Título da Norma
	IEC 62493	*Assessment of lighting equipment related to human exposure to electromagnetic fields*
SC 22H	IEC 62040-2	*Uninterruptible power systems (UPS) - Part 2: Electromagnetic compatibility (EMC) requirements*
TC 26	IEC 60974-10	*Arc welding equipment - Part 10: Electromagnetic compatibility (EMC) requirements*
TC 34	IEC 61547	*Equipment for general lighting purposes - EMC immunity requirements*
TC 44	IEC 60204-31	*Safety of machinery - Electrical equipment of machines - Part 31: Particular safety and EMC requirements for sewing machines, units and systems*
SC 45A	IEC 62003	*Nuclear power plants - Instrumentation and control important to safety - Requirements for electromagnetic compatibility testing*
TC 46	IEC TR 62153-4-1	*Metallic communication cable test methods - Part 4-1: Electromagnetic compatibility (EMC) - Introduction to electromagnetic (EMC) screening measurements*
SC 47A	IEC 61967	*Integrated circuits - Measurement of electromagnetic emissions, 150 kHz to 1 GHz*
	IEC 62132	*Integrated circuits - Measurement of electromagnetic immunity, 150 kHz to 1 GHz*
SC 62A	IEC 60601-1-2	*Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral standard: Electromagnetic compatibility - Requirements and tests*
SC 65A	IEC 61326	*Electrical equipment for measurement, control and laboratory use - EMC requirements*
SC 65B	IEC 61298-3	*Process measurement and control devices - General methods and procedures for evaluating performance - Part 3: Tests for the effects of influence quantities*
	IEC 60770-1	*Transmitters for use in industrial-process control systems - Part 1: Methods for performance evaluation*
TC 79	IEC 62599-2	*Alarm systems - Part 2: Electromagnetic compatibility - Immunity requirements for components of fire and security alarm systems*
TC 95	IEC 60255-26	*Measuring relays and protection equipment - Part 26: Electromagnetic compatibility requirements*
TC 96	IEC 62041	*Safety of transformers, reactors, power supply units and combinations thereof - EMC requirements*

Comitê	Norma ou Família de Normas	Título da Norma
TC 100 TA 5	IEC 60728-2	*Cable networks for television signals, sound signals and interactive services - Part 2: Electromagnetic compatibility for equipment*
	IEC 60728-12	*Cabled distribution systems for television and sound signals - Part 12: Electromagnetic compatibility of systems*

Além das normas da IEC, deve-se citar as normas publicados pelo *Institute of Electrical and Electronics Engineers* (IEEE) relacionadas a CEM de equipamentos e sistemas, sendo apresentadas as principais na Tabela 5. Deve-se ainda mencionar as famílias de normas e guias IEEE C62 e IEEE C63 que apresentam, por exemplo, normas, métodos de testes e recomendações gerais para diversas perturbações eletromagnéticas. As normas militares MIL-STD devem ser mencionadas por apresentarem métodos de testes para emissões e susceptibilidade (conduzidas e radiadas), que embora não sejam mandatórias fora das forças armadas americanas, são adotadas por diversas organizações externas (US DEPARTMENT OF DEFENSE, 2015). Ressalta-se ainda a importância da NRC (em inglês, *Nuclear Regulatory Commission*) com diversos guias regulatórios na área de compatibilidade, destacando-se o guia REG 1.180 para análises de interferência para sistemas de instrumentação e controle (U.S. NUCLEAR REGULATORY COMISSION, 2003).

Tabela 5 – Normas IEEE relacionadas a CEM.

Norma	Ano de Publicação	Nome
IEEE Std. 139	1988 (Reafirmada em 2012)	*IEEE Recommended Practice for the Measurement of Radio Frequency Emission from Industrial, Scientific, and Medical (ISM) Equipment Installed on User's Premises*
IEEE Std. 187	2018	*IEEE Standard for Measurement of Emissions from FM and Television Broadcast Receivers in the Frequency Range of 9 kHz to 40 GH*
IEEE Std. 299	2006	*IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures*
IEEE Std. 299-1	2013	*IEEE Standard Method for Measuring the Shielding Effectiveness of Enclosures and Boxes Having all Dimensions between 0.1 m and 2 m*
IEEE Std. 377	1980 (Reafirmada em 2008)	*IEEE Recommended Practice for Measurement of Spurious Emission From Land-Mobile Communication Transmitters*

Norma	Ano de Publicação	Nome
IEEE Std. 475	2000 (Reafirmada em 2006)	*IEEE Standard Measurement Procedure for Field Disturbance Sensors 300 MHz to 40 GHz*
IEEE Std. 1128	1998	*IEEE Recommended Practice for Radio-Frequency (RF) Absorber Evaluation in the Range of 30 MHz to 5 GHz*
IEEE Std. 1302	2019	*I EEE Guide for the Electromagnetic Characterization of Conductive Gaskets in the Frequency Range of DC to 40 GHz*
IEEE Std. 1309	2013	*IEEE Standard for Calibration of Electromagnetic Field Sensors and Probes (Excluding Antennas) from 9 kHz to 40 GHz*
IEEE Std. 1560	2005	*IEEE Standard for Methods of Measurement of Radio Frequency Power Line Interference Filter in the Range of 100 Hz to 10 GHz*
IEEE Std. 1957.1	2008	*IEEE Standard for Validation of Computational Electromagnetics Computer Modeling and Simulations*
IEEE Std. 1957.2	2010	*IEEE Recommended Practice for Validation of Computational Electromagnetics Computer Modeling and Simulations*
IEEE Std. 1613	2003	*IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations*
IEEE Std. 1613.1	2013	*IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Transmission and Distribution Facilities*
IEEE Std. 1642	2005	*Recommended Practice for an Electromagnetic Site Survey (10 kHz to 40 GHz)*
IEEE Std. 1688	2015	*IEEE Standard Requirements for the Control of Electromagnetic Interference Characteristics of Replaceable Electronic Modules*
IEEE C37.90.1	2012	*IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus*
IEEE C37.90.2	2004 (Reafirmada em 2010)	*IEEE Standard for Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers*
IEEE C37.90.3	2001	*IEEE Standard Electrostatic Discharge Tests for Protective Relays*

Percebe-se que as normas IEC-61000 possuem grande abrangência e apresentam equivalência com a maioria dos requisitos de avaliação apresentados nas outras normas, tais como as MIL-STD e IEEE. Um trabalho de comparação entre as normas militares e civis foi realizado pela NRC apresentado, inicialmente, em um guia (U.S. NUCLEAR REGULATORY

COMMISSION, 2003) em que são consideradas as abrangências das normas das instituições anteriormente citadas, apontando as equivalências dos métodos, eventuais diferenças técnicas nos procedimentos de execução dos testes, entre outros tópicos.

2.3 Segurança Funcional e Publicações Relacionadas

Atualmente, nos mais diversos ambientes, equipamentos elétricos e eletrônicos são utilizados para desempenhar inúmeras funções, incluindo atividades que envolvem segurança dos usuários ou pessoas envolvidas. Neste contexto, a segurança funcional surge com objetivo de garantir que os riscos sejam reduzidos a níveis toleráveis e que seus impactos, em caso de ocorrência, sejam minimizados.

Segurança é a imunidade a riscos que não são toleráveis, ou em outras palavras, é a imunidade de ocorrência de riscos inaceitáveis de causem lesão física ou danos à saúde das pessoas, seja de modo direto ou de modo indireto através de danos ao ambiente (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010). Três categorias ou aspectos da segurança de sistemas elétricos e eletrônicos são apontados: O primeiro é a segurança primária, relacionada aos riscos associados a choque elétrico e queimaduras realizadas diretamente pela parte física de equipamentos; o segundo é a segurança funcional relacionada a segurança de equipamentos e sistemas que dependem de funcionamentos adequados para execução de medidas de redução de risco; a terceira é a segurança indireta, que se preocupa com as consequências indiretas de mau funcionamento (STOREY, 1996).

Considerando os aspectos relacionados à segurança funcional, essa é definida como uma parte da segurança geral, sendo relacionada a processos e a sistemas básicos de controle que dependem do correto funcionamento de sistemas instrumentados de segurança (SIS) e de outras camadas de proteção. Assim, a segurança funcional está relacionada aos equipamentos e sistemas elétricos e eletrônicos, tendo como base apenas sistemas ativos (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010).

A preocupação mencionada anteriormente relativa à segurança funcional dos modernos sistemas eletrônicos programáveis não é nova. Relata-se que a partir nos anos 1950, a indústria iniciou um processo de desenvolvimento de métodos para identificação de riscos e para quantificação das consequências de falhas, percebendo que as práticas reativas (aprendizado com os erros passados) não eram suficientes. Embora a utilização de diversos métodos de determinação de risco se tornasse comum nas décadas seguintes, a elaboração de guiais formais e normas eram, ainda, raros e fragmentados (SMITH e SIMPSON, 2016).

O aumento da utilização de programas computacionais (*software*) durante a década de 1980 atraiu a atenção para a necessidade de dar um tratamento para as falhas sistemáticas uma vez que não elas não podiam ser quantificadas. Nesta abordagem, enquanto o uso das taxas de falha para o hardware dos equipamentos era visto como um método acreditado para a medição da confiabilidade do equipamento, a mesma abordagem não parecia razoável para *software*, sendo necessário a utilização de técnicas qualitativas. Em 1989, o HSE (do inglês, *Health and Safety Executive*), agência governamental do Reino Unido, publicou um guia incentivando a utilização de uma abordagem dupla (quantitativa e qualitativa) para a garantia de segurança funcional aos equipamentos com alguma programação (HEALTH AND SAFETY EXECUTIVE, 1989).

Essa iniciativa desencadeou os trabalhos da IEC, que em 1995, através da junção de estudos realizados por dois grupos (um para *software* e outro para *hardware*), lançou um rascunho da norma IEC 1508 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 1995). Nota-se que esta já apresentava uma abordagem dupla com base na análise de risco, alterando a mentalidade de que a realização do projeto de maneira ordenada e direcionada era suficiente para atingir níveis satisfatórios de segurança. Deste modo, propunha-se a avaliação dos riscos para se determinar quais necessitariam ser reduzidos e, assim, adotar requisitos de segurança adicionais.

Posteriormente, este documento é revisado, e publicado em 2001 como a série de normas IEC 61508, '*Functional safety of electrical/electronic/programmable electronic safety-related systems*' (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010). As edições iniciais desta são constituídas por 7 partes descritas na Tabela 6.

Tabela 6 – Estrutura da família de normas IEC 61508.

Parte	Descrição
1	Requisitos Gerais
2	Requisitos de segurança para sistemas elétricos / eletrônicos / eletrônicos programáveis
3	Requisitos de *software*
4	Definições e abreviações
5	Exemplos de métodos para determinação dos níveis de integridade de segurança
6	Guias de aplicação da IEC 61508-2 e IEC 61508-3
7	Visão geral de técnicas e medidas

Deste modo, a segurança funcional aborda tanto as falhas aleatórias de hardware quanto as falhas sistemáticas. As primeiras se referem as falhas específicas de componentes, sendo possível atribuir taxas de falhas com base em dados estatísticos de componentes similares para prever o desempenho do equipamento ou sistema que utiliza o componente analisado. As falhas sistemáticas, por sua vez, não podem ser atribuídas a uma falha de um componente específico, sendo provenientes de falhas de software, problemas de tolerância de projeto, entre outras. Observa-se alvos quantitativos podem ser estabelecidos apenas para falhas aleatórias de hardware, devendo a abordagem qualitativa (SMITH e SIMPSON, 2016). Neste contexto, define-se o conceito de nível de integridade de segurança (do inglês, Safety Integrity Level - SIL): níveis discretos de avalição de performance na execução de funções de segurança por equipamentos elétricos e eletrônicos.

A norma IEC 61508 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010) define quatro níveis, de SIL1 a SIL4, sendo o último o mais alto nível de integridade de segurança. Para cada nível, são impostos requisitos para ambas as integridades de segurança: a sistemática e a de hardware. Para a garantia da integridade de segurança de hardware, é utilizada uma abordagem probabilística, em que, para cada SIL, são definidos alvos de máxima probabilidade de ocorrência de falhas de segurança e fatores de redução de risco que devem ser atingidas para cada função de segurança executada pelos equipamentos ou sistemas analisados. Para garantia da integridade sistemática, é realizada a recomendação de requisitos para cada uma das diferentes etapas de desenvolvimento de equipamento ou sistemas que irão desempenhar as funções de segurança.

Diversas normas foram publicadas, posteriormente, com aplicações específicas em relação a segurança funcional, atendendo os requisitos gerais da família de normas básicas da série IEC 61508 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010), sendo apresentadas na Tabela 7.

Tabela 7 – Normas correlacionas à família IEC 61508.

Norma	Ano de Publicação	Edição	Nome
IEC 61513	2011	2.0	*Nuclear power plants - Instrumentation and control important to safety - General requirements for systems*
IEC 61511 (Serie)	2020	1.0	*Functional safety - Safety instrumented systems for the process industry sector -*

Norma	Ano de Publicação	Edição	Nome
			Part 1: Framework, definitions, system, hardware and software requirements *Part 2: Guidelines for the application of IEC 61511-1* *Part 3: Guidance for the determination of the required safety integrity levels*
IEC 62061	2005 (AMD1:2012 AMD2:2015)	1.2	*Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems*
IEC 61800-5-2	2016	2.0	*Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional*
IEC 60601-1	2005 (AMD1:2012)	3.1	*Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*
ISA-S84.00.01	2004	3.0	*Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*
EN50128	2011	2.0	*Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*
EN50129	2018	2.0	*Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*
ISO 14791	2010	2.0	*Medical Devices – Application of Risk Management to Medical Devices*
IEC 61800-5-2	2016	2.0	*Adjustable speed electrical power drive systems. Safety requirements - Functional*

Alguns livros e materiais diversos foram publicados com o objetivo de detalhar e exemplificar os conceitos trabalhos nas normas internacionais (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010). O livro *"The Safety Critical Systems Handbook"*, cuja primeira edição foi publicada em 2001, traz um guia para a aplicação das normas IEC 61508 e IEC 61511 (SMITH e SIMPSON, 2016). Este apresenta métodos de modelagem de confiabilidade, inúmeros exemplos de aplicação em forma de estudo de casos e modelos para guiar a aplicação das normas para atingir segurança funcional. Adicionalmente, muitos fornecedores de equipamentos elétricos e eletrônicos disponibilizam guias que trazem uma introdução as normas geral e específica e exemplos de aplicações em suas respectivas áreas de atuação (MTL INSTRUMENTS GROUP, 2002) (ROCKWELL AUTOMATION, 2013).

Da mesma forma, muitos artigos científicos discutem resultados de aplicações específicas em análise de segurança funcional, tais como em sistemas de detecção de gases tóxicos ou combustíveis (KOSMOWSKI, 2006). As experiências práticas, tais como mencionadas anteriormente, são enfatizadas na literatura, visando o aperfeiçoamento da aplicação das normas, no processo de aprovação, avaliação e certificação de sistemas relacionados à segurança (GALL, 2008).

2.4 Resiliência Eletromagnética

Todos os sistemas elétricos, eletrônicos ou eletrônicos programáveis (E/E/PE) estão sujeitos a serem afetados por perturbações eletromagnéticas, sendo possível, por esse motivo, a ocorrência de falhas ou mau funcionamento. Essa preocupação se torna ainda mais relevante para os dispositivos que desempenham funções de segurança e que necessitam atender os requisitos de segurança funcional nos níveis mínimos determinados (SIL) para cada umas das funções desempenhadas pelo dispositivo.

Deve-se lembrar que os sistemas eletrônicos relacionadas à segurança devem se manter seguros por todo seu ciclo de vida, ainda que quase todos os ambientes eletromagnéticos tendam a se tornar cada vez mais intensos, à medida que o uso de tecnologias eletrônicas aumenta. Outro fator agravador reside no fato das novas tecnologias eletrônicas modernas serem, em geral, mais suscetíveis e causarem mais EMI, devido a diversos fatores como a redução de tamanho de transistores, a diminuição dos níveis de tensão de operação e nível lógico, o aumento das conversões de potência com chaveamento e das comunicações sem fio (ARMSTRONG, 2010).

Há algum tempo, acreditava-se que a declaração realizada pelos fabricantes de que seus equipamentos eram conformes com as diretivas de CEM, os tornava livres de quaisquer problemas e mau funcionamento relacionados a CEM. Entretanto, as diretivas de CEM não abordam adequadamente com requisitos de segurança funcional (ARMSTRONG, 2002). Um passo à frente, até mesmo apenas a execução de testes tradicionais de compatibilidade eletromagnética não são suficientes para alcançar segurança funcional por diversos motivos (ARMSTRONG, 2010): falhas e usos previsíveis são ignorados; câmaras de teste convencionais não simulam um ambiente real de aplicação; perturbações EM não são testadas simultaneamente; o ambiente de todo o ciclo de vida do equipamento é ignorado; entre outros.

Além das limitações dos testes convencionais de CEM citadas-acima, deve-se ressaltar que os equipamentos eletrônicos programáveis possuem muitos possíveis estados digitais, não

sendo possível testar cada um dos estados que possuam uma complexidade mínima. Adicionalmente, os sistemas digitais programáveis não são lineares, de maneira que mesmo que fosse possível testar 99% de todos os estados digitais, o que não é possível em uma escala de tempo prática, não seria permitido realizar predições para o 1% não testado (ARMSTRONG e DUFFY, 2020).

Deste modo percebe-se a necessidade de ir muito além da metodologia convencional, baseada apenas na execução de teste de imunidade, e realizar a implementação de uma metodologia de avaliação de riscos funcionais (ARMSTRONG, 2010). Ou seja, a abordagem mais apropriada para a segurança funcional relacionada a CEM é através da avaliação de riscos relacionados à segurança funcional em relação aos efeitos de perturbações eletromagnéticas, que deve incluir em sua análise, métodos de avalição de risco que são requeridos pelas normas internacionais (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010) (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016). Neste método, o ambiente EM e possíveis efeitos sobre as funções de segurança são avaliados, de forma que medidas de projeto e verificação sejam realizadas para atingir o nível de segurança desejado devido às falhas e mau funcionamento que possam ocorrer devido a EMI. Essa avaliação requer que essa verificação seja feita baseada na natureza de cada risco, o número de pessoas expostas e o risco de aumento dos perigos devido a resposta do equipamento a perturbações EM (ARMSTRONG, 2003).

As práticas relacionadas ao gerenciamento de riscos funcionais em relação às perturbações eletromagnéticas podem ser chamadas, de forma mais sucinta, de resiliência eletromagnética (ARMSTRONG e DUFFY, 2020). Esse conceito foi apresentado no guia prático da *Institution of Engineering and Technology* (IET) (INSTITUTION OF ENGINEERING AND TECHNOLOGY, 2017) que apresenta uma abordagem com os passos recomendados para cumprir os requisitos impostos na norma IEC 61000-1-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016). É importante salientar que a IEC 61000-1-2 é a publicação principal para segurança funcional relacionada a CEM, sendo lançada em 2001 com o status de especificação técnica e tornando-se uma norma internacional em 2016. Como descrito na norma, o objetivo é direcionar os possíveis efeitos de perturbações eletromagnéticas em sistemas relacionadas à segurança e especificar requisitos para fases relevantes do ciclo de vida dos sistemas relacionados à segurança. Mantêm-se uma intima relação entre essa norma e a IEC 61508 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010), compartilhando todas as definições e as etapas definidas no ciclo de vida de segurança dos sistemas.

Deve-se ainda mencionar a recém-publicada norma IEEE 1848 (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 2020) que fornece um conjunto de métodos práticos para auxiliar no gerenciamento dos níveis de risco devido a perturbações eletromagnéticas por todo o ciclo de vida dos equipamentos e sistemas eletrônicos. Essa publicação deverá impactar diversas normas para aplicações específicas de equipamentos elétricos e eletrônicos que deverão abordar as técnicas discutidas na norma acima-citada. As técnicas e medidas apontadas na norma IEEE 1848 englobam a aplicação de técnicas desde o projeto, como aplicação de princípios de segregação, redundância e diversidade (por exemplo, uso de múltiplos caminhos de comunicação, uso de diferentes métodos de detecção de uma mesma variável, etc.) e de métodos de correção de erro (como, por exemplo, uso de sistemas de votação), passando pelos ciclos de verificação e validação, e garantindo a segurança funcional durante todo o ciclo de vida do sistema. Nas etapas de verificação e validação, o uso de técnicas para a determinação de risco são fundamentais para a determinação e análise de um conjunto razoável de condições (perturbações e falhas) previsíveis para garantir a resiliência eletromagnética dos sistemas analisados.

2.5 Técnicas de Determinação de Risco

Embora a preocupação humana com os fatos que poderiam dar errado ser antiga (código de Hamurabi, por exemplo, no século XVIII a.C.), o conceito de responsabilidade na produção e utilização de um produto seguro é surpreendentemente moderno. Tradicionalmente, os estudos científicos sobre segurança destacam-se em três períodos principais: o período da tecnologia, o período dos fatores humanos e o período do gerenciamento organizacional de riscos (HALE e HOVDEN, 1998). De maneira similar, outros autores, tais como Hudson (HUDSON, 2007), sugerem que o desenvolvimento em três fases: a fase técnica, a fase de sistemas e a fase cultural. Apesar das nomenclaturas distintas, ambas visões sugerem um desenvolvimento sequencial, tendo propósitos semelhantes. Neste trabalho, a nomenclatura e classificação de Hale e Hovden (HALE e HOVDEN, 1998) serão adotadas devido a sua ampla utilização e aceitação.

No primeiro período, o foco principal se encontrava no desenvolvimento de medidas para evitar acidentes com maquinário, explosões e para prevenir que estruturas se colapsassem. Esse período tem seu início com a Revolução Industrial no século XVIII e se estende até o período pós-Segunda Guerra Mundial. Neste período, os investigadores e engenheiros focavam seus

esforços na avaliação de causas raízes de acidentes de ordem técnica por acreditarem que os acidentes causados por outras fontes (como erros humanos) não poderiam ser impedidos. Entre as publicações pioneiras relacionadas à segurança, destaca-se o livro sobre segurança industrial de Herbert Heinrich publicado em 1931 (HEINRICH, 1931), que continha abordagens para a prevenção de acidentes.

A necessidade de análises de confiabilidade ganhou reconhecimento no período pós-Segunda Guerra Mundial, dado que os problemas de manutenção, reparo e falhas em campo tinham se tornado muito recorrentes nos equipamentos militares. Com os avanços, tanto na área civil, em especial nos campos de comunicação e transporte, quanto na área militar, envolvida no início dos programas espaciais, sistemas complexos de tecnologia surgem, emergindo a necessidade por métodos de determinação de riscos e segurança. Entre estes inclui-se, por exemplo: a análise de modos de falhas (*Failure Mode and Effect Analysis – FMEA*) desenvolvido em 1949 pelas Forças Armadas Americanas para sistemas de controle de voo; o método de análise de árvores de falha (*Fault Tree Analysis – FTA*), que surgiu, em 1961, devido à preocupação com a possibilidade de disparo não-intencional do sistema de controle de lançamento do míssil *Minuteman;* e o método HAZOP, desenvolvido em 1963 na ICI (*Imperial Chemical Industries*), sendo semelhante ao FMEA por realizar tanto a identificação quanto análise dos riscos em relação a sua probabilidade e seus efeitos.

No início dos anos 50, a análise de confiabilidade já havia se tornado um novo campo da engenharia, unindo as técnicas de teoria da probabilidade com teoria de confiabilidade, originando a conhecida Avaliação Probabilística de Segurança – APS (do inglês, *Probabilistic Safety Assessment* – PSA). A aplicação desta metodologia é, ainda hoje, amplamente utilizada como uma abordagem padrão para a avaliação de segurança, sendo complementada pela análise de segurança determinística nos estudos e avaliações em plantas nucleares modernas (AGENCY, 2016).

O segundo período relacionado à abordagem científica da segurança, conhecido como período dos fatores humanos, teve seu início com o acidente da planta nuclear de *Three Mile Island* em 1979. Até aquele momento, os métodos desenvolvidos (FMEA, HAZOP, Arvore de Falhas e Árvore de eventos) eram considerados suficientes para avaliar a segurança de instalações nucleares. Entretanto, após este evento, verificou-se que os fatores humanos não poderiam ser desconsiderados nas análises de segurança. Embora os fatores humanos já fossem estudados desde a década de 40, estes estudos focavam, primordialmente, na análise da eficiência e produtividade (CZAJA e NAIR, 2012), sem se aterem aos aspectos relacionados à segurança.

Os estudos com base na APS, que já havia sido estabelecida como uma norma industrial para como lidar com questões de segurança e confiabilidade, passou a incluir os fatores a partir do acidente em 1979. Desenvolve-se e aplica-se, então, a Avaliação de Confiabilidade Humana – ACH (do inglês, *Human Reliability Assessment* – HRA). Assim, a ACH surgiu como uma extensão dos métodos existentes de modo a englobar também os fatores humanos, e tendo passado, posteriormente, por grandes evoluções. Desenvolveram-se, então, análises mais especializadas. Mencionam-se, por exemplo, a técnica de predição de taxa de erro humano (do inglês, *technique for human error rate prediction* – THERP), que tem como base a aplicação de árvores de falha para determinação da probabilidade de erro humano para a realização de tarefas específicas; e o método HEART (do inglês, *Human Error Assessment and Reduction Technique*), avaliação conhecida pela sua simplicidade ao definir 9 (nove) tipos básicos de tarefas e associar cada uma delas a um potencial erro humano e a 38 condições que possam produzir erros (KIRWAN, GIBSON, *et al.*, 2005).

O terceiro período, conhecido como gerenciamento organizacionais, tem sua origem motivada por duas razões principais. A primeira estava relacionada com a crescente insatisfação com a abordagem normativa, já que, nem sempre ela era suficiente para garantir segurança. A segunda estava na percepção de que as abordagens de modelos de cadeias de eventos possuíam limitações, ao cobrirem, apenas, causalidades lineares. A partir da ocorrência de diversos acidentes, como o da nave Challenger e do reator de Chernobyl, percebeu-se que os métodos utilizados até aquele momento, como PSA-ACH, tinham limitações e que as abordagens organizacionais deveriam ser consideradas em adição aos fatores humanos. A partir deste momento, as abordagens de sistemas de gerenciamento de segurança são enfatizadas, sendo introduzidos métodos baseados na engenharia de resiliência e na engenharia de sistemas (REASON, 1997). Neste período surgiram, por exemplo, modelos e técnicas de avaliação de acidentes e incidentes de causas complexas interdependentes, como o AcciMap e o Modelo do Queijo Suíço (do inglês, Swiss Cheese Model) (RASMUSSEN, 1997) (REASON, 2000).

A consideração de duas novas fases adicionais foi sugerida na literatura: o período chamado de era de integração ou período holístico, e o período chamado de era adaptativa.

O quarto período, conhecido como período de integração ou holístico, é, na realidade, uma abordagem que visa integrar as preocupações dos períodos anteriores (tecnologia, fatores humanos e gerenciamento organizacional de riscos), analisando também suas interrelações e interdependências (GLENDON, CLARKE e MCKENNA, 2006). Deste modo, os três primeiros períodos seriam combinados para a definição de procedimentos para gerenciamento de riscos.

O quinto período ou era adaptativa foi sugerido com objetivo de ir além de uma abordagem de integração das etapas anteriores (BORYS, ELSE e LEGGETT, 2009). Sua origem tem como base as discussões atuais de engenharia de resiliência que contempla as necessidades de adaptações devido aos complexos sistemas organizacionais que precisam ser gerenciados, a consideração de maneiras de mitigação de efeitos críticos após a ocorrência de acidentes e as maneiras de abordar a detecção de riscos, incluindo os inesperados e os desconhecidos. Esse período se relaciona aos conceitos de engenharia de resiliência apresentados no livro *"Resilience Engineering: Concepts and Precepts"* (HOLLNAGEL, WOODS e LEVESON, 2006), que é uma coletânea de textos de diversos especialistas de engenharia de resiliência. Ressalta-se citar que os organizadores deste livro são criadores de importantes técnicas adaptativas de gerenciamento de risco, como o método FRAM (*Functional Resonance Analysis Method*) criado por Erik Hollnagel e o método STAMP (*Systems-Theoretic Accident Model and Processes*) criado por Nancy Levenson (HOLLNAGEL, 2004) (LEVESON, 2011).

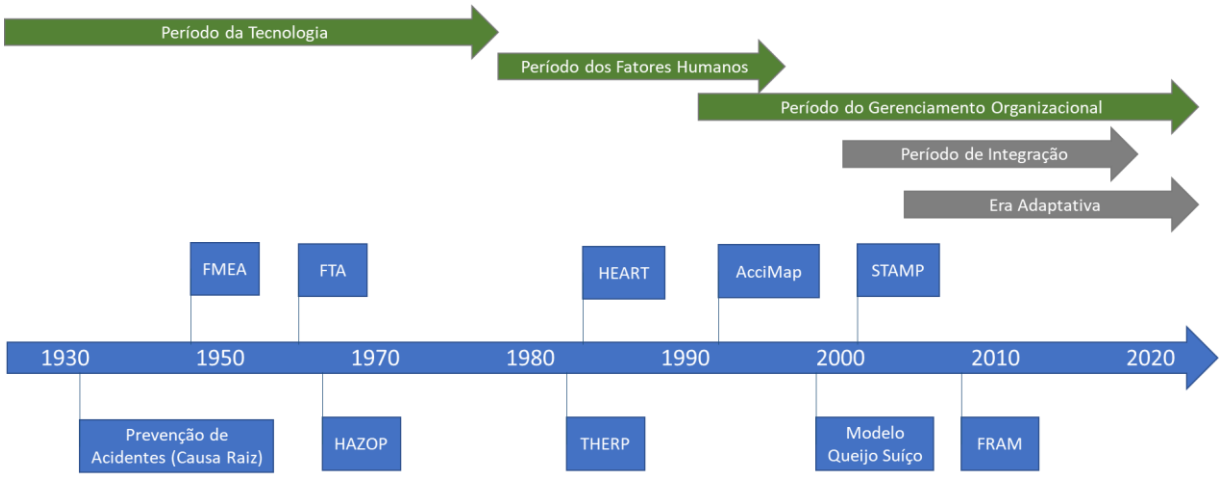


Figura 1: Histórico cronológico das eras dos estudos científicos sobre segurança e das técnicas para a determinação de riscos.
Fonte: Adaptado de (WATERSON, ROBERTSON, *et al.*, 2015).

Em uma visão mais ampla, além de cumprirem um papel importante no desenvolvimento de projetos e certificação de produtos, as técnicas de gerenciamento de riscos são essenciais para a conformidade dos requisitos legais, tais como na exigência de adoção de programas de gerenciamento de riscos ocupacionais (PGR), adotados ao redor do mundo, como, por exemplo, na União Europeia (COUNCIL OF THE EUROPEAN UNION, 1989), EUA (US DEPARTMENT OF LABOR, 1994) e no Brasil (SECRETARIA ESPECIAL DE PREVIDÊNCIA E TRABALHO, 2020). A norma reguladora NR-10 (MINISTÉRIO DO

TRABALHO E PREVIDÊNCIA SOCIAL, 2016), por exemplo, requisita a adoção de técnicas de análise de risco como medida de controle de riscos elétricos nas intervenções em instalações elétricas.

Diversos métodos de gerenciamento de risco são utilizados em variadas aplicações industriais. Muitos métodos são recomendados por normas internacionais, destacando-se, para esse propósito, as normas ISO (do inglês, *"International Organization for Standardization").* Em 1987, essa organização publicou a família de normas internacionais ISO 9000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2015), buscando formalizar o gerenciamento e controle de qualidade, dando visibilidade aos métodos de determinação de risco. Posteriormente, em 2009, a ISO publicou sua família de normas relacionadas ao gerenciamento de riscos, incluindo um guia com os princípios e regras gerais no gerenciamento de riscos – ISO 31000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018), um guia na seleção e aplicação sistemática de técnicas de determinação de risco – IEC/ISO 31010 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019) e um manual de termos técnicos aplicável a essa área de conhecimento – ISO Guide 73 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2009). Esse conjunto de normas fornece uma padronização entre as diferentes normas e metodologias existentes em diversas áreas industriais e regiões, apresentando uma base comum para as empresas e profissionais que utilizem processos de gerenciamento de riscos.

Embora grande parte da prática atual na determinação de riscos ainda tenha como base as técnicas dos três primeiros períodos do estudo científico de segurança, cada vez mais, busca-se o desenvolvimento ou melhoria de técnicas que possam reunir os diversos níveis de análise de segurança, com abordagens integrativas e adaptativas. Diversos métodos utilizam, por exemplo, a combinação entre duas ou mais técnicas com o objetivo de criar métodos que sejam mais eficientes na determinação de riscos. Cita-se ainda, a existência de métodos potenciais a serem utilizados, de maneira isolada ou conjunta (híbridos), como as abordagens que utilizem aplicações de inteligência artificial, tais como redes neurais, redes bayesianas, e de outras áreas de conhecimento, como a lógica fuzzy (SU, ZHANG, *et al.*, 2018) (LOGHMANPOUR, KANWAR, *et al.*, 2015) (HU, ZHANG, *et al.*, 2015) (ZHOU e ZAIN, 2016).

Através desta breve análise bibliográfica, que os aspectos de segurança e de CEM foram tratados como pontos distintos e sem interrelação no passado, entretanto, diante das tecnologias atuais, e eventuais impactos sociais e ambientais, novas metodologias de análise de risco fazem-se necessárias. Essa necessidade é claramente apontada na norma IEC 61508-1 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010), que indica a análise de

riscos como uma das etapas no processo de segurança funcional, sendo necessária no desenvolvimento de sistema de segurança que incorporem elementos elétricos, eletrônicos ou eletrônicos programáveis; e na norma IEC 61000-1-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016), que relacionando segurança funcional e CEM, reafirmando este posicionamento e incluindo a necessidade de avaliação do ambiente eletromagnético na análise de risco proposta na primeira norma acima-citada.

Detalhes dos métodos de análise de riscos mais utilizados historicamente e de métodos mais recentes para o gerenciamento e análise de riscos, identificados na revisão anteriormente exposta, serão apresentados a seguir, na qual pretende-se realizar uma avaliação inicial na busca daquelas que possam ser adequadas ao gerenciamento de segurança funcional e de compatibilidade eletromagnética, a serem detalhados na metodologia a ser apresentada no capítulo posterior.

2.5.1 Modelo do Queijo Suíço de Acidentes (*Swiss Cheese Model*)

O modelo do queijo suíço de acidentes é uma ferramenta de avaliação e gerenciamento de riscos que oferece um entendimento profundo de camadas de proteção. Entende-se por uma camada de proteção, uma ação preventiva que reduz a chance de um incidente ocorrer, ou uma ação de mitigação que diminua a severidade de um acidente. O nome da técnica tem origem ao se relacionar os sistemas humanos a múltiplas fatias de queijo suíço, empilhados lado a lado. Nessa comparação, cada fatia representa uma camada de proteção do sistema e as aberturas no queijo são as fragilidades do sistema. Para a ocorrência de ume evento indesejado, é necessário o alinhamento das fragilidades de cada uma das camadas de proteção. O método é também conhecido por modelo de Reason, devido ao nome do seu criador (REASON, 1997).

Nesse modelo, quase todas as falhas nas barreiras ou espaços nas fatias queijo são provenientes da combinação de dois tipos de fatores: as falhas ativas e as condições latentes. As falhas ativas são ações inseguras realizadas por pessoas que estão em contato direto com os sistemas ou pessoas de interesse, em caso de sistemas humanos, tendo impacto direto na integridade das defesas. Elas podem ser caracterizadas por erros, violações de procedimentos, mal funcionamentos, lapsos, etc. Por outro lado, as condições latentes são falhas incorporadas ao sistema, processo ou procedimento, que permanecem inativas até serem acionadas por uma falha ativa. Em geral, as condições latentes surgem de decisões gerenciais ou de definições realizadas durante a fase de projeto do sistema ou processo (REASON, 2000).

Os primeiros passos do modelo ocorreram no final da década de 1980, quando James Reason da Universidade de Manchester trabalhava na definição de uma estrutura geral para o entendimento da dinâmica de ocorrência de acidentes, sendo diferenciadas as falhas humanas ativas e latentes, tendo publicado, em 1990, o livro "Human Error" (REASON, 1990). A ideia inicial do livro era fornecer essencialmente um relato psicológico cognitivo da natureza, variedades e fontes dos erros humanos. Cita-se ainda que o conceito de queijo suíço não havia sido cunhado, fato que ocorreu alguns anos depois por Rob Lee, o diretor do Escritório de Investigação de Segurança Aérea (*Bureau of Air Safety Investigation – BASI*) em Camberra, mas eram apresentados os conceitos de "planos" que representavam as origens dos erros humanos que poderiam vir a contribuir para a falha de sistema complexo: os tomadores de decisão, gerenciamento, pré-condições, atividades produtivas e defesas. Um segundo marco do desenvolvimento do método ocorreu nos primeiros anos da década de 1990, onde os planos produtivos foram reduzidos para três (organização, ambiente de trabalho e pessoas) e o plano de defesa foi estendido para três, tendo Reason realizado, nesse modelo, a diferenciação entre erro e violações. O último marco do modelo ocorreu na publicação, por Reason, do livro "Managing the Risks of Organizational Accidents" (REASON, 1997) em 1997, quando o modelo sofreu adequações e tomou a forma atual, onde três elementos básicos são considerados (perigos, defesas e perdas), com dois fatores que causam as fraquezas (falhas ativas e as condições latentes) (REASON, J.; HOLLNAGEL, E.; PARLES, J., 2016).

O modelo do queijo suíço tem sido aplicado nos mais diversos campos, incluindo, por exemplo, as áreas de aviação, de cuidados médicos e gerenciamento organizacional. Na área médica, entre os recentes usos desta técnica encontra-se sua aplicação na revisão literária para melhoria dos processos e de prevenção de erros em cirurgias por meio de listas de verificação de segurança (COLLINS , NEWHOUSE , *et al.*, 2014). Na área de gerenciamento organizacional, propôs-se uma adaptação do modelo do queijo suíço para permitir que organizações possam entender como aprender por meio de projetos anteriores e como distribuir com sucesso o conhecimento de projeto entre os elementos da organização, como aprendizado individual, tecnologia, infraestrutura, etc. (DUFFIELD e WHITTY, 2015).

Na aviação, o modelo do queijo suíço tem sido utilizado para múltiplos propósitos, como, por exemplo, na avaliação das técnicas de gerenciamento de recursos da tripulação e na modelagem e avaliação de fatores humanos e organizacionais envolvidos nas ocorrências acidentes aéreos gerais.

2.5.2 Análise de Modos de Falha e Efeitos (FMEA)

A FMEA é uma técnica que identifica os modos e mecanismos de falhas com seus respectivos efeitos, bem como os meios para evitar ou mitigar as falhas. É classificado como um método '*bottom-up*' (indutivo) devido a ordem adotada na análise: inicia com as possíveis falhas de componentes do sistema, discute suas causas e avalia posteriormente seus efeitos nas funções executados pelo sistema (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019). É um processo interativo, sendo um método de suporte para avaliações de manutenção, segurança e logística. Devido a sua versatilidade, o método tem sido adaptado para uso em diversos campos de aplicação.

Existem diversas variantes de FMEA, entretanto, elas podem ser divididas em três tipos básicos, sendo eles: a FMEA de sistema ou FMEA funcional, focado para a fase conceitual de um projeto quando realizada a análise funcional do sistema global; a PFMEA (*Process* FMEA), voltado para a melhoria de processos, em especial de manufatura; e a DFMEA (*Design* FMEA), para desenvolvimento de novos produtos ou componentes (DHILLON, 1999).

Uma conhecida variante da FMEA é a FMECA (Análise de Modos de Falha, Efeitos e Criticidade), que reuni as características do FMEA com a adição de uma análise crítica que define a significância de cada modo de falha. Em geral, a análise crítica baseia-se em uma classificação dos modos de falha em relação a severidade, ocorrência e detecção (método RPN, do inglês *"Risk Priority Number"*).

Conforme já comentado, a FMEA foi desenvolvida em 1949 pelas Forças Armadas Americanas para rastrear problemas críticos e prevenir acidentes e mau funcionamento nos sistemas de controle de voo. Os procedimentos para realização da FMEA foram apresentados, naquele mesmo ano, em forma de relatório (US DEPARTMENT OF DEFENSE, 1949). Nota-se que este relatório se tornou uma norma militar MIL-STD-1629A em 1980 (US DEPARTMENT OF DEFENSE, 1980), sendo utilizada como referência para a nomenclatura e para a aplicação da técnica na indústria. Nos anos 60 e 70, houve uma grande expansão no uso da FMEA como técnica em engenharia de confiabilidade, com atenção especial para as indústrias automotivas que iniciaram sua utilização. Importantes passos dessa evolução neste período foram a definição de uma abordagem sistemática realizada por Coutinho (COUTINHO, 1964), em 1962, que criou o termo 'Análise de Falha-Efeito' e o desenvolvimento da FMECA pela agência espacial americana NASA (Administração Nacional da Aeronáutica e Espaço ou do inglês, *National Aeronautics and Space Administration*), visando obter a confiabilidade desejada para sistemas espaciais (JORDAN, 1972). Em 1987, a ISO (do inglês, *"International*

Organization for Standardization") publicou a família de normas internacionais ISO 9000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2015), buscando formalizar o gerenciamento e controle de qualidade, dando visibilidade para a FMEA que passou a ser difundida em diversas áreas.

A FMEA / FMECA tem sido abordada com vasta amplitude na literatura. A norma IEC 60812 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2018) é a principal referência normativa relacionada a estes métodos, contendo as melhores práticas para sua realização e sua aplicação. A adoção internacional desta norma levou ao cancelamento da norma militar MIL-STS-1629A (US DEPARTMENT OF DEFENSE, 1980), antes utilizada como principal referência internacional destes métodos. Diversos outros guias internacionais estão disponíveis descrevendo as recomendações práticas para o desenvolvimento desta técnica em diversas áreas, tais como para o desenvolvimento de produtos (SAE INTERNATIONAL, 2012), em processos de montagem e manufatura (SAE INTERNATIONAL, 2009), na indústria de equipamentos de semicondutores (VILLACOURT, 1992), etc.

A FMEA/FMECA é, também, recomendada como uma das técnicas indicadas para utilização no processo de gerenciamento de riscos pelas norma IEC/ISO 31010 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019), já anteriormente citada, e pelo guia ANSI/ASSP Z590.3-2011 (AMERICAN SOCIETY OF SAFETY PROFESSIONALS, 2011), que indica oito técnicas de determinação de risco apropriadas para avaliar riscos ocupacionais e riscos relacionados ao desenvolvimento de processos.

Diversos artigos têm discutido sua evolução e utilização, sendo que uma revisão de artigos publicados nos 45 primeiros anos de existência da técnica (de sua criação até 1994) relacionados a aplicação destas técnicas foi realizada por Bouti e Kadi (BOUTI e KADI, 1994). Este aborda seus pontos principais, como princípios, tipos, melhorias sugeridas, combinação com outras técnicas e aplicações, e sua utilização nas áreas de manufatura e de projeto de produtos. Posteriormente, uma análise complementar foi realizada para avaliar a produção científica de 1994 a 2010 sobre a FMEA (SUTRISNO e LEE, 2012), com base em 20 diferentes revistas acadêmicas de 8 (oito) bases de dados, sendo focada na avaliação de confiabilidade em serviço. Mais recentemente, em 2017, um estudo apresentou a avaliação de mais de 300 artigos científicos e patentes, publicados desde 1978 com a técnica da FMEA / FMECA, classificando os problemas analisados em 4 (quatro) classes diferentes categorias (aplicabilidade, representação de causa e efeito, análise de risco e solução de problemas) e 18 subcategorias (SPREAFICO, RUSSO e RIZZI, 2017).

Outra área de recorrentes pesquisas sobre FMEA está relacionada a tentativa de estabelecer algum nível de automatização no processo de sua execução, uma vez que, como mencionado anteriormente, o seu desenvolvimento mais comum depende do conhecimento de especialistas. As primeiras tentativas de desenvolvimento automatizado da FMEA datam do final da década de 1970 e início da década de 1980. Eles tinham como objetivo verificar a consistência de análises e calcular as probabilidades de falhas para atingir níveis de confiabilidade de sistemas elétricos e eletrônicos (LEGG, 1978). Diversos outros modelos de automatização foram desenvolvidos posteriormente, aplicáveis em diversas áreas de conhecimento.

Menciona-se, por exemplo, o uso da lógica *fuzzy* para determinação da criticidade das falhas durante a análise crítica (severidade, ocorrência e detecção) (CHIN, CHAN e YANG, 2008). Observa-se que existe uma grande similaridade entre os métodos *bottom-up* de análise de segurança e a construção de conjuntos da lógica *fuzzy*, uma vez que ambos dependem da experiência de especialistas e muitos parâmetros são difíceis de serem expressas objetivamente, sendo representados, por vezes, por meio de variáveis linguísticas (variáveis não-numéricas onde são atribuídas palavras ou frases para categorização) (DE CICCO e FANTAZZINI, 2003).

A engenharia de sistemas, área de conhecimento interdisciplinar que aborda o desenvolvimento e gerenciamento de sistemas artificiais de elevada complexidade, também já foi sugerida para a execução de modelos semiautomatizados de FMEA, visando integrar a análise de topologia de sistemas e de estruturas de hierarquia para determinação de comportamentos de falha durante várias fases de projetos (PAPADOPOULOS, PARKER e GRANTE, 2004). Pode-se citar, ainda, a utilização de modelos automáticos de FMEA com base em engenharia de conhecimento e na inteligência artificial (WIRTH, BERTHOLD, *et al.*, 1996) (HUNT, PRICE e LEE, 1993).

A FMEA e a FMECA já foram utilizadas em avaliações de risco relacionados a perturbações elétricas (SLAUSON, LESSARD, *et al.*, 1985). Sabath (SABATH, 2014) propôs, por exemplo, um método adaptado da FMECA para identificação, análise e desenvolvimento de estratégias de mitigação para riscos associados a EMI, denominado de TSECA (do inglês, *Threat Scenario, Effect, and Criticality Analysis)*.

A norma IEC 61000-1-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016), já citada anteriormente como referência para o gerenciamento de segurança funcional de sistemas e equipamentos elétricos e eletrônicos em relação às perturbações eletromagnéticas, menciona a FMEA e a FMECA como técnicas recomendadas para a etapa de verificação e validação. A execução destas técnicas é recomendada no mais alto nível funcional dos sistemas

relacionados a segurança. São indicadas ainda as técnicas de Árvore de Falhas (FTA), Árvore de Eventos (ETA) e dos diagramas de causa-consequência.

2.5.3 Análise de Árvores de Falha (*Fault Tree Analysis* – FTA)

A análise de árvore de falhas (AAF) é um método dedutivo que representa graficamente as condições e outros fatores que causam ou que contribuem para a ocorrência de determinados eventos ou falhas (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019). O início da AAF ocorre com a definição de um evento indesejado ou uma falha, chamado de evento inicial (em inglês, *top event*) e determina todas as formas de sua ocorrência por meio de símbolos gráficos em um diagrama lógico, relacionando os eventos por meio de portas lógicas para estabelecer critérios de dependências entre eles. Os fatores identificados na árvore podem, por exemplo, ser associados com falhas de componentes, erros humanos ou qualquer outro evento pertinente.

O método foi desenvolvido em 1961 pelos Laboratórios *Bell Telephone* quando eles estavam realizando uma avaliação de segurança, a pedido da Força Aérea Americana, para uso no sistema de controle do míssil balístico *Minuteman*. A mão-de-obra da *Bell Telephone*, grandes conhecedores da lógica Booleana nas aplicações para equipamentos de telecomunicação, adaptaram tais princípios para criar o método (DE CICCO e FANTAZZINI, 2003). Posteriormente, a companhia Boeing aprimorou os procedimentos para aplicação da técnica e fez uso de computadores para desenvolver análises qualitativas e quantitativas de árvores de falha, tornando-a bastante popular nas décadas seguintes (AVEN, 2015). Os principais resultados desta evolução na Boeing foram publicados por David Haasl em 1965 (HAASL, 1965). Desde então, a metodologia tem sido utilizada em diversos campos de aplicação, recebido propostas de melhorias e sido utilizada em integração com outras técnicas de determinação de riscos, tais como redes de Petri , diagramas de blocos de confiabilidade, FMEA e simulação de Monte Carlo (TALEBBERROUANE, KHAN e LOUNIS, 2016) (LABIB e READ, 2015) (PEETERS, BASTEN e TINGA, 2017) (TAHERIYOUN e MORADINEJAD, 2015).

Observa-se que essa análise é um método *top-down* (dedutivo), uma vez que se inicia com os eventos de mau funcionamento do sistema como um todo (efeitos) e parte para a descoberta de suas motivações (causas). O método permite o desenvolvimento de ambas as análises, qualitativas ou quantitativas.

Para a realização das análises qualitativas é necessário um maior conhecimento do sistema analisado e das causas e formas de ocorrência das falhas, onde diagramas e esquemáticos são ferramentas de suporte importantes. Dentre as análises qualitativas das árvores de falha, as técnicas mais proeminentes são *os conjuntos de corte mínimo* e *falhas de causa comum*. Os *conjuntos de corte mínimo* fornecem informações sobre as vulnerabilidades de um sistema ao representar os conjuntos de componentes que podem desencadear uma falha ao sistema (evento inicial), caso ocorram mau funcionamento simultâneo do conjunto de componentes. Deste modo, os conjuntos mínimos expõem a falta de confiabilidade de um sistema, caso eles sejam numerosos e contenham poucos elementos em cada um deles, por representarem o caminho mínimo para a ocorrência do evento inicial (TANG e DUGAN, 2004). A segunda técnica de análise qualitativa das árvores de falha, a análise de falhas de causa comum, aborda os casos em que duas ou mais falhas tem potencial de ocorrer simultaneamente ou em curto período devido a uma mesma causa, podendo elas estarem ou não representadas na árvore de falhas (RUIJTERS e STOELINGA, 2015).

Para a análise quantitativa, as probabilidades de ocorrência dos eventos primários devem ser conhecidas, de modo a possibilitar o cálculo das taxas de falha dos eventos intermediários e posteriormente, do evento inicial de acordo com o modelo. Essa abordagem é comum para análises de confiabilidade durante o desenvolvimento de produtos ou de sistemas. Para essas análises, inúmeras técnicas podem ser utilizadas para a realização dos cálculos numéricos na árvore de falha, sendo eles divididos em dois grandes grupos: medidas de importância, que indica o quão crítico um certo componente é, e medidas estocásticas, que em sua maioria estão associadas as taxas de falhas (RUIJTERS e STOELINGA, 2015)

Em alguns casos, onde as probabilidades são desconhecidas, um modelo semiquantitativo pode ser desenvolvido, ao se atribuir uma probabilidade descritiva categorizada (por exemplo, classificação de alta, média ou baixa). As árvores de falha também podem ser desenvolvidas por meio de uma abordagem oposta, ou seja, iniciar com eventos desejados, sendo o resultado conhecidos como árvores de sucesso, embora essas sejam menos comuns (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016).

Um dos maiores benefícios da FTA é conseguir descrever as inter-relações complexas entre recursos humanos, equipamentos, materiais e ambiente (DE CICCO e FANTAZZINI, 2003). A sua versatilidade permite a realização de análises de vários fatores de forma qualitativa ou quantitativa, podendo ser utilizada em diversos campos de aplicação (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019). Além disso, existem diversas ferramentas de software para execução da FTA (RELIOTECH, 2020) (ALD SERVICES, 2020) (RELIASOFT,

2020) (ISOGRAPH LTD, 2020) que permitem sua execução auxiliada e com possibilidades de integração com outras técnicas de análise de risco ou outras ferramentas de gerenciamento (BASU, 2016).

Apesar de ser uma ferramenta bastante efetiva no tratamento de riscos, quando utilizada para sistemas complexos, que incluem muitos equipamentos e variáveis de processo, a árvore de falhas cresce e exige grandes esforços de tempo, além de dificultar a verificação se todos os modos de falha estão cobertos (BAIG, RUZLI e BUANG, 2013), podendo necessitar de ferramentas auxiliares para gerenciar as falhas. Verifica-se, também, que a técnica não aborda falhas parciais (aceitando apenas opções binárias) e não trata interdependências temporais em sua abordagem tradicional. Em relação as análises quantitativas, as incertezas nas probabilidades dos eventos bases serão incluídos na probabilidade do evento primário, podendo resultar em altos níveis de incerteza (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

A primeira tentativa de se obter um guia geral para o desenvolvimento de árvores de falha ocorreu pela Comissão Nuclear Regulatória dos Estados Unidos como uma resposta para o acidente de Three Mile Island ao publicar o manual NUREG 0492 (U.S. NUCLEAR REGULATORY, 1981), onde apresenta os conceitos de construção da FTA e diversos exemplos, como a aplicação deste a um sistema de tanque de pressão e a um sistema elétrico para acionamento de motores. Atualmente, a norma IEC 61025 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016) é a principal referência normativa para as árvores de falhas, descrevendo os objetivos e partes que constituem a FTA, e fornece um guia para sua aplicação para realizar a análise, identificar eventos e modos de falha apropriados e a simbologia a ser utilizada.

A documentação da evolução das árvores de falha tem sido abordada na literatura técnica desde as décadas seguintes a sua criação, quando surgiram os primeiros artigos de revisão sobre o tema (FUSSEL, POWERS e BENNET, 1974) (LEE, GROSH, *et al.*, 1985). Recentes revisões têm abordado diversos aspectos da técnica, como:

- O uso da técnica na análise de confiabilidade e as diversas modificações sofridas pela FTA para atingir adequações necessárias (BAIG, RUZLI e BUANG, 2013);
- Revisão da modelagem, análises e ferramentas da FTA através da pesquisa e análise de mais de 150 artigos;
- O extenso uso de FTA na análise de confiabilidade com base em modelos, apontando seus mecanismos de operação, aplicabilidade e desafios (KABIR, 2017);

- Avaliação e tratamento das diversas incertezas envolvidas no desenvolvimento de árvores de falhas (YAZDI, KABIR e WALKER, 2019).

Em relação à disciplina de CEM, árvores de falhas têm sido utilizadas na resolução de diversos sistemas. Como exemplo, menciona-se o desenvolvimento de uma árvore de falha para um sistema complexo (rede de computadores) exposto a EMI, onde as interferências conduzidas e radiadas foram modeladas separadamente e suas diferentes fontes são consideradas (GENENDER, MLECZKO, *et al.*, 2011). Menciona-se também a aplicação de uma metodologia de análise com base na teoria de probabilidade apresentada por Congguang e Canavero (CONGGUANG e CANAVERO, 2016), utilizando uma FTA, para avaliação dos riscos e seus efeitos, e redes bayesianas, para verificação das vulnerabilidades e proteções do sistema em um determinado ambiente eletromagnético, sendo os dois métodos comparados ao final.

Como citado anteriormente, em relação ao gerenciamento de segurança funcional devido a EMI, a norma IEC 61000-1-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016) também menciona a FTA como técnicas recomendadas para a etapa de verificação e validação para o gerenciamento de segurança funcional em relação a CEM. Diversas aplicações da técnica com esse objetivo podem ser encontradas na literatura. Menciona-se, por exemplo, as análises de modos de falha de estruturas de instrumentação e controle de equipamentos elétricos e eletrônicos, como, por exemplo, de uma cadeira de rodas e de um queimador a gás (BOERLE e LEFERINK, 2004) (GROOT BOERLE, 2002). Pode-se citar a utilização da técnica para a avaliação de segurança funcional em relação a imunidade eletromagnética aplicada para dispositivos de proteção (relés) (ZHOU, ZOU, *et al.*, 2019).

2.5.4 Análise de Perigos e Operabilidade (*Hazard and Operability Study* - HAZOP)

É um processo sistemático com o objetivo de identificar os desvios que processos, sistemas ou equipamentos sofreram em relação ao inicialmente projetado. Adicionalmente, são examinadas as possíveis causas e avaliados suas respectivas consequências (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016). O método foi desenvolvido na ICI (Imperial Chemical Industries) em 1963, sendo que o primeiro artigo científico sobre o tema foi publicado em 1976 por Bert Lawley (KLETZ, 2010).

Antes de sua realização é necessário a criação de mapas de processos, mapas de produtos ou diagramas do sistema. Estes mapas e diagramas são essenciais para a visualização dos nós e variáveis de cada uma das seções a serem avaliadas. A execução deve ser realizada

por especialistas de diferentes áreas correlatas ao item discutido, onde os potenciais desvios são identificados por palavras-chave (‘guide-word’) combinadas com parâmetros do processo (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016).

Como pontos fortes desta técnica se destacam: fornece um método sistemático para a determinação de risco e geração de ações de tratamento deles; é aplicável para uma grande faixa de sistemas, processos e procedimentos, considerando inclusive os efeitos de erros humanos; cria um registro de processo, podendo ser usado na aprovação junto a órgãos oficiais. Por outro lado, a técnica possui algumas limitações: detalhamento exigido pela técnica pode consumir muito tempo de projeto; forte dependência da experiência dos participantes que podem incluir viés na análise; discussão pode se concentrar em detalhes do projeto e não em questões mais amplas, como influências externas.

A norma IEC 61882 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016), cuja primeira edição foi publicada somente em 2001, é uma norma internacional dedicada exclusivamente a fornecer um guia para a aplicação do procedimento HAZOP, incluindo definições, preparação, sessões de avaliação e documentação resultante. Estudo de casos são apresentados e exemplos de documentação são disponibilizados.

Revisões literárias têm sido apresentadas, abrangendo detalhes deste o surgimento da técnica na indústria química, principais referências publicadas, comparações com outras técnicas e evoluções no escopo, como, por exemplo, automatização do HAZOP, seu uso com suporte de simulações dinâmicas (DUNJÓ, FTHENAKIS, *et al.*, 2009).

Deve-se ressaltar ainda a relação entre o uso desta técnica e a área de segurança funcional. O HAZOP foi utilizado como suporte para a determinação do nível de integridade de segurança ou SIL (*Safety Integraty Level*), sendo aplicado, exemplo, no estudo de caso de uma refinaria (CALIXTO, 2007). Tem-se ainda a utilização do HAZOP como ferramenta para identificação dos impactos das possíveis falhas em um processo de aplicação de uma análise de camadas de proteção (LOPA) para determinação do SIL necessário (DOWELL, 1998).

Em relação aos últimos avanços na técnica, metodologias híbridas têm sido propostas. Pode-se mencionar, por exemplo, a metodologia HAZOP_rpn, que possui suas bases no HAZOP e no uso de um número de priorização de risco (do inglês, Risk Priority Number - RPN). Adicionalmente, o uso de um sistema de inferência Fuzzy para estimativa do número de priorização de risco permitiu a criação da metodologia FuzzyHAZOP_rpn (LAPA e GUIMARÃES, 2006). Diversas outras aplicações da técnica HAZOP com lógica fuzzy são encontradas nas mais diversas, tais como na indústria de processo e na indústria química (GAO e WANG, 2018) (AHN e CHANG, 2016). Cita-se ainda a utilização de variações do HAZOP,

como, por exemplo, com o uso de representação gráfica por meio de SGD (do inglês, ‘signed directed graph’) para identificação dos erros operacionais mais prováveis que podem gerar riscos de segurança (WANG, CHEN, *et al.*, 2009).

2.5.5 THERP

THERP (do inglês, *Technique for Human Error Rate Prediction*) é um método de Avaliação de Confiabilidade Humana - ACH (do inglês, *Human Reliability Assessement* – HRA) que tem por objetivo definir a probabilidade de erro humano ao realizar uma ou um conjunto de tarefas, de modo que medidas possam ser tomadas para a redução da chance de ocorrência desses erros analisados. Grande parte das aplicações do método estão relacionadas a estimativa de probabilidade de erros que indivíduos ou times possam cometer ao realizar um determinado procedimento sob diversas condições de pressão, como limitações de tempo, por exemplo (SWAIN e GUTTMANN, 1983). O método é geralmente referenciado como uma abordagem de decomposição devido as suas descrições de tarefas apresentarem um alto nível de detalhamento em relação as outras técnicas. Destaca-se ainda que seu processo lógico apresenta grande ênfase nos procedimentos de recuperação após a ocorrência de erros (BELL e HOLROYD, 2009).

A primeira versão do método THERP foi apresentada em 1962 em um simpósio durante a Sexta Reunião Anual da Sociedade de Fatores Humanos. O método foi desenvolvido pelo Dr. Alan Swain, sendo considerado o primeiro método formal de ACH. No ano seguinte, os laboratórios Sandia, na qual o Dr. Alan Swain trabalhava, apresentaram uma monografia que continha os princípios da quantificação de erros humanos utilizando o THERP, e nos anos posteriores focou-se na coleta de dados de performance humana para o banco de dados dos laboratórios Sandia, cujo foco inicial possuía relação com a determinação da confiabilidade na montagem de armas nucleares nos Estados Unidos. Em 1969, Swain conheceu Jens Rasmussen, professor e especialista em segurança de sistemas e fatores humanos, sendo o inventor do método Accimap, que trabalhava no Laboratório Nacional Risø, localizado na Dinamarca, e juntos eles discutiram as formas de aplicação do THERP para a área nuclear. Essas aplicações foram oficializadas através da consideração da utilização da técnica no documento WASH-1400 (RASMUSSEN, 1975) em 1975, e, finalmente, na publicação, em 1983, do *handbook* NUREG/CR-1278 (SWAIN e GUTTMANN, 1983), que apresentava métodos, modelos e probabilidades de erros humanos para permitir as avaliações quantitativa e qualitativa de ocorrência de erros humanos em plantas nucleares (BORING, 2012).

Embora o método tenha recebido críticas devido ao seu foco nas habilidades e ações humanos, sem considerar, por vezes, o contexto dos fatores organizacionais, o THERP tem sido utilizado amplamente em diversas aplicações, em especial na área nuclear. Diversas validações independentes do método foram publicados, destacando-se a realizada por Kirwan et al. em 1996 e 1997 (KIRWAN, 1996) (KIRWAN, KENNEDY, *et al.*, 1997), onde foram avaliadas as técnicas THERP, HEART e JHEDI, apontando que todas as três apresentavam um bom nível de precisão, sem a dominância de nenhuma delas, e mais recentemente, (SHIRLEY, SMIDTS, *et al.*, 2015) . Cita-se ainda que o THERP deu origem ao Programa de Avaliação de Sequência de Acidentes (do inglês, *Accident Sequence Evaluation Program – ASEP),* criado, também por Swain, para a Comissão Regulatória Nuclear Americana, cujo foco principal era versão reduzida da análise de confiabilidade humana realizada pelo primeiro método (BELL e HOLROYD, 2009). Entre as mais recentes aplicações do método pode-se citar a avaliação de erros da tripulação de voos que podem ocasionar acidentes (YANG, TAO e BAI, 2014), a avalição de taxas de erros humanos durante a manutenção de instalações embarcadas (em específico, tarefas de manutenção de bombas condensadoras) (ABBASSI, KHAN, *et al.*, 2015), a análise empírica da confiabilidade humana para o processo de limpeza de tanques a bordo de um navio-tanque químico (AKYUZ e CELIK, 2015), etc.

2.5.6 HEART

A Técnica de Avaliação e Redução de Erro Humano (do inglês, *Human Error Assessment and Reduction Technique* – HEART) é um método de avaliação de confiabilidade humana (ACH) que tem como base a literatura de performance humana para o desenvolvimento de tarefas. O HEART foi desenvolvido para ser um método rápido e simples para a quantificação de riscos de erros humanos. Para esse propósito, ele considera que a confiabilidade humana básica é dependente da natureza genérica da tarefa a ser executada e que determinadas condições influenciam na execução destas tarefas.

No HEART, a probabilidade de erros humanos são definidas a partir da classificação das tarefas a serem desenvolvidas em nove grandes grupos (Tipos Genéricos de Tarefas, do inglês, *Generic Task Types* – GTTs), sendo cada uma delas relacionada a um Potencial de Erro Humano (do inglês, Human Error Potential – HEP), e, posteriormente, da identificação das condições que podem influenciar na produção de erros (*Error-Producing Conditions* – EPCs), sendo essas já estabelecidas em lista pré-definida com 38 condições. A técnica considera ainda

as formas de prevenção dos erros identificados no projeto e forma de controle adicionais para mitigação e redução de possíveis impactos (BELL e HOLROYD, 2009).

A técnica foi desenvolvida na década de 1980 por J. C. Williams, sendo lançada em 1985, quando este publicou um artigo com seus resultados iniciais (WILLIAMS, 1985), enquanto trabalhava no Corpo de Geração Central de Energia do Reino Unido. Nos anos posteriores, o mesmo autor apresentou mais resultados e um melhor detalhamento da técnica em um conjunto de artigos (WILLIAMS, 1986) (WILLIAMS, 1988).

O método HEART, assim como já foi mencionado para método THERP, é um dos poucos métodos que foram validados empiricamente. As validações realizadas por Kirwan et al. (KIRWAN, 1996) (KIRWAN, KENNEDY, *et al.*, 1997) estenderam-se também ao método HEART e demostraram a eficiência na aplicação da técnica, embora tenha sido observado que melhorias de consistência poderiam ser realizadas. Cita-se ainda o estudo de consolidação dos conceitos e dos tipos genéricos de tarefas (GTTs) utilizados na aplicação do HEART apresentado por Williams (BELL e WILLIAMS, 2016), onde foram revisados mais de 35000 artigos para avaliar a consistência das aplicações em relação ao conceito original.

O método é uma ferramenta transversa, sendo aplicável a qualquer domínio onde a confiabilidade humana é importante, tendo sido aplicada com sucesso em diversas indústrias, incluindo, por exemplo, a área nuclear, médica, a aviação e a ferroviária. Sabe-se que o método é, hoje, o mais utilizada para avaliação de erros humanos (CAN e DELICE, 2020). Entre as aplicações mais relevantes e recentes do método encontram-se, por exemplo, abordagens para determinação das probabilidades de erro humano para atividades críticas, como as operações de carregamento de navios-tanque, sendo este um processo com riscos a vida humana e ao ambiente marítimo (AKYUZ e CELIK, 2016), e avaliações de confiabilidade humana durantes os procedimentos de manutenção, tais como na indústria de fabricação de cabos (AALIPOUR, AYELE e BARABADI, 2016) e nas operações marítimas e *off-shore* (ISLAM, ABBASSI, *et al.*, 2017).

Cita-se também o método NARA (do inglês, Nuclear Action Reliability Assessment), uma versão específica do HEART para a área nuclear, que foi desenvolvido, em 2005, para atender as necessidades das avaliações probabilísticas de segurança das plantas nucleares no Reino Unido, sendo uma ferramenta de propriedade da companhia British Energy. Cita-se ainda a Avaliação de Confiabilidade de Ação do Controlador (do inglês, Controller Action Reliability Assessment – CARA), uma versão específica do método HEART para gerenciamento de controle de tráfego aéreo desenvolvido em 2007 (BELL e HOLROYD, 2009). O método de análise de confiabilidade humana SPAR-H, desenvolvido pela NRC, baseia-se, também, no

HEART e possui ênfase para aplicações na área nuclear (IDAHO NATIONAL LABORATORY, 2005).

2.5.7 AcciMap

O AcciMap é uma representação gráfica de um cenário acidental particular que mostra o fluxograma de causas de eventos (atos e decisões) através dos vários níveis hierárquicos do sistema. É um método de natureza genérica, ou seja, pode ser aplicado em diversos domínios e áreas de interesse. As hierarquias dos sistemas e suas interações, entradas e saídas, processos de transformação e regulamentação de componentes do sistema são explicitamente representados neste diagrama, sendo apropriado para sistemas técnicos-sociais complexos (UNDERWOOD e WATERSON, 2012).

No processo de desenvolvimento de um AcciMap, para uma determinada fonte de risco, deve-se inicialmente identificar a estrutura de controle e seus respectivos controladores (atores ou tomadores de decisão) relevantes. Para cada ator, determinam-se os seus objetivos e critérios de performance, bem como avaliam-se suas capacidades de controle e as informações disponíveis para eles sobre o estado atual do sistema em relação a objetivos de produção, verificando-se os limites de segurança de um ponto de vista da realimentação de controle (RASMUSSEN, 1997). O diagrama típico de Accimap aborda as falhas em seis níveis de análise: política governamental e orçamento; órgãos reguladores e associações; planejamento e orçamento do governo local (incluindo gestão de empresas, gestão técnica e operacional); processos físicos e atividades do ator (controlador); e equipamentos e arredores (WATERSON, JENKINS e SALMO, 2017).

O método foi criado e utilizado primeiramente, em 1997, por Jens Rasmussen. Rasmussen buscava alternativas para as representações tradicionais de sistemas técnico-sociais, onde esses eram decompostos em elementos estruturais, modelados separadamente. Sua proposta era modelar o comportamento dinâmico dos sistemas e atores por decomposição de fluxos de comportamento em eventos. De acordo com Rasmussen, cada nível sistémico está relacionado no gerenciamento de segurança através do controle de riscos por meio de leis, regras e instruções. Ainda argumenta que acidentes estão, geralmente, esperando para serem liberados, por meio das práticas rotineiras de trabalho, incluindo as variações normais de comportamento (RASMUSSEN, 1997). Deve-se ainda citar a influência da teoria de controle no desenvolvimento da técnica de AcciMap, sendo ela projetada para levar a abordagem

utilizada nos sistemas de controle para a análise de acidentes (WATERSON, JENKINS e SALMO, 2017). Fato reforçado e apontado por Leveson (LEVESON, 2017), ao observar a influência da teoria de controle no trabalho de Rasmussen a partir da década de 1960.

O uso de Accimaps requer treinamento e educação formal e ainda existe uma falta de guias de uso, que afetam a acessibilidade e a consistência do método entre os estudos (SALMON, WILLIAMSON, *et al.*, 2010). Entretanto, salienta-se que, ainda assim, o método fornece um resumo claro e conciso de acidentes e a propagação de eventos através de toda a estrutura de um sistema pode ser visualizada, facilitando a criação de intervenções de segurança (BRANFORD, 2011). A investigação e avaliação de acidentes por meio da técnica AcciMap tem sido utilizada em diversas áreas de conhecimento, incluindo a área naval (AKYUZ, 2015), aviação (DEBRINCAT, BIL e CLARK, 2013), entre outros.

Embora diversos estudos com objetivo de validação e verificação de confiabilidade do método tenham sido realizados, sua validação ainda se encontra em desenvolvimento. Em sua tese, Branford (BRANFORD, 2007) apresentou os resultados do estudo de um acidente com a ferramenta AcciMap realizado por diversos participantes (incluindo especialistas) e comparou os resultados das análises realizadas, concluindo que, embora existissem similaridades entre os resultados encontrados, as variações existentes demostraram que o método de Accimap nem sempre produz resultados inteiramente válidos e confiáveis. Outro estudo, realizou a comparação de quatro estudos para analisar um mesmo acidente, utilizando os métodos AcciMap e o método STAMP (abordado no item 2.5.8 dessa dissertação) (GONÇALVES FILHO, JUN e WATERSON, 2019). As comparações indicaram que o método STAMP produz uma faixa mais abrangente de recomendações nos múltiplos níveis sistemáticos enquanto o AcciMap tende a focar em recomendações mais gerais, concluindo-se que métodos mais estruturados como o STAMP podem ajudar a produzir resultados de análises de acidentes mais confiáveis. Outros dois estudos também compararam os métodos AcciMap e STAMP, adicionando nas comparações outras técnicas como HFACS (do inglês, *Human Factors Analysis and Classification System*) (SALMON, CORNELISSEN e TROTTER, 2012) e o modelo de investigação da ATSB (do inglês, *BASI*) (UNDERWOOD e WATERSON, 2014). O primeiro estudo sugere que, embora o Accimap e o STAMP tenham maior abrangência na identificação dos fatores que contribuem para a ocorrência de eventos e acidentes, a abordagem do HFACS, em geral, é mais confiável devido à sua natureza taxonômica, utilizando uma classificação, estrutura e nomenclatura bem definidos, de modo a garantir um maior direcionamento em sua realização. O segundo estudo, por sua vez, sugere que o modelo ATSB seja mais adequada para aplicações na indústria, enquanto o método STAMP seja mais aplicável

para uso em pesquisas; para o AcciMap, indica-se que ele pode atender as necessidades de ambas as partes (indústria e academia).

2.5.8 Functional Resonance Analysis Method (FRAM)

FRAM é um método que utiliza os princípios e conceitos de engenharia de resiliência e descreve falhas de sistemas (eventos adversos) como um resultado da ressonância funcional vinda da variabilidade da performance normal dos sistemas, isto é, os eventos são o resultado do aumento de amplitude de uma ou mais funções devido a interação de diversas pequenas variações de partes do sistema. O método foi desenvolvido por Erik Hollnagel (HOLLNAGEL, 2004) e tem sido aplicado em diversas áreas como saúde, gerenciamento de tráfico aéreo, aviação e operações marítimas.

O método baseia-se na criação de um modelo representativo das funções, onde as características de cada função fornecem meios para descrever sua variabilidade potencial em cada um dos aspectos analisados. O princípio da ressonância é, então, invocado para explicar como grandes efeitos podem surgir de variações pequenas, sendo a dinâmica de dependência das funções o foco da avaliação ao invés da própria probabilidade de falha. As relações de dependência determinam se é possível duas funções serem acopladas, dependendo das condições de performance. Deste modo, elas não são baseadas em relações de causa ou efeito predefinidas, mas sim devem identificar acoplamentos intencionais e não intencionais. O método pode ser utilizado para investigação de acidentes, de modo a encontrar onde as interações geradoras dos eventos adversos podem ter surgido, ou para avaliação de risco, para explicar como a variabilidade de performance do sistema podem ocorrer devido as interações entre as características das diversas funções avaliadas e, então, identificar os riscos potenciais da situação dada (HOLLNAGEL, 2012).

O método é fundamentado em quatro princípios e premissas de como os sistemas e organizações funcionam, que são descritos abaixo (HOLLNAGEL, HOUNSGAARD e COLLIGAN, 2004):

- O princípio da equivalência de sucessos e falhas: é a premissa de que diferentes tipos de efeitos não requerem necessariamente diferentes tipos de causas, mas que uma mesma explicação pode ser utilizada em muitos casos. Explicações em como ocorrem eventos adversos geralmente são realizados ao tomar o sistema em partes ou componentes, abordagem chamada de decomposição, e, então, encontrar mau

funcionamento ou falhas destas partes de modo a explicar as consequências ocorridas. Essa visão tem como base o fato que o sucesso ou fracasso de uma atividade tem diferentes causas, entretanto, essa não é a visão adotada pelo método FRAM e pela engenharia de resiliência. Pelo método, o fato de que os resultados de dois casos são diferentes não significa que as causas básicas, também, sejam diferentes.

- O princípio dos ajustes aproximados: É a premissa de que pessoas ajustam constantemente o que eles realizam de modo que as suas ações correspondam as condições vigentes. Em geral, as condições de trabalho ou para realizar uma tarefa nem sempre são as esperadas ou as prescritas e, portanto, é necessário constantemente ajustar a performance para adequar às condições existentes. Como os recursos são limitados, os ajustes serão sempre aproximados e, embora isso seja suficiente na maioria dos casos, isso é também a razão quando algo errado ocorre.
- O princípio dos resultados emergentes: É o reconhecimento de que nem todos os resultados podem ser explicados por uma causa específica e identificável. A variação causada pelos ajustes realizados diariamente raramente é grande o suficiente para ser a causa de uma grande falha. Entretanto, as variações de múltiplas funções podem coincidir e afetar mutuamente a outra de modos inesperados, levando a impactos inesperados e desproporcionais (consequências não lineares). Deste modo, ambos, falhas e operação normal, podem ser emergentes da variação das funções ou de seus acoplamentos.
- O princípio da ressonância: nos casos em que não é possível ou razoável prover explicações com o princípio de causa e efeito, a ressonância, cujo conceito é descrito a seguir, pode ser utilizada para descrever e explicar resultados e interações não lineares. Este princípio descreve que variações perceptíveis de performance são o resultado de múltiplos ajustes aproximados que são necessários nas atividades cotidianas, de modo que a variabilidade de um número de funções pode coincidir e estabelecer influências entre estas, podendo levar ao aumento de amplitude de uma ou mais funções com resultados adversos, sejam positivos ou negativos.

Durante sua aplicação, o método FRAM considera seis aspectos das funções ou atividades de interesse, que são representadas graficamente em um hexágono, como apresentado no modelo da Figura 2: entradas representam o que ativam a função ou o que é utilizado para produzir a saída, constituindo uma ligação com a função primária; a saída representa o resultado da função, sendo a ligação com a função subsequente; os recursos são

necessidades ou consumíveis para produzir a saída; as pré-condições são condições que precisam existir antes de uma função ser executada; o tempo refere-se a todas restrições temporais que afetem a função (início, término, duração, etc.); os controles são os meios pelos quais as funções são monitoradas ou controladas.

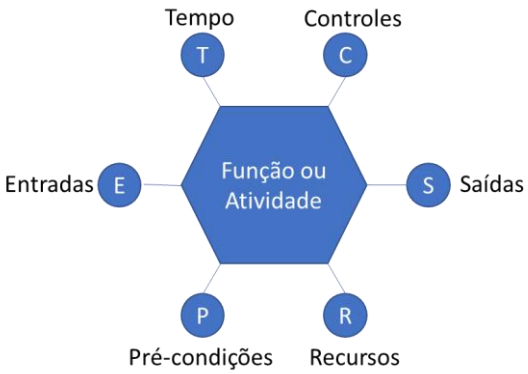


Figura 2: Os seis aspectos de uma atividade ou função no método FRAM.
Fonte: Adaptado de (HOLLNAGEL, HOUNSGAARD e COLLIGAN, 2004).

A maioria das aplicações do método são em sistemas aeronáuticos, tendo sido utilizado, por exemplo, para analisar os efeitos da automação sob condições variáveis na cabine do piloto. Este foi utilizado na avaliação do acidente do voo 965 na Colômbia em 1995 (SAWARAGI, HORIGUCHI e HINA, 2006), assim como para realizar análises do acidente do MD83 ao se aproximar do aeroporto de Paris, em 1997 (NOUVEL, TRAVADEL e HOLLNAGEL, 2007) e o acidente entre as aeronaves Gol Voo 1907 e Embraer Legacy 600 no espaço aéreo amazônico (CARVALHO, 2011). Entretanto, observa-se que o método FRAM também tem sido utilizado em outras áreas, como em para avaliação de riscos em plantas nucleares (LUNDBLAD, SPEZIALI, *et al.*, 2008), no setor de saúde (SUJAN e FELICI, 2012), etc. Observa-se que o método, por possibilitar a análise de sistemas complexos, mostra-se, inicialmente, adequado para a determinação de risco para obtenção de resiliência eletromagnética, embora aplicações não tenham sido encontradas.

Lembra-se, ainda, que sua utilização já foi comparada com outros métodos de avaliação de segurança, por exemplo, na segurança industrial (árvore de falha e rede Bayesiana) (SMITH, VEITCH, *et al.*, 2017) e com outros modelos de análises de acidentes (STAMP e Accimap) (UNDERWOOD e WATERSON, 2012).

2.5.9 Systems-Theoretic Accident Model and Processes (STAMP)

STAMP é um modelo de causalidade de acidentes inspirado na teoria de sistemas. Nesta técnica, os sistemas são vistos como componentes interrelacionados mantidos em um estado de equilíbrio dinâmico por malhas de realimentação, sendo tratados como processos dinâmicos que estão continuamente se adaptando para atingir seus resultados e para reagir as mudanças internas e do ambiente ao redor (LEVESON, 2011).

Um dos principais objetivos da técnica é superar as limitações apresentadas pelos modelos de acidentes baseados em eventos. Os eventos considerados quase sempre envolvem algum tipo de falha de componente, erro humano ou evento relacionado a energia. São exemplos destas técnicas, a FMEA (sequência direta ou método indutivo) e a Árvore de Falhas (sequência inversa ou método dedutivo). Estas técnicas são enfáticas nas relações lineares de causalidade, tornando difícil a inclusão de relações não-lineares, incluindo a realimentação. Além disso, alguns fatores são difíceis de serem incluídos em modelos de cadeia de eventos, como por exemplo, o compromisso da gestão com a segurança e a cultura básica de segurança em organização ou em uma indústria (LEVESON, 2004). Na teoria do STAMP, ao invés de definir o gerenciamento de segurança em termos de prevenção de falhas de componentes, define-se uma estrutura de controle de segurança que irá forçar o atendimento de restrições comportamentais de segurança e garantir sua contínua efetividade diante das mudanças e adaptações que ocorrem ao longo do tempo (LEVESON, 2011).

O método foi desenvolvido por Nancy Leveson (LEVESON, 2004) em 2004, tendo como conceitos básicos as restrições impostas ao sistema, as malhas de controle, os modelos de processos, e os níveis de controle. Em relação as restrições impostas, a proposta de Levenson era iniciar a abordagem com a identificação daquelas que eram necessárias para manter a segurança, ao contrário das técnicas que analisam o acidente como uma série de eventos. Deste modo, o acidente é visto como um resultado da falta de restrições impostas no projeto do sistema ou em sua operação, isto é, causado pela aplicação inadequada de restrições de comportamento em cada nível de um sistema técnico-social. Com esse resultado, é possível projetar uma estrutura de controle, um sistema físico e condições operacionais que garantam o cumprimento das restrições (LEVESON, 2004).

As duas ferramentas mais utilizadas hoje que tem como base o STAMP são o STPA (do inglês, *System Theoretic Process Analysis*) e o CAST (do inglês, Causal Analysis based on System Theory). O STPA é um método de análise para avaliação de potenciais causas de acidentes durante o desenvolvimento dos projetos de modo que riscos podem ser eliminados ou

controlados. O CAST é um método de análise retroativa que examina um acidente ou incidente que ocorreu e identifica os fatores causadores (LEVESON e THOMAS, 2018). Os dois métodos estão diretamente relacionados por utilizarem como base o mesmo modelo de causalidade, sendo o STPA, entretanto, uma análise que visa prever e antecipar a ocorrência de acidentes, enquanto o CAST é realizado para análises de cenários que já ocorreram. Os resultados de uma das análises podem ser utilizados na outra ferramenta, como, por exemplo, a análise de acidentes passados realizados pelo CAST pode ser utilizada como dados de entrada para o STPA na identificação de cenários plausíveis que precisam ser eliminados ou controlados (LEVESON, 2019).

O método STAMP tem sido aplicado para avaliações de risco ou modelos de acidentes nas mais diversas áreas, com bastante relevância nas publicações recentes. Pode-se citar aplicações na aviação (ALLISON, REVELL, *et al.*, 2017), na área naval (ROKSETH, UTNE e VINNEM, 2017), automotiva (ABDULKHALEQ, LAMMERING, *et al.*, 2017), cuidados à saúde (LEVESON, SAMOST, *et al.*, 2020), entre outras. Enfoca-se que atenção especial deve ser dada às aplicações de sistemas de instrumentação e controle (THOMAS e LEVESON, 2013) (THOMAS, DE LEMOS e LEVESON, 2012), uma vez que a técnica tem como base a inclusão de restrições nas estruturas de controle para evitar as condições acidentais.

O método STAMP tem sido comparado com diversos outros métodos de análise de risco e de avaliação de acidentes, que tem demonstrado suas vantagens em relação aos mesmos. Como já citado anteriormente, a comparação com o método AcciMap (GONÇALVES FILHO, JUN e WATERSON, 2019) indicou que o método STAMP tende a produzir resultados de análises de acidentes mais confiáveis que o método AcciMap. Em comparação com o método FMEA, observou-se em uma aplicação na área automotiva (direções assistidas eletricamente) (MARTÍNEZ, 2015), que o STAMP permitiu a descoberta de condições de risco, interações inseguras entre sistemas e comportamentos dependentes de interação humana que não foram encontradas na aplicação do FMEA, em especial nos estágios iniciais de projeto.

O método STAMP também foi comparado com o método de árvores de falha (FTA) na análise de riscos de um veículo espacial, criado pela Agência de Exploração Aeroespacial Japonesa para o transporte de componentes e outros itens para a Estação Espacial Internacional (ISHIMATSU, LEVESON, *et al.*, 2010). Observou-se que as causas de risco encontradas na análise FTA, técnica utilizada inicialmente durante o projeto, foram também identificadas pelo STPA e que, adicionalmente, foram encontrados novos fatores não identificados anteriormente. Destaca-se a viabilidade e a utilidade do STPA para as análises de segurança de sistemas, especialmente nas fases iniciais do projeto de sistemas complexos.

Menciona-se, também, a utilização das técnicas do Queijo Suíço e CAST para analisar as falhas mais importantes que ocorreram na aviação da Guarda-Costeira Americana de modo a identificar potenciais fontes sistemáticas de riscos (HICKEY e HOMMES, 2013). O estudo identificou que a utilização do método STAMP permitiu a identificação de melhorias nos controles do sistema de aviação da Guarda-Costeira Americana que não foram encontrados com a utilização dos modelos de Queijo Suíço.

2.6 Princípios Metodológicos

2.6.1 Definições em CEM e Mecanismos de Acoplamento

A compatibilidade eletromagnética se refere a capacidade de um equipamento ou sistema de funcionar satisfatoriamente em seu ambiente eletromagnético sem introduzir perturbações eletromagnéticas que possam comprometer a operação e a segurança de qualquer outro equipamento naquele ambiente. As preocupações com CEM são comuns a todas as aplicações elétricas e eletrônicas, incluindo todas as fases de projeto: concepção, definição de requisitos, design, fabricação, instalação e testes (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 1990). Os mecanismos de controle de IEM têm como base dois aspectos básicos: as perturbações e a imunidade eletromagnética. Perturbações eletromagnéticas referem-se à contribuição de sinais conduzidos e radiados que possam causar interferência de um produto, ou seja, a geração de energia eletromagnética por fontes, de maneira acidental ou deliberada, e sua liberação para o meio. O objetivo de limitar as perturbações é controlar o ambiente eletromagnético em que outros produtos devem operar. Imunidade é a capacidade de um equipamento de operar satisfatoriamente, sem degradação, na presença dos sinais resultantes das emissões (ruído) (OTT, 2009). Em outras palavras, atinge-se a compatibilidade eletromagnética quando os níveis de perturbações e imunidade são controlados de modo que os níveis de imunidade dos dispositivos, dos equipamentos e sistemas, em qualquer localização, não sejam atendidos. Deste modo, a busca da CEM tem como função primária garantir a segurança e confiabilidade dos sistemas, nos diversos campos de aplicação e nos mais variados ambientes eletromagnéticos.

Menciona-se que os mecanismos de controle de IEM abrangem a avaliação das fontes de perturbação e das vítimas de interferência, como ilustrado na Figura 3.

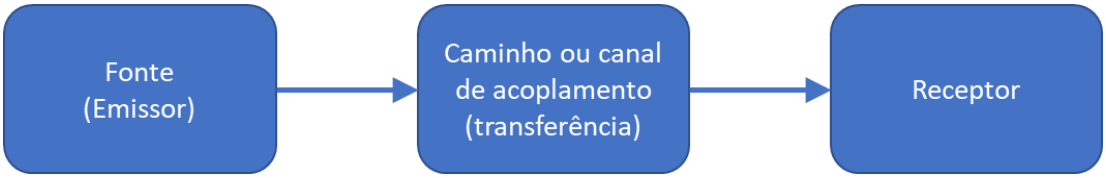


Figura 3:Estrutura básica dos acoplamentos eletromagnéticos.
Fonte: Adaptado de (PAUL, 2006).

A interferência eletromagnética ocorre se a energia eletromagnética recebida, causar no receptor, uma operação indesejada. A partir da estrutura básica apresentada na Figura 3, pode-se concluir que existem três maneiras de se prevenir a interferência: suprimir a emissão na fonte; tornar o caminho de acoplamento o mais ineficiente possível; ou tornar o receptor imune à emissão (PAUL, 2006).

A IEC classifica as principais perturbações relacionadas à IEM em seis categorias (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2020):

1. Perturbação conduzida em baixas frequências;
2. Perturbação radiada em baixas frequências;
3. Perturbação conduzida em alta frequência;
4. Perturbação radiada em alta frequência;
5. Descargas eletrostáticas;
6. Pulsos eletromagnéticos de grande amplitude (em inglês, HEMP – *High-amplitude nuclear electromagnetic pulse*).

Dentro de cada categoria acima-citadas estão inclusos diversos fenômenos, cujo detalhamento pode ser encontrado na Tabela 3, apresentada na seção 2.2.

É importante salientar que os métodos de determinação de riscos para segurança funcional considerando os eventos de interferência eletromagnética, devem abranger todas as perturbações relacionadas anteriormente, de acordo com o ambiente eletromagnético analisado.

2.6.2 Segurança Funcional e Resiliência Eletromagnética

Essa seção tem como objetivo destacar os procedimentos sugeridos visando atingir resiliência eletromagnética, em especial, os aspectos relacionados aa determinação de risco. Os procedimentos indicados têm como base as principais referências na literatura relacionada ao tema em estudo, sendo, inicialmente, mencionadas as recomendações das normas IEC 61508 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010) e IEC 61000-1-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016).

A norma IEC 61508 é a publicação básica atual relacionada à segurança funcional de equipamentos elétricos, eletrônicos e eletrônicos programáveis (E/E/PE). Como já mencionado no item 2.3, ela apresenta as recomendações gerais para obtenção de segurança funcional. Nota-se, no entanto, que esta não apresenta requisitos específicos para o tratamento dos efeitos das perturbações eletromagnéticas. Para esse propósito, a norma IEC 61000-1-2 fornece um guia para a avaliação das perturbações eletromagnéticos nos sistemas elétricos relacionados à segurança.

Ressalta-se que o processo para obtenção segurança funcional considerando os aspectos de CEM envolve todo o ciclo de vida do sistema ou equipamento, desde a concepção do projeto até o seu descomissionamento (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010). Esse ciclo e a relação entre as principais referências normativas são apresentados na Figura 4.

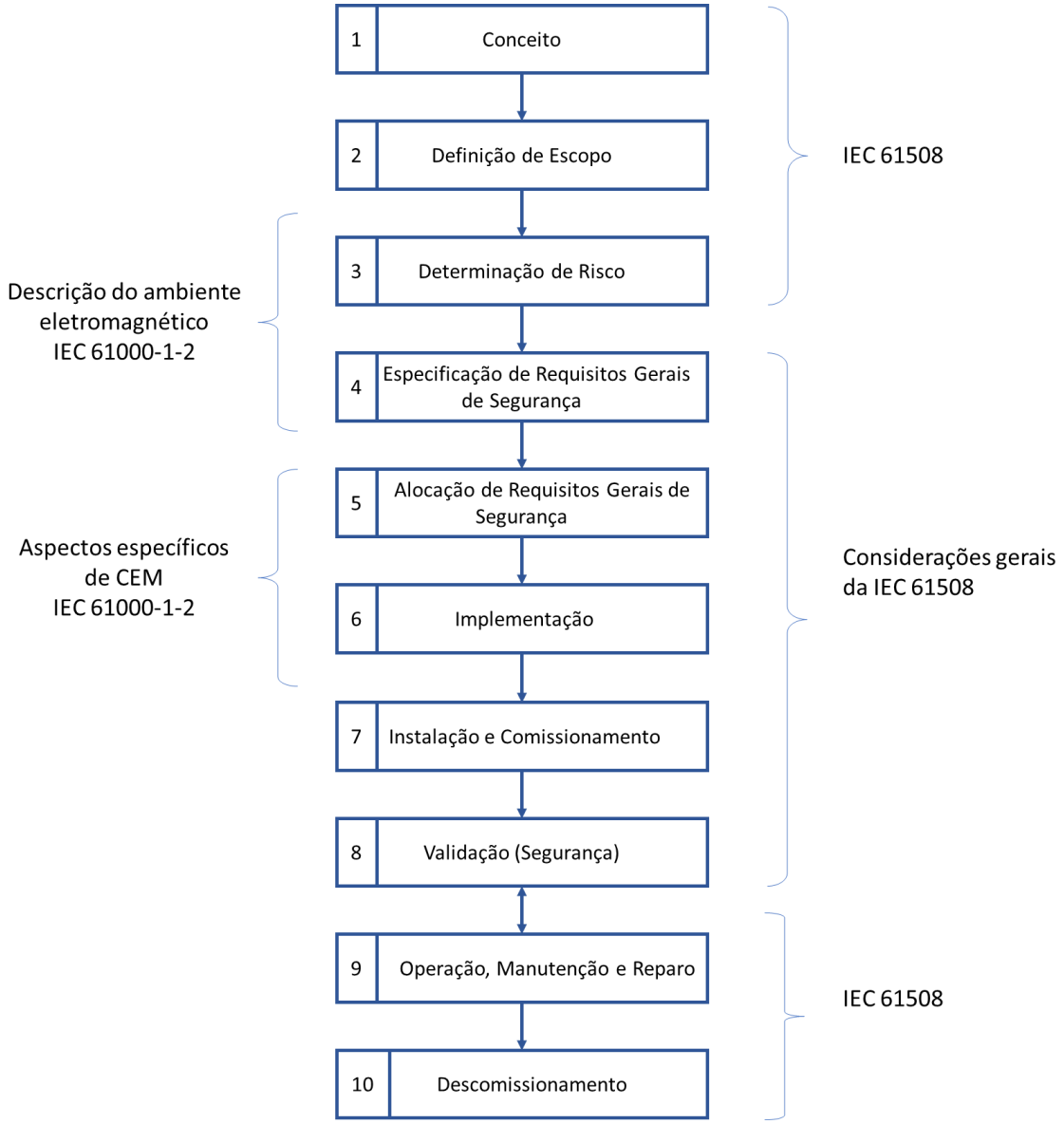


Figura 4: Ciclo de vida de segurança funcional e aspectos de CEM, relacionando as normas IEC 61508 e IEC 61000-1-2.
Fonte: Adaptado de (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010) e (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016).

Para um maior entendimento, cada uma das etapas apresentadas na Figura 4 são descritas em maior detalhe na Tabela 8, de acordo com numeração utilizada anteriormente.

Tabela 8 – Descrição das atividades relacionadas na Figura 4 para obtenção da resiliência eletromagnética. Fonte: Adaptado de (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010) e (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2016).

Etapa	Descrição das atividades de segurança funcional
1 – Conceito	Entendimento do sistema ou equipamento sob controle e seu ambiente de utilização, como condições físicas, de legislação etc., de modo a permitir as etapas seguintes, descritas abaixo.
2 – Escopo	Determinação dos limites e interfaces do equipamento sob controle e seu respectivo sistema de controle. Especificação do escopo da análise de risco, como por exemplo, tipos de riscos a serem analisados.
3 – Determinação de Risco	Determinação de riscos (eventos iniciadores e sequência de eventos) relacionados aos equipamentos e sistemas de controle, em todos os modos de operação. Todas as circunstâncias com probabilidade de ocorrência devem ser consideradas, incluindo mal uso e condições de falhas. Nota-se que as considerações sobre o ambiente eletromagnético devem ser realizadas nesta etapa, como a sua avaliação, níveis de testes e métodos, considerações sobre as perturbações eletromagnéticas e níveis de integridade de segurança (SILs).
4 – Especificação de requisitos de segurança	Desenvolvimento de especificação para requisitos gerais de segurança (funções de segurança e integridade de segurança) para os sistemas E/E/PE relacionados à segurança e determinação de medidas redução de risco.
5 – Alocação de requisitos de segurança	Alocação das funções de segurança para os sistemas relacionados à segurança projetados. Determinação de níveis de integridade de segurança (SIL) para cada função de segurança a ser executada por um sistema E/E/PE.
6 – Implementação	Criação dos sistemas E/E/PE de acordo com as especificações de requisitos. Devem ser considerados os aspectos de CEM para sistemas e de equipamentos.
7 – Instalação e Comissionamento	Desenvolvimento de um plano para instalação e comissionamento dos sistemas E/E/PE de segurança para garantir que a segurança funcional requerida será atingida.
8 – Validação (Segurança)	Desenvolvimento de um plano de validação de segurança para equipamentos E/E/PE. O processo de validação e verificação deve analisar os critérios de performance e a filosofia de testes, inspeções, análises e demonstrações, os níveis e métodos de testes de imunidade em relação a segurança funcional.

Etapa	Descrição das atividades de segurança funcional
9 – Operação, Manutenção e Reparo	Apresentação de plano para operação, manutenção, reparos e modificações dos sistemas E/E/PE, de modo a garantir que a segurança funcional requerida é atingida durante essas etapas (operação, manutenção e reparo).
10 – Descomissionamento	Definição dos procedimentos para garantir segurança funcional durante e após as atividades de descomissionamento e descartes dos equipamentos controlados.

Dentre todas as etapas apresentadas anteriormente na Figura 4, ressalta-se que o foco principal deste trabalho se encontra na utilização de técnicas para a realização de determinação de risco (etapa 3 do diagrama). Enfatiza-se que estas visam atender os critérios e necessidades da análise de segurança funcional, em especial, àquelas relacionadas às perturbações eletromagnéticas. Deve-se observar que a determinação de risco, embora seja realizado como um dos primeiros passos no ciclo de vida de segurança, apresenta resultados com impactos em todas as etapas seguintes. Os documentos produzidos na determinação de risco devem ser readequados à medida que modificações são realizadas no projeto, sendo utilizados durante o projeto, desenvolvimento, instalação, operação etc. A determinação de risco é, portanto, um processo contínuo, sendo realizado e atualizado juntamente com a evolução no desenvolvimento dos sistemas e equipamentos.

2.6.3 Etapas de Determinação de Riscos

Observa-se que, a determinação de risco é um importante passo no processo de obtenção de resiliência eletromagnética. A fim de esclarecer a nomenclatura e definições utilizadas, observa-se que a determinação de risco, foco deste trabalho, é parte integrante do gerenciamento de riscos. O gerenciamento de riscos, por sua vez, é um processo gerencial contínuo com objetivo de identificar, analisar e avaliar perigos potenciais em sistemas ou atividades, e identificar e introduzir medidas de controle para eliminar ou reduzir os efeitos potenciais para as pessoas e para o ambiente (RAUSAND, 2011). A determinação de risco é um dos três elementos principais do gerenciamento de riscos, juntamente com o planejamento e o tratamento de riscos (AVEN, 2015). Adicionalmente, o gerenciamento de riscos compreende, ainda, a comunicação entre as partes interessadas e o monitoramento regular (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

Como apresentado, a determinação de risco (do inglês, *risk assessment*) é o elemento principal do gerenciamento de riscos. Ele é composto por três etapas principais

(INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019): Identificação de riscos (do inglês, *risk identification*), análise de riscos (do inglês, *risk analysis*) e a avaliação de riscos (do inglês, *risk evaluation*). É importante salientar que, embora na tradução oficial da norma IEC/ISO 31010 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019) tenha sido utilizado o termo "processo de avaliação de risco" para a tradução de "*risk assessment"*, essa opção pode causar confusão com a terceira etapa da determinação de risco (avaliação de risco). Deste modo, nesta dissertação, optou-se pela utilização da tradução "determinação de risco", por evitar erros de entendimento e ser a tradução utilizada em diversas normas de determinação de risco de dispositivos médicos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2019).

A identificação de riscos tem o objetivo de identificar as fontes e a natureza dos riscos, avaliando também a incerteza associada com a atividade ou fenômenos em consideração. Essa etapa avalia todo o universo de eventos e tenta responder à questão "O que poderia dar errado?". Recomenda-se a inclusão de ao menos quatro grandes fontes de falhas: as falhas de hardware, as falhas de software, falhas organizacionais e falhas humanas (HAIMES, 2008).

A análise de riscos é um uso sistemático da informação disponível para estimar as probabilidades e as consequências para indivíduos, propriedades e para o ambiente dos riscos identificados na etapa anterior. São realizadas nesta etapa: a análise de consequência, a análise de frequência ou probabilidade, análise da efetividade dos controles existentes e a estimativa do nível de riscos. Para sistemas complexos, poderá ser necessária a utilização de mais de uma técnica para atender as necessidades desta etapa. As técnicas podem ser quantitativas, qualitativas ou semiquantitativa, de acordo com a abordagem para quantificação das consequências e probabilidades de ocorrência. Recomenda-se ainda nesta etapa, a consideração de incertezas e realização de análise de sensibilidade (avaliação de significância das incertezas nos dados a partir da determinação da mudança relativa dos resultados devido a alterações dos parâmetros individuais de entrada) (RAUSAND, 2011) (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

A avaliação de riscos tem como objetivo a comparação dos níveis estimados de risco com os critérios definidos, de modo a determinar o nível de significância de cada risco. Ela utiliza a informação da análise de risco para a tomada de decisões sobre as ações futuras. Entre as decisões, encontram-se a necessidade de tratamento para um risco, quais riscos devem ser tratados primeiramente, quais atividades devem ser executadas, a seleção entre as opções existentes, etc. Uma estratégia bastante utilizada para sistema de segurança é a definição de três níveis para os riscos: intoleráveis, necessitando de tratamento independentemente de quaisquer

outros fatores; toleráveis, devendo ser reduzidos até seja possível economicamente; e riscos negligenciáveis, que não necessitam de tratamento (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

Pode-se sumarizar as relações entre o gerenciamento de risco, a determinação de risco e todas as suas partes constituintes pela Figura 5.

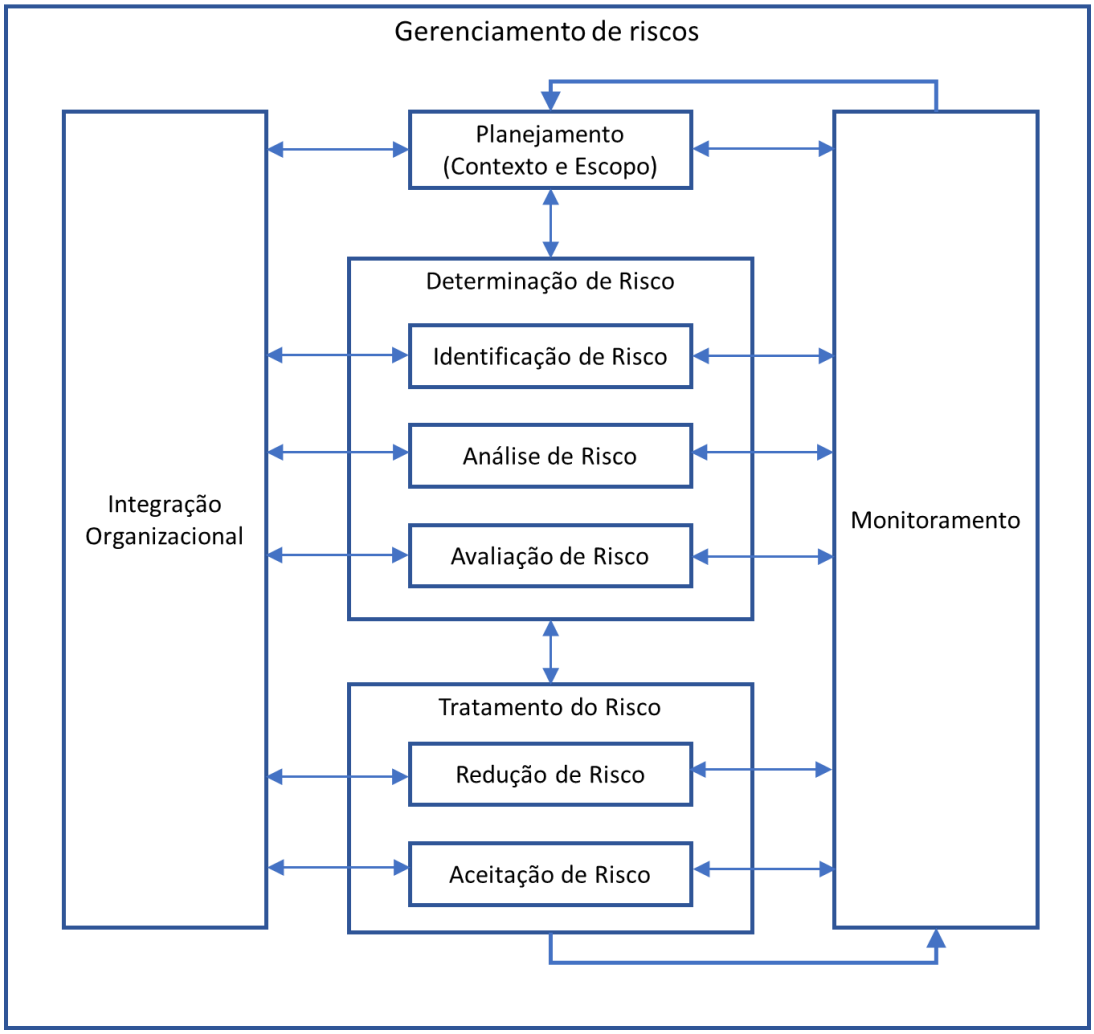


Figura 5: O gerenciamento de riscos e a determinação de riscos. Fonte: Adaptado de (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

As etapas de determinação de riscos, apresentadas na estrutura da Figura 5, são utilizadas, neste trabalho, para a definição das categorias dos critérios a serem definidos para a classificação de cada uma das técnicas de determinação de risco apesentadas, definidos na seção 3.2.

3 Metodologia

Neste capítulo, apresenta-se a metodologia proposta para a comparação e determinação do elenco das técnicas para a determinação de riscos em relação a resiliência eletromagnética, sendo estabelecidas duas grandes etapas: a revisão sistemática de técnicas de determinação de risco; e a apresentação de estrutura de hierarquização dos métodos de avaliação de risco para obtenção de resiliência eletromagnética, sendo este, por sua vez, composto pela definição de critérios gerais e específicos para a análise de decisão de multicritério.

3.1 Procedimento Proposto para Seleção de Técnicas de Determinação de Risco Adequadas para Resiliência Eletromagnética

Nesta seção, apresenta-se uma proposta para o procedimento de seleção de técnicas adequadas de determinação de risco para a obtenção de resiliência eletromagnética. Este procedimento consiste em quatro passos principais, descritos a seguir.

Passo 1: Estabelecimento de critérios aplicáveis: Para permitir a comparação entre as técnicas, é necessário a definição de uma base comparativa. Deve-se, portanto, estabelecer os critérios aos quais as técnicas de determinação de risco serão avaliadas. Com esse objetivo, propõe-se a definição de duas categorias de critérios: os critérios gerais (caráter eliminatório), utilizados nas classificações genéricas das técnicas, e os critérios específicos (caráter classificatório), relacionados a adequação daquelas para a utilização nos processos de obtenção de resiliência eletromagnética. A definição e origem dos critérios está detalhada na seção 3.2.

Passo 2: Definição das técnicas de determinação de risco para comparação: A definição das técnicas de avaliação de risco a serem comparadas pode ser realizada de diversas maneiras, por exemplo, com base no conhecimento prévio dos especialistas e das partes interessadas envolvidas nos projetos em questão. Neste trabalho, optou-se pela execução de uma pesquisa sistemática na literatura para definir as técnicas de determinação de risco de maior relevância nos últimos anos que serão, posteriormente, avaliadas em relação aos critérios previamente estabelecidos. O objetivo da pesquisa sistemática é evitar o enviesamento na escolha das técnicas e garantir uma ampla avaliação de diversas técnicas, sendo descrita na seção 3.3.

Passo 3: Formulação do problema de seleção: Após a definição dos critérios e opções de técnicas disponíveis, deve-se indicar o escopo e os objetivos do problema de seleção. Nesta

fase, deve-se verificar a existência de relações de dependência entre critérios e opções, para garantir a consistência das informações e evitar a ponderação com peso sobreavaliado de determinados critérios, obtendo resultados mais confiáveis. Após a determinação das dependências, recomenda-se a criação de um diagrama ou matriz para apresentação visual das relações entre os grupos de avaliação, permitindo a realização do próximo passo. Essa etapa ainda deve incluir a verificação dos critérios gerais estabelecidos previamente, de modo a considerar as técnicas que consideram os objetivos mínimos da avaliação.

Passo 4: Método de Apoio Multicritério à Decisão – AMD (do inglês, *Multi-Criteria Decision Analysis – MCDA ou Multi-Criteria Decision Making – MCDM)*: Para classificar as técnicas de avaliação de risco, de acordo com os critérios estabelecidos, é necessária a utilização de um método de análise de decisão. Os métodos AMD são ferramentas para conduzir uma decisão com múltiplos critérios e opções, capturando o ponto de vista subjetivo dos tomadores de decisão. Neste trabalho, propõe-se a utilização do Processo de Redes Analíticas (do inglês, *Analitycal Network Process – ANP*) para estruturação do problema de decisão e cálculo de prioridades (escores) a partir dos critérios específicos derivados. O ANP é uma generalização do *Analytic Hierarchy Process (AHP)*, outra técnica de MCDA criada por Thomas L. Saaty com base nas comparações pareada; entretanto, ao contrário do AHP, onde o problema de decisão é estruturado de forma hierárquica, no ANP o problema de decisão é estruturado em forma de rede. Neste método, grupos e nós (elementos) substituem os níveis hierárquicos, permitindo a consideração de dependências entre critérios, subcritérios e alternativas (SAATY, 2004). Uma breve discussão dos métodos de AMD e o detalhamento da aplicação do ANP são abordados na seção 3.4.

A Figura 6 apresenta a estrutura propostas para a seleção de técnicas de determinação de risco em relação a obtenção de resiliência eletromagnética. Pode-se observar que, como já descrito anteriormente, apenas os critérios específicos são utilizados para realizar a classificação das técnicas por meio da análise de apoio à decisão multicritério no passo 4, sendo que os critérios gerais serão utilizados com caráter eliminatório no passo 3, durante a formulação e pré-seleção das técnicas de avaliação de risco.

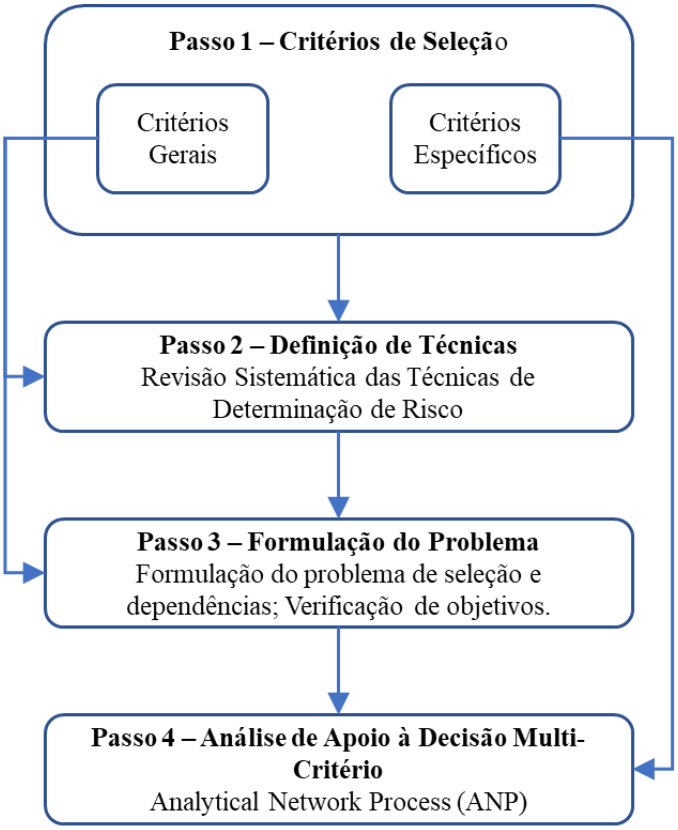


Figura 6: Estrutura metodológica de seleção de técnicas de determinação de risco em relação à resiliência eletromagnética.

3.2 Critérios de Seleção

Para permitir a comparação dos métodos de determinação de risco em relação a sua adequação para utilização nos processos de obtenção de resiliência eletromagnética, devem ser definidas os critérios que compõe a base comparativa para o processo de seleção. Com este objetivo, definem-se duas categorias para os critérios a serem utilizados:

- Critérios Gerias: são definidos com base nas classificações apontadas em literatura para as técnicas de determinação de risco em um contexto amplo de aplicação;

- Critérios específicos: são definidos a partir das necessidades e dificuldades apontadas na literatura e na experiência prática para a área de resiliência eletromagnética.

A definição dos critérios gerais tem como objetivo a seleção dos métodos que atendem os requisitos mínimos para aplicação no sistema que deve ser analisado. Portanto, sua utilização é de caráter eliminatório. Por outro lado, a definição dos requisitos específicos tem como

objetivo a classificação dos métodos de determinação de risco mais adequados para a obtenção da resiliência eletromagnética, apresentando uma abordagem de hierarquização.

Nas subseções seguintes, são discutidos os critérios estabelecidos, assim como os níveis e classificações de cada um deles.

3.2.1 Critérios Gerais

A escolha de uma técnica deve ser adequada ao nível de importância da decisão a ser realizada e deve considerar todas as limitações impostas aos sistemas analisados. Para analisar estas restrições, inicialmente, optou-se por utilizar uma abordagem com requisitos e aplicações reconhecidos de acordo com a norma IEC/ISO 31010 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019), que são descritas a seguir.

a) Objetivo: O objetivo do estudo deve estar alinhado com as funções executadas pelo método para a determinação de risco. Entre as funções executadas pelas técnicas, encontram-se as categorias descritas abaixo:

- Coletar ideias das partes interessadas e especialistas (F1);
- Identificação de riscos (F2);
- Determinação de fontes, causas e iniciadores de riscos (F3);
- Análise de controles existentes (F4);
- Entendimento de consequências e probabilidades (F5);
- Análise de dependências e interações (F6);
- Mensuração dos riscos (F7);
- Avaliação de significância dos riscos (F8);
- Seleção entre opções (F9);
- Registro e relato das ações (F10).

Observa-se que cada uma das possíveis funções executadas pelas técnicas pode ser aplicada em etapas específicas de determinação de risco:

- Identificação: F1, F2, F3;
- Análise: F2, F3, F4, F5, F6, F7;
- Avaliação: F1, F8, F9.

Pode-se observar que a função F10 é executada apenas para registro das ações, após as três etapas de determinação de risco, quando necessário.

b) Tipo de análise desejada: Os métodos podem apresentar diferentes abordagens em relação a sua avaliação e mensuração dos riscos, permitindo avaliações numéricas ou outras baseadas em escalas descritivas.

- Quantitativa;
- Qualitativa;
- Semiquantitativo;
- Ambos (quantitativa e qualitativa).

c) Escopo: O contexto em que os riscos são aplicáveis devem ser claramente definidos de modo a garantir que a escolha do método seja apropriada.

- Organizacional;
- Departamental / Projeto;
- Equipamento ou Processo.

d) Nível de decisão ou a magnitude potencial dos riscos envolvidos: O nível de importância da decisão depende da magnitude dos riscos, podendo ser considerados os seguintes níveis:

- Estratégico;
- Tático;
- Operacional.

e) O tempo disponível para a tomada de decisão: A avaliação também pode ou não conter restrições de tempo. Nota-se que, em alguns casos, como, por exemplo, em projetos cujos ciclos são essencialmente curtos, pode-se inviabilizar a utilização de determinados métodos.

- Curto;
- Médio;
- Longo;
- Qualquer.

f) Necessidade de informação prévia: A disponibilidade de informação e dados presentes ou necessários que obrigatoriamente devem ser obtidas previamente antes da aplicação do método.

- Alto;
- Médio;

- Baixo.

g) Complexidade para aplicação: A escolha das técnicas deve considerar, ainda, o tipo de sistema analisado, avaliando a variedade e a dificuldade dos riscos envolvidos.

- Baixa: equipamentos isolados / componentes ou consideração apenas de falhas aleatórias;
- Média: sistemas ou consideração de falhas sistemáticas;
- Alta: sistemas complexos.

h) O nível de especialidade e experiência disponíveis ou que podem ser obtidos (*personnel skills*): A correta utilização de determinadas técnicas pode depender da necessidade de treinamento do pessoal técnico envolvido na análise ou requerer experiência em sua aplicação. Portanto, essa demanda também deve ser considerada.

- Baixo (intuitivo)
- Médio (treinamento curto)
- Alto (treinamento significativo)

3.2.2 Critérios Específicos de Resiliência Eletromagnética

Os critérios específicos são estabelecidos, neste trabalho, com o objetivo de superar as dificuldades apontadas em literatura para a disciplina de engenharia de segurança funcional relacionada a compatibilidade eletromagnética, conhecida como resiliência eletromagnética. As principais características e preocupações relacionadas a resiliência eletromagnética são compilados na primeira coluna da Tabela 9 (ARMSTRONG, 2010) (ARMSTRONG e DUFFY, 2020) (ARMSTRONG, 2016). As medidas ou análises para superar as considerações apontadas em literatura são propostas neste trabalho na segunda coluna da Tabela 9. Elas foram obtidas com o objetivo de garantir que as considerações realizadas na literatura sejam integradas na determinação de risco, garantindo que, deste modo, essas características sejam consideradas no processo de obtenção de resiliência eletromagnética.

Tabela 9 – Características abordadas em literatura e critérios derivados.

Características	**Medidas Aplicáveis / Critérios Possíveis**
Falhas ou variações na produção de equipamentos que podem afetar imunidade não são consideradas	Análises de variância e incerteza (processo e ambiente): a. Projeto: variáveis críticas de projeto necessitam ser avaliadas; b. Montagem: Partes do processo de montagem que podem impactar nos aspectos funcionais do equipamento c. Ambiente eletromagnético: Avaliação do ambiente eletromagnético da aplicação, considerando possibilidades em relação aos espectros esperados e respectivas intensidades.
O ambiente simulado através dos ensaios se difere do ambiente eletromagnético real (tipos de modulação e frequências convencionais são diferentes das interferências eletromagnéticas reais)	
Erros de montagem, instalação e configuração são ignorados	
Mal uso dos equipamentos não são previstos na avaliação	Avaliação de aspectos de mal uso: Avaliação de Confiabilidade Humana - ACH
Falhas concorrentes ou interação entre falhas não analisadas	- Falhas de Causa Comum (FCC) - Comportamento temporal e hierárquico dos sistemas
Perturbações eletromagnéticas simultâneas não são testadas ou simuladas	
Efeitos sistemáticos são ignorados (combinação entre partes imunes não criam um sistema imune)	Análise de falhas sistemáticas
Falhas causadas por IEM não podem ser testadas ou simuladas.	
Efeitos das condições ambientais e utilização são ignorados	Avaliação de desgastes por temperatura, mecânicos, químicos, biológicos e operacionais (repetição, fricção etc.).
Os níveis de perturbações mais altos atribuídos para os testes, nem sempre são os mais críticos.	A serem considerados na avaliação do ambiente eletromagnético, citado no item (c) da primeira linha da tabela

A partir das possíveis medidas aplicáveis, apontadas na segunda coluna da Tabela 9, sugere-se a utilização dos seguintes critérios específicos:

- Critério específico nº 1: Avaliação de Envelhecimento;
- Critério específico nº 2: Falhas sistemáticas;
- Critério específico nº 3: Avaliação de Confiabilidade Humana – ACH;
- Critério específico nº 4: Falhas de Causa Comum – FCC;
- Critério específico nº 5: Comportamento temporal e hierárquico dos sistemas;
- Critério específico nº 6: Análise de Incertezas.

3.3 Revisão Sistemática das Técnicas de Determinação de Risco

Devido à grande quantidade de métodos existentes para realizar a determinação de risco, pretende-se adotar um procedimento no qual os métodos sejam pré-selecionados, para uma posterior hierarquização, considerando-se sua relevância e os critérios para alcançar resiliência eletromagnética, ou seja, deseja-se realizar uma revisão sistemática (pré-seleção) dos métodos a serem hierarquizados para uso nas análises com o objetivo de alcançar segurança funcional de sistemas elétricos e eletrônicos relacionados à segurança considerando as perturbações eletromagnéticas. Para realizar esse procedimento, propõe-se a execução da metodologia de revisão sistemática descrita a seguir.

A revisão proposta tem como ponto de partida a avaliação das técnicas de determinação de risco descritas na Tabela 10, estabelecidas em função de terem sido citadas nos artigos científicos obtidas durante o processo de revisão bibliográfica deste trabalho. Uma breve descrição de cada uma das técnicas apresentadas na tabela pode ser encontrada no Anexo B.

Tabela 10 – Métodos avaliados na revisão sistemática das técnicas de determinação de risco.

Absolute Probability Judgment (APJ) / Direct numerical estimation	Hazardous Scenario Analysis (HAZSCAN) / Hazard identification (HAZID)
Accident Hazard Index (AHI)	Hierarchical Task Analysis (HTA) Hierarchical Task Network (HTN)
Accident Sequences Precursor (ASP)	Human Error Assessment and Reduction Technique (HEART)
AcciMap Approach	Human Factor Event Analysis (HFEA)
Action Error Analysis (AEA)	Human Factors Analysis and Classification System (HFACS)
ALARP, ALARA ou SFAIRP	Incident Review / Incident Report
Anticipatory Failure Determination (AFD)	Layer of protection analysis (LOPA) / Barrier Analysis
Barrier and operational risk analysis (BORA)	Markov analysis
Bayesian statistics or Bayesian Networks / Statistics / Nets / Model	Master Logic Diagram
Bow-tie analysis/method	Maximum Credible Accident Analysis (MCAA)
Brainstorming	Method Organised Systematic Analysis of Risk (MOSAR - Méthode Organisée et Systémique d'Analyse de Risques)
Business impact analysis / assessment (BIA)	Monte Carlo Simulation

Causal Mapping or Causal Map	Normal Accident Theory (NAT)
Cause-and-consequence analysis (CCA) or diagrams	Nuclear Action Reliability Assessment (NARA)
Cause-and-effect analysis / Cause-effect diagram / Ishikawa Diagram / Fish-bone diagram / Herringbone diagram	Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
Cindynic Approach	Optimal Risk Assessment (ORA)
Clinical Risk and Error Analysis (CREA)	Petri Nets (or Time Petri Nets)
Cognitive Reliability and Error Analysis Method (CREAM)	Predictive, Epistemic Approach (PEA)
Common cause failure (CCF) analysis	Preliminary Hazard Analysis (PHA) / Primary hazard analysis
Concept Hazard Analysis (CHA)	Rapid Risk Analysis Based Design (RRABD) / Rapid Risk Assessment (RRA)
Concept Safety Review (CSR)	Reliability block diagrams (RBD) / Dependence diagram (DD)
Cost-benefit analysis	Reliability centred maintenance
Cost-Of-Risk Analysis (CORA)	Risk and Vulnerability analysis (RVA)
Cross Impact Analysis	Risk indices / Risk Level Indicators (RLI) / Key Risk Indicators (KRIs)
Decision matrix risk-assessment (DMRA)	Risk-based Maintenance (RBM)
Decision tree analysis	Scenario analysis / Scenario-based design
Delphi / Estimate-Talk-Estimate or ETE	SEQHAZ Hazard Mapping
Event tree analysis (ETA)	Sequentially Timed Event Plotting (STEP)
External Events Analysis	Sneak circuit analysis / Sneak Analysis
Facilitated Risk Analysis and Assessment Process (FRAAP) / Facilitated risk analysis process (FRAP)	Structure « What if? » (SWIFT)
Failure mode effect analysis (FMEA)	Structured or semi-structured interviews
Failure mode effect and critically analysis (FMECA)	Success Likelihood Index Methodology / Success Likelihood Index Method (SLIM)
Fault/Functional Hazard Analysis (FHA)	Swiss Cheese Model (SCM) - SCM-based model - Reason Model (the ATSB accident investigation model)
Fault insertion testing / Fault Injection testing	System Hazard Identification, Prediction and Prevention (SHIPP)
Fault tree analysis (FTA)	Systematic Human Error Reduction and Prediction Analysis (SHERPA)
Fine Kinney method	Systems-Theoretic Accident Model and Processes (STAMP = CAST + STPA)
FN curves	Technique for Human Error Rate Prediction (THERP)
Functional Resonance Analysis Method (FRAM)	Technique for Human Event Analysis (ATHEANA)
Game Theory	Toxicological risk assessment / Toxicity assessment (TA)

Goal-Oriented Failure Analysis (GOFA)	Value at Risk (VaR) / Conditional Value at Risk (CVaR) (CoVaR)
Hazard Analyzis and Critical Control Points (HACCP)	Weighted risk analysis (WRA)
Hazard and Operability studies (HAZOP)	Worst-case analysis and Worst-case testing
Hazard Identification and Ranking (HIRA)	

Para a determinação da relevância de cada uma das técnicas adotaram-se os critérios descritos a seguir:

1. Técnicas de determinação de risco consideradas: Como apontado anteriormente, consideram-se as técnicas descritas na Tabela 10;
2. Tipo de publicações avaliadas: São avaliados os artigos científicos publicados em revistas e conferências e livros. Desconsideram-se as patentes, capítulos isolados de livros e relatórios de quaisquer outras origens (governamentais ou privados);
3. Tema das publicações: Consideram-se publicações que descrevam detalhadamente, sugiram melhorias, apresentem revisões literárias ou apliquem (com execução demonstrada) a técnica de determinação de risco e subáreas correlacionadas (avaliação de perigos ou de falha, confiabilidade, disponibilidade, segurança, resiliência, análise funcional, etc.), não havendo, entretanto, restrições em relação as áreas de conhecimento da aplicação. Publicações que apenas citem, façam referência ou apenas utilizem os resultados do método sem demonstrar sua aplicação ou demais desenvolvimentos não são consideradas. As técnicas de determinação de risco que são variantes diretas de outras técnicas primárias serão contabilizadas para a técnica primária. Quando utilizada mais de uma técnica em aplicações diretas, estas são contabilizadas para todas as técnicas utilizadas. Publicações que apresentem uma nova metodologia com base em um ou mais métodos, são consideradas como uma nova técnica (híbrida);
4. Língua das publicações: Inglês;
5. Período das publicações: Serão consideradas publicações realizadas entre os anos de 2015 e 2020 (inclusive). Este período é considerado em função do período de elaboração deste documento e visando enfatizar as tendências recentes na utilização das técnicas de determinação de risco, cobrindo, inclusive, o período de publicação das normas internacionais IEC 61000-1-2 (INTERNATIONAL

ELECTROTECHNICAL COMMISSION, 2016) e IEEE 1848 (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 2020);

6. Relevância e citações: Para selecionar os artigos com maior relevância, foram incluídos artigos que tenham ao menos 20 citações nas ferramentas de busca consultadas. Essa abordagem foi definida em função de uma análise preliminar para a redução do universo de obras a serem avaliadas e viabilização desta revisão sistemática;
7. Ferramentas acadêmicas de busca e banco de dados de publicações científicas:
   Pesquisa dos artigos e livros: Para a pesquisa dos artigos e livros relacionados as técnicas de análise de risco foram avaliadas diversas bases de dados e ferramentas de busca, decidindo-se pela adoção das seguintes bases de dados e ferramentas de busca de conteúdos científicos:
   - SCOPUS (http://www.scopus.com); e
   - Web of Science (https://login.webofknowledge.com/).

O *SCOPUS* é o maior banco de dados de resumos e citações de literatura revisada por pares: revistas científicas, livros e anais de conferência, tendo sido fundado em 2004. Ele cobre campos da ciência, tecnologia, medicina, ciências sociais, e artes e humanidades (ELSEVIER, 2020). De acordo com os dados apontados pelo seu provedor, o *Scopus* possui atualmente publicações de mais de 23 mil revistas científicas e mais de 9.8 milhões de artigos de conferência de mais de 120 mil eventos ao redor do mundo. Além disso, possui uma vasta quantidade de livros, superando a marca dos 200 mil livros em sua base.

O *Web of Science* é uma ferramenta de busca de conteúdos acadêmicos, mantida pela Clarivate Analytics, que possui artigos publicados a partir do ano de 1900 em 254 categorias de assuntos. Relaciona publicações de mais de 34 mil revistas científicas, possuindo mais de 170 milhões de registros (CLARIVATE, 2020).

Além das características dos bancos de dados apontadas acima, ressalta-se que as ferramentas selecionadas possuem os recursos necessários de filtragem e seleção para atender os critérios de busca estabelecidos pela metodologia descrita nessa seção (3.3). Uma consideração deve ser realizada em relação ao *Google Scholar*, o banco de dados com maior volume de informações acadêmicas da atualidade (GUSENBAUER, 2019). Ressalta-se que ele não foi utilizado por motivações técnicas, devido a este não apresentar os requisitos de filtragem necessárias (tipos de

conteúdo, número de citações etc.) para a execução da metodologia. Adicionalmente, autores tem apontado inconsistências em sua utilização (como, por exemplo, a indexação de revistas científicas não-existentes) (CLERMONT e DYCKHOFF, 2012) e a falta de transparência da sua cobertura (GUSENBAUER, 2019)

A escolha por grandes bases de dados ocorre devido a estas disponibilizarem conteúdos de diversas áreas de aplicação, sendo que o objetivo é buscar as aplicações das técnicas em diversas áreas possíveis, uma vez a análise de risco é multidisciplinar. Ressalta-se que muitas técnicas surgiram para avaliações de aspectos sociais e se encaminharam para aplicações voltadas aos sistemas elétricos e eletrônicos, assim como, o caminho inverso também já foi realizado.

Deve-se observar que as palavras chaves para cada técnica de análise de risco utilizadas nas ferramentas de busca dos bancos de dados são apresentadas no Anexo A.

8. Avaliação final de relevância das técnicas: A avaliação para classificação de relevância das técnicas tem como base dois parâmetros: o número total de artigos publicados no período que atendam os critérios estabelecidos desta pesquisa e a soma total de citações de todos os artigos e livros de cada técnica. Cada um destes parâmetros irá compor um valor normalizado entre 0 e 1 (resultado da relação entre o número encontrado e o máximo obtido para o mesmo parâmetro) que serão somados e posteriormente divididos por dois para compor uma média que representa o valor final de relevância das técnicas (R-Fator). Ou seja:
   - Fator de número de artigos (A-Fator): Número total de artigos de uma técnica divido pelo maior número de artigos encontrados para a técnica com mais artigos entre as avaliadas;
   - Fator de número de citações (C-Fator): Número total de citações dos artigos de cada técnica dividido pelo número máximo de citações para a técnica com mais citações;
   - Fator de relevância final (R-Fator): Valor de relevância final de cada uma das técnicas consideradas, calculado pela média dos fatores A-Fator e C-Fator.

$$\text{R-Fator} = (\text{A-Fator} + \text{C-Fator}) / 2$$

Ressalta-se que, quando um artigo for apresentado em ambas as bases de dados e apresentar diferenças em relação ao número de citações, será utilizada um operador

maior para definir o maior número de citações apresentadas pelos dois bancos de busca. Caso apareça em apenas uma delas, será considerado esse número diretamente.

9. Análises posteriores: Para as análises posteriores, serão consideradas as técnicas mais relevantes com base no Princípio de Pareto (regra 20/80), princípio utilizado em diversas áreas de conhecimento como economia, engenharia de software, entre outros, que afirma que, para muitos eventos, aproximadamente 80% dos efeitos vêm de 20% das causas.

3.4 Método de Apoio Multicritério à Decisão (AMD): Analytical Network Process (ANP)

Para completar a metodologia na escolha ou hierarquização das técnicas de determinação de riscos adequadas ao processo de obtenção de resiliência eletromagnética, é proposta a utilização de uma ferramenta que se constitui na realização de análises de decisão multicritério (do inglês, *Multi-Criteria Decision Making* - *MCDM*) para avaliação e hierarquização das técnicas a serem aplicadas, em função da sua adequabilidade às considerações relacionadas à resiliência eletromagnética.

Os métodos de apoio multicritério à decisão são ferramentas valiosas para resolver questões que possuam múltiplos atores, critérios e objetivos, sendo utilizadas para a decisão em problemas em que se deve realizar a seleção, a categorização, hierarquização ou descrição de opções. Em geral, os problemas de decisão multicritério são compostos por cinco componentes: o objetivo, as preferências dos tomadores de decisão, as alternativas, os critérios e os resultados (MATEO, 2012). Normalmente, os métodos podem ser classificados em relação à quantidade de alternativas em consideração, seja de atributos (tomada de decisão de múltiplos atributos) ou de objetivos (tomada de decisão de múltiplos objetivos), ou em relação as abordagens dos métodos, que podem ser (ISHIZAKA e NEMERY, 2013):

- Abordagem de agregação completa: Atribui-se uma avaliação para cada critério e as avaliações são sintetizadas em uma avaliação global. Neste caso, existe uma compensação de avaliações, ou seja, uma avaliação negativa para um critério pode ser compensada por uma boa avaliação em outro;
- Abordagem de superação: Nesta abordagem, a hierarquização das opções pode ser parcial pois a noção de incomparabilidade é permitida, sendo que duas opções

podem ter a mesma avaliação, entretanto seus comportamentos podem ser diferentes e, portanto, incomparáveis;

- Abordagem de objetivo ou meta: São definidas metas para cada um dos critérios e, então, são identificadas as opções mais próximas da referência ideal.

Observa-se que existem diversas técnicas para cada uma das abordagens. Foram consideradas para utilização neste trabalho as técnicas listadas a seguir:

- AHP (do inglês, *Analytical Hierarchical Process*);
- ANP (do inglês, *Analytical Network Process*);
- MAUT (do inglês, *Multi-Attribute Utility Theory*);
- MACBETH (do inglês, *Measuring Attractiveness by a Categorical Based Evaluation Technique);*
- PROMETHEE (do inglês, *Preference Ranking Organization METHod for Enrichment Evaluations*);
- ELECTRE (do francês, *Elimination Et Choix Traduisant la REalité*);
- TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution).

A Tabela 11 apresenta um resumo das principais características dos métodos de apoio multicritério à decisão (ISHIZAKA e NEMERY, 2013), assim como suas principais referências.

Tabela 11 – Métodos de decisão multicritério e características. Fonte: Adaptado de (ISHIZAKA e NEMERY, 2013).

Técnicas	**Abordagem**	**Características**	**Principais Referências**
AHP	Agregação	AHP é uma técnica utilizada para auxiliar, de forma estruturada, na tomada de decisões complexas com base em comparações pareadas (dois a dois) entre as alternativas. A técnica foi desenvolvida por Thomas L. Saaty nos anos de 1970 e tem sido aplicada em diversas áreas de conhecimento. Possui uma abordagem hierárquica, onde objetivos, critérios e alternativas são representados em três diferentes níveis em uma estrutura hierárquica.	(SAATY, 1977) (VAIDYA e KUMAR, 2006)
ANP	Agregação	Método criado por Thomas L. Saaty em 1996, sendo uma forma generalizada do AHP. Também utiliza a comparação pareada para a avaliação das opções, entretanto, ao contrário do AHP que estrutura o problema de decisão em uma hierarquia, o ANP o faz em forma de uma rede. O método permite a avaliação de casos em que existem interdependências entre as alternativas e critérios.	(SAATY, 1996) (ISHIZAKA e NEMERY, 2013) (SAATY, 2004)

MAUT	Agregação	O método pressupõe que as preferências dos tomadores de decisão podem ser representadas em uma função, chamada de função de utilidade. As avaliações de utilidade descrevem o grau de bem-estar que as alternativas geram aos avaliadores, sendo que o método tem o objetivo de otimizar a função que agrega todos os pontos de vista.	(KEENEY e RAIFFA, 1976) (WALLENIUS, DYER, *et al.*, 2008)
MACBETH	Superação	Apesar de parecer similar ao AHP do ponto de vista do usuário, pela necessidade de comparações pareadas realizadas pelo tomador de decisão, o método se difere por utilizar na sua avaliação uma escala de intervalos ao invés de uma escala de proporção, além de possuir um processo de cálculo diferente. Seus problemas são estruturados em árvore ou hierarquia, com diferenciação dos nós de critérios em relação aos outros.	(BANA E COSTA e VANSNICK, 1999)
PROMETHEE	Superação	Método que permite a hierarquização de ações (escolhas ou alternativas) utilizando, como base, graus de preferência (avaliações entre zero e um que representam o	(BRANS, VINCKE e MARESCHAL, 1986) (BEHZADIAN, KAZEMZADEH, *et al.*, 2010)

		quanto uma ação é preferível em relação a outra) e em funções de preferência para cada critério (que modela relação e preferência). Ele é utilizado em conjunto com o plano de Gaia, uma representação em duas dimensões que apresenta de modo gráfico todas as partes do problema de decisão (critérios, as ações e informações de preferência).	
ELECTRE	Superação	ELECTRE faz referência, na realidade, a toda uma família de técnicas de superação. Os métodos utilizam, entretanto, são mais complexos em relação aos métodos de agregação devido a grande quantidade de parâmetros técnicos e a complexidade do algoritmo para a obtenção das recomendações finais. Inicialmente desenvolvido na década de 1960 por Bernard Roy, a técnica possui a vantagem de não realizar compensações entre critérios nas avaliações ou de estabelecer qualquer tipo de normalização.	(ROY3, 1968) (ROY, 1991) (GOVINDAN e JEPSEN, 2016)
TOPSIS	Objetivo	Este método, proposto por Hwang e Yoon em 1981, permite a avaliação de opções em relação	(HWANG e YOON, 1981)

		aos critérios ao determinar o desempenho das alternativas por meio do cálculo das suas distâncias para a solução ideal (minimização) e para a solução anti-ideal (maximização). O tomador de decisão deve obter as informações de performance das alternativas em relação aos critérios assim como avaliar os pesos relativos dos critérios.	(LAI, LIU e HWANG, 1994) (BEHZADIAN, KHANMOHAMMADI OTAGHSARA, *et al.*, 2012)

Neste trabalho, propõe-se a utilização do Processo de Redes Analíticas (do inglês, Analytical Network Process – ANP) para estruturação do problema de decisão e cálculo de prioridades (score). O ANP é uma generalização do Analytic Hierarchy Process (AHP), sendo também criada por Thomas L. Saaty e tendo como base as comparações de pares; entretanto, ao contrário do AHP, onde o problema de decisão é estruturado de forma hierárquica, no ANP o problema de decisão é estruturado em forma de rede (SAATY, 2004). Neste método, grupos (*clusters*) e nós (elementos) substituem os níveis hierárquicos, permitindo a consideração de dependências entre critérios, subcritérios e alternativas. Essas dependências, também chamadas de realimentações (*feedbacks*), podem ser modeladas neste método. Deste modo, uma estrutura hierárquica não é mais necessária, onde cada agrupamentos substituem os níveis e cada agrupamento contém elementos e nós para descrição da rede. Além disso, a ANP fornece uma ferramenta para verificar a consistência das informações fornecidas a respeito das comparações pareadas, sendo conhecida como índice de consistência. Este índice não é uma medida da qualidade ou experiência do tomador de decisão; ele apenas detecta possíveis contradições nas entradas (ISHIZAKA e NEMERY, 2013).

No processo de aplicação do ANP, a influência de cada nó em outros nós (ou seja, objetivo, alternativas e critérios) em uma rede pode ser reunida em uma **supermatriz**. Cada elemento da supermatriz estabelece a relação entre os elementos representados na interseção de colunas e linhas. Quando um elemento não influencia outro elemento, sua prioridade de influência é atribuída (não derivada) como zero (SAATY, 2004). Dois tipos de dependências são possíveis: as internas e as externas. As primeiras ocorrem dentro de um grupo (cluster),

enquanto as segundas ocorrem entre nós de grupos diferentes. Figura 7 exibe a disposição de uma supermatriz e a localização das dependências e pesos atribuídos na mesma para o caso sem dependências externas.

Observa-se que os julgamentos dos avaliadores para as alternativas em relação aos critérios são inseridos nas intersecções das linhas relativas as alternativas com as colunas relativas aos critérios. Os pesos que os critérios têm em relação ao objetivo principal da avaliação de priorização são adicionados nas intersecções das linhas relativas aos critérios e na coluna relativa ao objetivo.

<table>
<tr><td colspan="2" rowspan="2"></td><td rowspan="2">Objetivo</td><td colspan="3">Alternativas</td><td colspan="3">Critérios</td></tr>
<tr><td>A1</td><td>A2</td><td>A3</td><td>C1</td><td>C2</td><td>C3</td></tr>
<tr><td>Objetivo</td><td colspan="2"></td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td></td></tr>
<tr><td rowspan="3">Alternativas</td><td>A1</td><td>0</td><td colspan="3" rowspan="3">Matriz de influência em cada alternativa (dependência interna no grupo de alternativas)</td><td colspan="3" rowspan="3">Priorização local de alternativa em relação aos critérios</td></tr>
<tr><td>A2</td><td>0</td></tr>
<tr><td>A3</td><td>0</td></tr>
<tr><td rowspan="3">Critérios</td><td>C1</td><td rowspan="3">Peso dos critérios</td><td>0</td><td>0</td><td>0</td><td colspan="3" rowspan="3">Matriz de influência em cada critério (dependência interna no grupo de critérios)</td></tr>
<tr><td>C2</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>C3</td><td>0</td><td>0</td><td>0</td></tr>
</table>

Figura 7: Tabela ilustrativa para supermatriz sem dependências externas. Fonte: Adaptado de (ISHIZAKA e NEMERY, 2013).

Para a obtenção da supermatriz e realização dos cálculos de priorização podem ser utilizados *softwares* específicos para a resolução do problema multicritério. A aplicação do ANP e a realização de todos os seus passos detalhados pode ser encontrado na literatura, como por exemplo, pelo livro publicada pelo autor do método Saaty (SAATY, 2005). De maneira simplificada, apresenta-se os seguintes passos:

1) Para cada critério, deverá ser criada uma matriz quadrada cuja dimensão é igual ao número de alternativas, de modo a compará-las dois a dois, com avaliações entre um (1) a nove (9), que representam valores de intensidade de importância em relação ao critério (o valor “um” equivale ter a mesma importância e o valor “nove” equivale a uma extrema importância de uma alternativa sobre a outra). Na diagonal principal, todos os valores deverão ser iguais a 1 (alternativa é comparada com ela mesmo) e os valores acima da diagonal principal deverão ser o inverso dos valores abaixo da diagonal principal. Por exemplo, o elemento X_{12} equivale a comparação do método 1

em relação ao método 2, e, posteriormente, ao se comparar o método 2 ao método 1, o valor deverá ser o inverso, ou seja, 1 / X_{12}).

	Alternativa 1	Alternativa 2	. . .	Alternativa N
Alternativa 1	1	X_{12}	. . .	X_{1N}
Alternativa 2	1 / X_{12}	1	. . .	X_{2N}
. . .	. . .	. . .	1	X_{3N}
Alternativa N	1 / X_{1N}	1 / X_{2N}	1 / X_{3N}	1

Figura 8: Matriz ilustrativa de comparações dois a dois das alternativas para cada critério.

2) Após a construção das matrizes de comparações pareadas, elas deverão ser normalizadas, sendo que cada elemento da matriz deverá ser divido pela soma dos valores da sua respectiva coluna, sendo que a soma dos elementos de cada coluna seja igual a 1 (um).
3) Para obtenção dos vetores-coluna de prioridades, que irão compor a área descrita como "Priorização local de alternativa em relação aos critérios" na supermatriz ilustrada na Figura 7), deve-se obter a média de cada uma das linhas das matrizes, de forma que cada matriz de comparação dois a dois irá gerar um deverá gerar um vetor-coluna de prioridade.
4) O vetor de pesos dos critérios em relação ao objetivo da decisão multicritério, apresentado na área "Peso dos critérios" na supermatriz ilustrada na Figura 7, deverá representar o quanto cada critério é relevante para a priorização, sendo que a soma dos elementos do vetor de pesos dos critérios deverá ser igual a 1 (um). Por exemplo, caso todos os critérios tenham o mesmo peso na avaliação, o valor de cada elemento do vetor de pesos deverá ser igual a 1 (um) dividido pelo número de critérios;
5) Para as matrizes que representam as influências internas dos grupos, deverá ser criada uma matriz quadrada com dimensão igual ao número de itens do grupo em que existe a dependência. Em geral, é mais comum a existência de dependências no grupo de critérios. Por isso, considera-se nesta explicação que uma matriz é necessária na área "Matriz de influência em cada critério (dependência interna no grupo de critérios)" da Figura 7. Para determinação da matriz de dependências no grupo de critérios, os critérios deverão ser comparados dois a dois, de forma semelhante ao que foi realizado com as alternativas em relação a cada um dos critérios, devendo a matriz ser normalizada ao final também.

6) Após a construção da supermatriz, para obtenção da priorização das alternativas em relação ao objetivo, deve-se, primeiramente, obter o vetor-coluna de pesos dos critérios considerando as dependências internas deste grupo, por meio da multiplicação do vetor-coluna original de pesos dos critérios pelos vetores-linha da matriz de dependência interna do grupo de critérios. Em outras palavras, multiplicação das matrizes "Peso dos critérios" e "Matriz de influência em cada critério (dependência interna no grupo de critérios)" destacadas na Figura 7;
7) Com o novo vetor de pesos de critérios que considera as dependências internas deste grupo, pode-se obter os valores de prioridades das alternativas em relação ao objetivo, com a multiplicação dos vetores-linha da matriz de priorização local de alternativa em relação aos critérios (como definido na Figura 7) pelo vetor-coluna de pesos dos critérios considerando as dependências internas do grupo de critérios, calculado no item 6 anterior. As alternativas que apresentam maiores valores, mostram-se mais adequadas em relação ao objetivo, de acordo com a avaliação realizada em função dos critérios estabelecidos.

4 Aplicações e Resultados

Neste capítulo é apresentada, inicialmente, uma aplicação do processo convencional de determinação de risco para cadeira de rodas motorizadas. Esta aplicação tem por objetivo ilustrar e ressaltar a necessidade da seleção de métodos de determinação de risco que sejam adequados para a avaliação de segurança funcional em relação à interferência eletromagnética. Na análise deste exemplo são aplicadas as técnicas FMEA e FTA, respectivamente, para as avaliações qualitativas e quantitativas, sendo ressaltadas as características destes métodos canônicos.

Posteriormente, são apresentados os resultados da revisão sistemática das técnicas de avaliação de risco, apontando a relevância destas na literatura recente, de acordo com os critérios estabelecidos na seção 3.3. Na sequência, realiza-se a aplicação do procedimento proposto de seleção de técnicas de determinação de risco adequadas para resiliência eletromagnética: utiliza-se o método de apoio multicritério à decisão ANP para avaliação das técnicas de determinação de risco em relação aos critérios gerais e específicos de resiliência eletromagnética, para a aplicação de cadeira de rodas motorizada.

4.1 Aplicação: Sistema de Controle de Cadeira de Rodas Motorizadas

4.1.1 Apresentação do problema

O objetivo desta aplicação é apresentar uma avaliação de risco em relação a resiliência eletromagnética para cadeiras de rodas motorizadas e scooters com velocidade máxima não superior a 15 km/h, destinadas ao uso interno e externo por pessoas com deficiências. Especificamente, será analisada um modelo de cadeira de rodas motorizada de classe B: com controle eletrônico de velocidade, direção eletrônica e controle eletrônico dos freios (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2019).

A escolha da avaliação de risco para esta aplicação - cadeira de rodas motorizada – é motivada por ser um exemplo de interesse em relação à compatibilidade eletromagnética, já que são relatadas diversas ocorrências de perturbações eletromagnéticas neste tipo de equipamento, mesmo sendo obrigatória a execução de testes normativos neste tipo de equipamento. O livro publicado por Keith Armstrong (ARMSTRONG, 2014), já citado anteriormente, compila mais de 500 casos de IEM de diversos níveis de complexidade, sendo que entre os diversos relatos avaliados nesta publicação, destacam-se os casos de incidentes de

interferência eletromagnética relacionados a cadeiras de rodas motorizadas. Uma seleção destes eventos incidentais ou acidentais com cadeiras de rodas devido à interferências eletromagnéticas apresentados no livro é descrita a seguir:

- Item 11 (*Electric wheelchairs erratic due to EMI):* A FDA (*US Food and Drug Agency*) ordenou que os fabricantes de cadeiras de rodas utilizassem blindagens e alertassem usuários sobre os riscos potenciais de interferência, após receber diversos relatos de movimentos não-intencionais de cadeiras de rodas motorizadas, como arranques repentinos quando próximos a transmissores de rádio (COMPLIANCE ENGINEERING, 1994);
- Item 129 (*Seven EMI incidents reported by Dag Björklöf*): Descrição de evento onde uma cadeira de rodas perdeu o controle ao se aproximar do mastro de uma antena de estação de rádio e, eventualmente, o ocupante é ejetado para a rua (BJÖRKLÖF, 1999);
- Item 220 (*Radio waves can cause unintended movements of electric wheelchairs and scooters*): A FDA realizou testes para demonstrar que ondas eletromagnéticas podem causar movimentos não-intencionais em cadeira de rodas motorizadas e scooters, sugerindo algumas precauções aos usuários, como evitar o uso próximo a transmissores ou de realizar modificações no produto, de modo a torná-los menos suscetíveis à interferência (DEPARTMENT OF HEALTH AND HUMAN SERVICES, 1994);
- Item 239 *(Complying with immunity standards might not defend against product liability lawsuits*): Uma empresa foi condenada por colocar no mercado um produto inseguro após uma cadeira de rodas ter sido ativada não-intencionalmente em uma plataforma de metrô e o seu condutor ficar gravemente ferido. A empresa se defendeu ao argumentar que os testes relevantes de compatibilidade haviam sido executados, entretanto, após uma investigação descobriu-se que a interferência havia sido causada por um campo de baixa intensidade na frequência de 1,89 GHz, enquanto o teste executado de suscetibilidade radiada havia sido realizado até 1GHz (GROOT BOERLE, 2002);
- Item 807 (*Medical immunity test standard initiated after wheelchair suffered EMI*): A norma ANSI C63.18 descreve um método recomendado para testar equipamentos médicos, quanto à imunidade contra emissores comuns, como telefones celulares e walkie-talkies. Nota-se que esta norma foi proposta e elaborada após ocorrências de movimentos não-intencionais em cadeira de rodas, quando próximas de viaturas policiais que utilizam a comunicação por rádio (MULLINEAUX, 2005).

Percebe-se com os eventos anteriormente descritos que a avaliação de compatibilidade eletromagnética, ou seja, adequação de níveis de perturbação e, em especial da imunidade ao ambiente eletromagnético para estes equipamentos, é de extrema importância para evitar que acidentes e incidentes possam ocorrer. Deve-se perceber ainda que a preocupação com as interferências eletromagnéticas para sistemas de segurança é crescente devido aos ambientes eletromagnéticos das instalações atuais estarem em constante alteração devido ao uso de "novas tecnologias", como conexões sem-fio, conversores de frequência, etc., o que tende a alterar as características dos campos eletromagnéticos nos mais diversos ambientes, tornando-os mais amplos.

4.1.2 Etapas da Aplicação

A avaliação de risco das cadeiras de rodas motorizadas em relação às interferências eletromagnéticas pode ser descrita nos seguintes itens:

1) Definição de produto e estrutura de controle utilizada: Para se iniciar uma avaliação de risco, o sistema deve ser bem definido. Com este objetivo, optou-se pela realização de um mapa de produto para a descrição da cadeira de rodas motorizada a ser analisada. Como o foco principal é a análise de segurança funcional em relação a interferências eletromagnéticas, será utilizada uma estrutura de controle já aplicada na literatura anteriormente (BOERLE e LEFERINK, 2004);

2) Avaliação dos modos de falha: Para a avaliação dos modos de falha de interesse, será utilizada a Análise de Modos de Falha e Efeitos (FMEA, do inglês, *Failure Mode and Effect Analysis*). A partir da aplicação da FMEA, serão classificados os modos de falha em relação a sua severidade, probabilidade de ocorrência e meios de detecção (conhecido como *SOD – Severity, Occurence and Detection*);

3) Avaliação das falhas: As falhas mais relevantes apontadas pelo FMEA são, então, avaliadas por meio de árvores de falhas (FTA, do inglês, *Fault Tree Analysis*). Nestas árvores são estabelecidas as relações lógicas e hierárquicas entre as diversas possíveis causas, permitindo uma avaliação quantitativa dos eventos no topo das árvores, através da definição da probabilidade dos eventos base.

4.1.3 Mapa de Produto e Estrutura de Controle

Para iniciar a avaliação de risco, é necessário o conhecimento dos equipamentos ou sistemas que serão analisados. Com este objetivo, decidiu-se pela utilização de uma estrutura de controle já aplicada na literatura anteriormente, sendo essa apresentada na Figura 9.

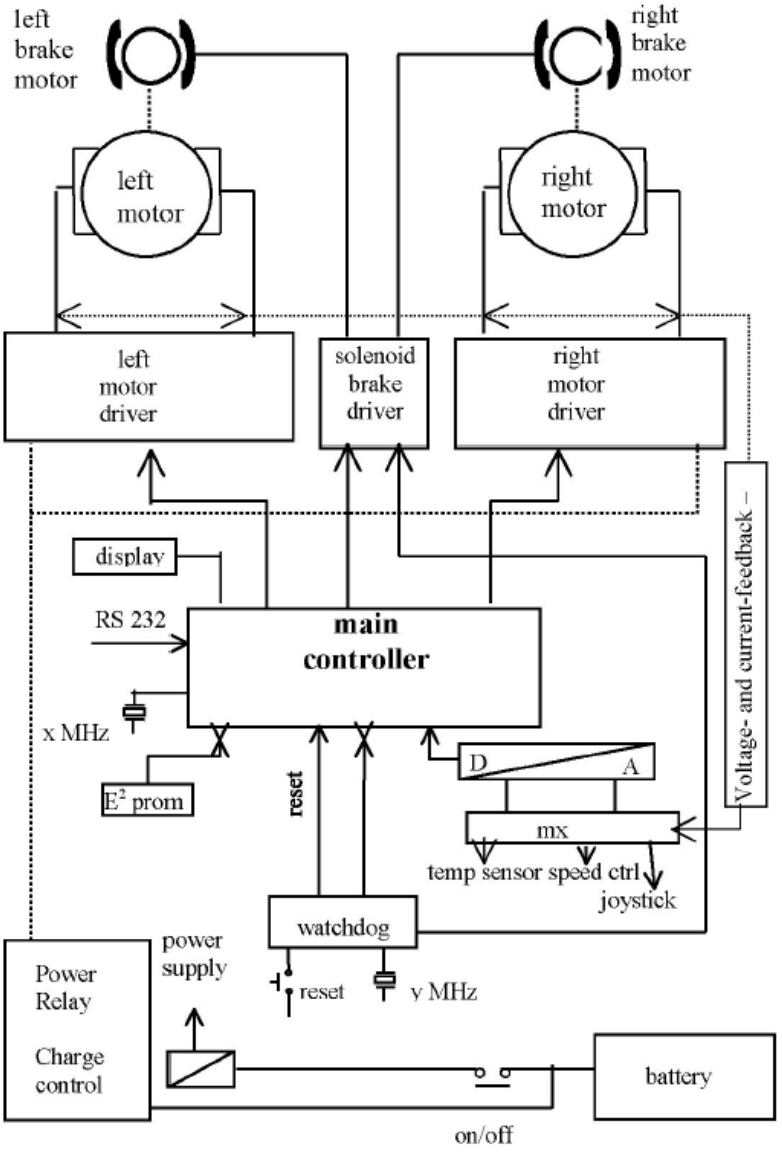


Figura 9: Estrutura de controle de cadeira de rodas motorizada (BOERLE e LEFERINK, 2004).

Um mapa de produto, onde são estabelecidas as relações entre os componentes de um equipamento, com as principais contribuições de cada uma das partes que constituem o produto também foi desenvolvido. Uma imagem do mapa é apresentada no Anexo C e, além disso, a

versão original e seus respectivos detalhamentos podem ser consultados no arquivo em anexo "MapadeProduto_Wheelchair_Final.xlsm"(*https://drive.google.com/file/d/1g1hMb1WScsNzedmNVX6L9spfNX-kLMt8/view?usp=sharing*).

Observa-se que os principais componentes da cadeira de rodas são:

- Controlador: Responsável pela aquisição de sinais do equipamento provenientes dos sensores, pelas atividades de software (gravação e execução em tempo real) e pela geração de sinais aos atuadores;
- Joystick: Dispositivo de entrada que consiste em uma alavanca que gira em uma base e informa seu ângulo ou direção para o dispositivo que está controlando;
- Motores elétricos: Máquina elétrica que converte energia elétrica em energia mecânica, sendo responsável pela propulsão da cadeira de rodas;
- Driver dos motores: Dispositivo que interpreta os comandos do controlador e realiza o acionamento dos motores de acordo com os sinais recebidos;
- Freios elétricos: Elementos responsáveis pela frenagem da cadeira de rodas. Neste caso possuem atuação elétrica (embora muitos modelos possam também possuir uma atuação mecânica em paralelo, com uma chave que informa ao controlador o *by-pass* mecânico realizado pelo usuário);
- Driver dos freios: Dispositivo que interpreta os comandos do controlador e realiza o acionamento dos freios de acordo com os sinais recebidos;
- Sensores de tensão: Leitura dos sinais de tensão nos terminais dos motores e baterias (nível de carga);
- Sensores de corrente: Leitura do sinal de corrente dos motores, para a malha de controle, permitindo o controle de velocidade em malha fechada;
- Bateria: Dispositivo que armazena energia para disponibilizá-la quando a cadeira de rodas motorizada está sendo utilizada;
- Controlador / Carregador da bateria: Responsável pelo controle das atividades de recarga da bateria e proteção dos demais circuitos em caso de falha do sistema de alimentação.

4.1.4 Aplicação da FMEA

A técnica FMEA foi aplicada para avaliação dos modos de falha e seus respectivos efeitos na cadeira de rodas motorizada. Em relação a classificação de severidade, ocorrência e detecção (SOD), utilizou-se uma escala de 1 (um) a 9 (nove), sendo possível todos os valores ímpares

nesta faixa. As definições de cada uma das faixas foram obtidas por meio da adaptação das referências utilizadas em (SYDOR, KRAUSS e KRAUSS, 2017). As escalas são detalhadas nas Tabela 12, Tabela 13 e Tabela 14 (escalas de severidade, ocorrência e detecção adotadas, respectivamente).

Tabela 12 – Escala de severidade adotada.

Avaliação	Severidade	Descrição
9	Catastrófico	Acidente fatal ou perda permanente da saúde e destruição completa do dispositivo.
7	Crítico	Sérios danos corporais e/ou sérios danos ao equipamento.
5	Marginal	Ferimentos de médio grau ao condutor (necessitando atenção médica) e danos ao equipamento.
3	Negligenciável	Pequenos ferimentos no condutor ou sérios danos no dispositivo.
1	Nenhum	Sem efeitos no condutor e equipamento.

Fonte: Adaptação de (SYDOR, KRAUSS e KRAUSS, 2017).

Tabela 13 – Escala de ocorrência adotada.

Avaliação	Ocorrência	Descrição	Frequência
9	Muito Frequente	Sem controles de prevenção. Nova tecnologia; muito pouco conhecimento sobre fatores, efeitos e ruídos.	$> 10^{-1}$
7	Frequente	Sem controles de prevenção. Nova tecnologia, pouco conhecimento de fatores, efeitos e ruídos.	$10^{-1} < F < 10^{-3}$
5	Ocasional	Alguns controles de prevenção. Nova tecnologia comprovada em outras indústrias. Algum conhecimento de fatores, efeitos e ruídos.	$10^{-3} < F < 10^{-5}$
3	Raro	Fortes controles de prevenção. Tecnologia existente com novo aplicativo. Conhecimento de muitos fatores, efeitos e ruídos.	$10^{-5} < F < 10^{-7}$

Avaliação	Ocorrência	Descrição	Frequência
1	Nenhum	Controles de prevenção significativos e comprovados. Projeto implementado anteriormente e com previsibilidade comprovada.	$< 10E^{-7}$
0	Reservado para Item de Linha de Severidade '9' na Seção "Resultados da Ação" do formulário FMEA.	Deve ser usado apenas para itens de segurança (gravidade 9) na área de resultados da ação. Indica que o pensamento da hierarquia de segurança foi aplicado e a ação apropriada levou ao fechamento.	

Fonte: Adaptação de (SYDOR, KRAUSS e KRAUSS, 2017).

Tabela 14 – Escala de detecção adotada.

Avaliação	Ocorrência	Critério	Cobertura
9	Muito remota	Possibilidade muito remota de que o controle evite ou detecte o modo, efeito ou causa da falha.	< 30%
7	Baixa	Baixa chance de que o controle evite ou detecte o modo, efeito ou causa da falha.	30 < > 50%
5	Moderada	Chance moderada de que o controle evite ou detecte o modo, efeito ou causa da falha.	50 < > 70%
3	Alta	Alta chance de que o controle evite ou detecte o modo, efeito ou causa da falha.	70 < > 90%
1	Quase certa	Quase certo de que o controle evitará o modo ou a causa da falha.	> 90%
0	Reservado para Item de Linha de Severidade '9' na Seção "Resultados da Ação" do formulário FMEA.	Deve ser usado apenas para itens de segurança (gravidade 9) na área de resultados da ação. Indica que o pensamento da hierarquia de segurança foi aplicado e a ação apropriada levou ao fechamento.	

Fonte: Adaptação de (SYDOR, KRAUSS e KRAUSS, 2017).

É importante salientar que neste modelo de FMEA, quando a severidade é classificada com valor máxima, ou seja, nove (9), as outras duas avaliações (ocorrência e detecção), não são consideradas, pois isso implica que esses modos de falha deverão ser obrigatoriamente analisados.

A análise de modos de falhas e efeitos é apresentada na Tabela 15. O desenvolvimento da FMEA pode também ser consultado, com os conteúdos auxiliares, no documento em anexo "FMEA_Wheelchair_Final.xlsm" (*https://drive.google.com/file/d/1BPiFn3jbpF9dyr1zBGA0J5aMxQsY7Gk6/view?usp=sharing*).

Tabela 15 – FMEA para cadeira de rodas motorizada em relação às interferências eletromagnéticas.

Linha	Componente / Sistema / Processo / Operações	Função	Potencial Modo de Falha	Potenciais Efeitos das Falhas	Severidade	Causas Potenciais / Mecanismos de Falha	Ocorrência	Prevenção: Projeto Atual / Controle de Processo	Detecção: Projeto Atual / Controle de Processo	Detecção	SOD
1	Controlador	Leitura de sinal A/D do joystick	- Ruptura ou ruído no sinal do joystick - Falha na digitalização do sinal do joystick	Condição degradada: Perda do controle de direção da cadeira, mas com possibilidade de parada.	5	Ambiente Externo Descarga Eletrostática (ESD) Imunidade a campo RF irradiado Imunidade a campo magnético na frequência da rede Ambiente Interno Descarga Eletrostática (ESD) Imunidade a campo RF irradiado Imunidade a campo magnético na frequência da rede Transiente rápido (burst) Surto (surge) Perturbação conduzida Queda de tensão e interrupções curtas Observação: DIferentes níveis de campo.	5	- Uso de cabos blindados - Adoção de elementos passivos, como filtros, para controle de emissão conduzida - Supressor de surtos - Blindagens eletrostáticas	- Detecção de erro - Correção de erros - Proteção de uma sequência	5	555
2		Leitura de sinal A/D proporcional à corrente do motor (controle de velocidade)	- Ruptura ou ruído no sinal do sensor de corrente - Falha na digitalização do sinal do sensor de corrente	Condição degradada: Perda do controle de velocidades da cadeira, mas com possibilidade de parada.	5		5			5	555
3		Leitura de sinal A/D proporcional à tensão	- Ruptura ou ruído no sinal do sensor de tensão - Falha na digitalização do sinal do sensor de tensão	Falso alarme de baixa-tensão na cadeira	3		3			5	335
4		Leitura do sinal A/D proporcional à temperatura do motor	- Ruptura ou ruído no sinal do sensor de temperatura - Falha na digitalização do sinal do sensor de temperatura	Redução de performance da cadeira ou parada desnecessária da cadeira (no caso de leitura errônea de alta temepratura).	5		5			5	555
5		Envio de sinal para os drivers dos motores	- Ruptura ou ruído no sinal de saída - Envio de nível de referência errado.	Condição degradada: Perda do controle de velocidades da cadeira, mas com possibilidade de parada.	5		5			5	555
6		Envio do sinal para o driver dos freios	- Ruptura ou ruído no sinal de saída - Envio de nível de referência errado.	Em movimento: Impossibilidade de frenagem da cadeira. Em parada: Liberação dos freios	9						9__
7		Interpretação de sinais de entrada (software)	Falha na aquisição ou manipulação de variáveis.	Ocasionará erros nas saídas do controlador (veja linha abaixo).	7	- Interferência em porta A/D - Interferência variável ponteiro - Falhas no escrita-interpretação do código-fonte	1	- Gerenciamento de requisitos de software - Uso limitado de interrupções - Uso limitado de variáveis de ponteiro de endereço de memória - Evitar recursão	- Técnicas de programação defensiva - Verificação de sequência	3	713
8		Geração dos sinais de saída (software)	Falha na manipulação de variáveis ou na definição de referência de saída.	Movimentação indesejada da cadeira Impossibilidade de frenagem da cadeira	9	- Interferência em porta A/D - Interferência variável ponteiro - Falhas no escrita-interpretação do código-fonte		- Uso limitado de interrupções - Uso limitado de variáveis de ponteiro de endereço de memória - Evitar recursão	- Técnicas de programação defensiva - Verificação de sequência		9__

Linha	Componente / Sistema / Processo / Operações	Função	Potencial Modo de Falha	Potenciais Efeitos das Falhas	Severidade	Causas Potenciais / Mecanismos de Falha	Ocorrência	Prevenção: Projeto Atual / Controle de Processo	Detecção: Projeto Atual / Controle de Processo	Detecção	SOD
9	Driver dos motores	Leitura dos sinais de controle do microcontrolador	Ruptura ou ruído no sinal do controlador	Perda da movimentação da cadeira ou falhas no acionamento dos motores	5	- Interferência eletromagnética (veja item nas linhas de 1 a 6)	5	Veja item linha 6	Veja item linha 6	5	555
10		Acionamento dos motores (inversor de saída)	Não acionamento dos motores quando demandados por falha no inversor	Impossibilidade de movimentação da cadeira (perigo em ambientes urbanos).	5	Falha no inversor (driver) dos motores	5	- Seleção de drivers adequados a aplicação - Testes que qualificação - Manutenção programada	- Envio de sinal de falha do driver (resumo de falha) para controlador	5	555
11		Idem (Anterior)	Condição degradada devido a chaveamento defeituoso	Falhas no acionamento dos motores	5	Falha no inversor (driver) dos motores	5	- Seleção de drivers adequados a aplicação - Testes que qualificação - Manutenção programada	- Envio de sinal de falha do driver (resumo de falha) para controlador	5	555
12		- Definição de direção de acionamento dos motores - Rotação da cadeira de rodas	Acionamento do movimento inverso ao requisitado.	Movimentação da cadeira em direção oposta	5	Falha no inversor (driver) dos motores	5	- Seleção de drivers adequados a aplicação - Testes que qualificação - Manutenção programada	- Envio de sinal de falha do driver (resumo de falha) para controlador	5	555
13	Driver dos freios solenóides	Interpretação dos sinais de controle do microcontrolador	Ruptura ou ruído no sinal do controlador	Em movimento: Impossibilidade de frenagem da cadeira. Em parada: Liberação dos freios	9	- Interferência eletromagnética (veja item nas linhas de 1 a 6)		Inclusão de trava de rodas manual (quando cadeira está parada).	Veja item linha 6		9__
14		Interpretação dos sinais de controle do watchdog	Ruptura ou ruído no sinal de watchdog (inicialização)	Permissão de acionamento da cadeira em alguma condição de avaria.	5	- Interferência eletromagnética (veja item nas linhas de 1 a 6).	3	Veja item linha 6	Veja item linha 6	3	5__
15		Acionamento dos freios (inversor de saída)	Não acionamento dos freios quando demandados	Em movimento: Impossibilidade de frenagem da cadeira. Em parada: Liberação dos freios	9	Falha no inversor (driver) dos freios		Inclusão de trava de rodas manual (quando cadeira está parada).	Veja item linha 6		9__
16	Motores (Direito e Esquerdo)	Propulsão da cadeira de rodas	Não acionamento devido a falha nos motores	Impossibilidade de movimentação da cadeira (perigo em ambientes urbanos).	5	- Falha sob demanda dos motores	5	Seleção de motores adequados a aplicação (potência, classe térmica, tecnologia).	- Falha é detectada pela ausência de movimento dos motores	3	553
17		Idem (Anterior)	Acionamento do movimento inverso ao requisitado.	Movimentação da cadeira em direção oposta.	5	- Curto-circuito dos enrolamentos do motor (falha do isolamento das bobinas)	5	- Utilização de materias isolantes adequados a classe térmica (B, F, H).	- Sem medidas de detecção preventiva.	7	557
18	Freios	Redução de velocidade e parada da cadeira de rodas	Falha no freio	Impossibilidade de frenagem da cadeira (movimento) ou liberação dos freios (parado).	9	- Desgaste dos freios (Vida últil) - Falha sob demanda dos freios		- Plano de manutenção com verificação e substituição dos freios.	- Deteção durante manutenção programada.		9__
19		Força de frenagem (energia elétrica para energia mecânica)	Ruptura ou ruído da tensão entre driver e freio	Condição degradada: Perda do controle de direção da cadeira, mas com possibilidade de parada.	9	- Interferência Eletromagnética (veja item nas linhas de 1 a 6)		- Uso de cabos blindados	- Detecção de erro - Correção de erros - Proteção de uma sequência		9__

Linha	Componente / Sistema / Processo / Operações	Função	Potencial Modo de Falha	Potenciais Efeitos das Falhas	Severidade	Causas Potenciais / Mecanismos de Falha	Ocorrência	Prevenção: Projeto Atual / Controle de Processo	Detecção: Projeto Atual / Controle de Processo	Detecção	SOD
20	Bateria	Acumular energia durante recarga	Impossibilidade de armazenamento de energia (vida útil ou falha)	Impossibilidade de movimentação da cadeira (perigo em ambientes urbanos).	3	Vida útil da bateria.	3	- Plano de manutenção da cadeira, includindo substituição d abateria	- Indicação de nível de carga em painel	3	333
21		Disponilizar energia durante uso da cadeira	Ausência ou baixo nível de tensão para motor (falha sob demanda)	Impossibilidade de movimentação da cadeira (perigo em ambientes urbanos).	3	Falha sob demanda da bateria.	3	- Plano de manutenção da cadeira, includindo substituição d abateria	- Indicação de nível de carga em painel	3	333
22		Idem (Anterior)	Ausência ou baixo nível de tensão para freio (falha sob demanda)	Impossibilidade de movimentação da cadeira (perigo em ambientes urbanos).	3	Falha sob demanda da bateria.	3	- Plano de manutenção da cadeira, includindo substituição d abateria - Falha segura do freio: Freio é normalmente fechado (acionado em falta de energia).	- Indicação de nível de carga em painel.	3	333
23	Módulo de controle da bateria	Carregamento da bateria	Falha no carregador	Impossibilidade de recarga da cadeira Impossibilidade de movimentação da cadeira após descarga	3	Falha do carregador	3	- Aprovação de carregador nos testes de validação - Em ocorrência, deverá ser substituído.	- Detecção é perceptível ao consumidor	7	337
24		Proteção da conexão entre bateria e os drivers dos motores (relé / disjuntor)	Desligamento dos motores (relé)	Impossibilidade de movimentação da cadeira (perigo em ambientes urbanos).	3	- Sobrecorrente devido a carga (por exemplo, motor com rotor travado). - Falha de isolamento (curto)	3	- Correto dimensionamento da proteção para condição de sobrecarga - Utilização de isolamentos adequados	- Detecção é perceptível ao consumidor	7	337
25	Sensor de corrente dos motores	Detecção de sinal de corrente	Falha no transdutor de corrente	Condição degradada: Perda do controle de velocidades da cadeira, mas com possibilidade de parada.	5	Falha de sensor de corrente	1	- Redundância de sensores	Controlador deve detectar ausência de sinal do sensor de corrente e apontar falha. Para interferência, se nível de sinal está dentro do range, não há detecção.	1	511
26		Idem (Anterior)	Interferência no transdutor (leitura por campo)	Controle de velocidade será afetado.	3	- Interferência Eletromagnética (Veja item nas linhas de 1 a 6)	1	- Redundância de sensores	- Programação defensiva: Verificação da faixa dos valores de todas as variáveis - Detecção de erro	1	311
27		Geração de sinal proporcional a corrente medida ao controlador	Falha no transdutor de corrente	Condição degradada: Perda do controle de velocidades da cadeira, mas com possibilidade de parada.	5	Mecanismos de falha do sensor de corrente	1	- Redundância de sensores	- Programação defensiva: Verificação da faixa dos valores de todas as variáveis - Detecção de erro	1	511
28	Sensor de tensão	Detecção de sinal de tensão	Falha no transdutor de tensão	Falso alarme de baixa-tensão na cadeira	3	Mecanismo de falha do sensor de tensão	5	- Sem medidas preventivas, necessitando a substituição do transdutor	- Programação defensiva: Verificação da faixa dos valores de todas as variáveis - Detecção de erro	3	353
29		Geração de sinal proporcional a tensão medida	Ruptura ou ruído no sinal do sensor de tensão	Falso alarme de baixa-tensão na cadeira	3	- Interferência Eletromagnética (Veja item nas linhas de 1 a 6) - Falha na conversão A/D	5	- Sem medidas preventivas, necessitando a substituição do transdutor	- Programação defensiva: Verificação da faixa dos valores de todas as variáveis - Detecção de erro	3	353
30	Joystick	Controle de direção da cadeira	- Ruptura ou ruído no sinal do joystick - Falha na digitalização do sinal do joystick	Condição degradada: Perda do controle de direção da cadeira, mas com possibilidade de parada.	5	- Interferência eletromagnética (veja item nas linhas de 1 a 6) - Falha dos componentes do joystick	5	- Uso de cabos blindados	- Detecção de erro - Correção de erros - Proteção de uma sequência	3	553

Algumas importantes considerações devem ser ressaltadas a após a realização do FMEA:

1. Observa-se que os mecanismos de modo de falha e suas consequências são distintos de acordo com o ambiente em que a cadeira de rodas motorizada é utilizada. Por exemplo, as perturbações conduzidas relacionadas à rede elétrica apenas ocorrerão quando o equipamento se encontrar em carregamento, situação geralmente associada a condições em que a cadeira se encontra em ambiente interno, em repouso. Portanto, para as análises posteriores, serão considerados os seguintes ambientes:
    a. Ambiente Interno (Indoor): Trata-se de ambiente residencial ou de escritório. Neste ambiente existe a possibilidade de realização do carregamento da bateria, situação em que podem ocorrer perturbações eletromagnéticas conduzidos e irradiadas;
    b. Ambiente Externo (Outdoor): Trata-se de ambiente comercial ou industrial. Neste caso, a condição de carregamento não é prevista, e são considerados apenas os modos de falhas associados as perturbações eletromagnéticas irradiados. Observa-se que, como premissa, são desconsiderados os efeitos do acionamento da bateria, considerando que medidas preventivas foram adotadas para evitá-los.

2. Os principais ensaios ou testes eletromagnéticos levantados durante a execução do FMEA foram:
    a. Imunidade à descarga eletrostática (ESD);
    b. Imunidade à campo de RF irradiado;
    c. Imunidade ao campo magnético na frequência da rede;
    d. Imunidade a transiente rápido (*burst*);
    e. Imunidade à surto (*surge*);
    f. Imunidade à perturbação conduzida induzidos causados por campos eletromagnéticos;
    g. Imunidade a quedas de tensão e interrupções curtas.

3. Os níveis para cada um dos testes de emissão e imunidade eletromagnética listados no item (2) acima são apresentados na Tabela 16. Essa definição está de acordo com os valores utilizados na ABNT NBR ISO 7176-21 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2019), norma que determina requisitos e métodos de ensaio para compatibilidade eletromagnética de cadeira de rodas motorizadas e scooters, assim

como suas respectivas referências com base em normas internacionais de CEM. Observa-se que, além dos testes previstos pela execução do FMEA, a ABNT NBR ISO 7176-21 define testes adicionais a serem executados neste tipo de dispositivo.

Tabela 16 – Ensaios de compatibilidade eletromagnética e respectivos níveis com base na ABNT NBR ISO 7176-21 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2019).

Propagação	**Ensaio**	**Nível Interno**	**Nível Externo**
-	Descarga Eletrostática (ESD)	± 2 kV, ± 4 kV e ± 6 kV para descargas de contato ± 2 kV, ± 4 kV e ± 8 kV para descargas pelo ar IEC 61000-4-2 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2008)	
Irradiados	Campo de RF irradiado	3 V/m, de 80 MHz a 1,0 GHz IEC 61000-4-3 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2020)	
	Campo magnético na frequência da rede	30 A/m, 50 Hz e 60 Hz (Nível 4) IEC 61000-4-8 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2009)	
Conduzidos	Transiente rápido (*burst*)	Power: 1kV – 100 kHz Signal: 0.5kV – 100 kHz (Nível 2) IEC 61000-4-4 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2012)	Não aplicável para essa avaliação
	Surto (*surge*) (5 pulsos "+" e 5 pulsos "-")	1 kV (nível 3) IEC 61000-4-5 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2014)	

Propagação	Ensaio	Nível Interno	Nível Externo
	Perturbação conduzida	3*Uo - 150kHz – 80 MHz (Nível 2) IEC 61000-4-6 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2013)	
	Quedas de tensão e interrupções curtas	0% meio ciclo, 0% um ciclo, 70% por 30 ciclos (Classe 2) IEC 61000-4-11 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2020)	Não aplicável para essa avaliação

4. Cada um dos modos de falha é avaliado em relação a sua severidade e ocorrência, de modo que seja possível realizar uma priorização das falhas que apresentem um maior risco (severidade x ocorrência). No FMEA realizado, observa-se dois grandes grupos de interesse:
    a. Os modos de falha com severidade classificada com nove (9);
    b. Os modos de falha com severidade classificada com cinco (5) e ocorrência com cinco (5).

Estes modos de falha deverão, portanto, ser avaliados nas análises posteriores. É apresentado na Tabela 17 o número de modos de falha de acordo com a sua classificação de severidade e ocorrência.

Tabela 17 – Relação de números de modos de falha de acordo com sua classificação de severidade (linhas) e ocorrência (colunas).

Severidade / Ocorrência	**1**	**3**	**5**	**7**	**9**
9	6				
7	*1*	0	0	0	0
5	*2*	0	11	0	0
3	1	6	2	0	0
1	0	0	0	0	0

5. Percebe-se que existem dois grandes grupos dentro dos efeitos dos modos de falha de interesse, que foram levantados no item anterior (4). Eles podem ser descritos como:
    a. Impossibilidade de frenagem;
    b. Acionamento não-intencional dos motores.

Esses dois grupos serão exatamente os eventos-topo das árvores de falha a serem desenvolvidas na aplicação do FTA.

4.1.5 Aplicação FTA

O objetivo desta análise é definir as taxas de falhas para os dois grandes grupos de efeitos indesejados avaliados pela FMEA, sendo eles:

- Impossibilidade de frenagem;
- Acionamento não-intencional dos motores.

Deve-se lembrar, entretanto, que as causas dos efeitos a serem avaliados, assim como suas frequências de ocorrência, são diferentes, de acordo com os ambientes a serem avaliados, sendo considerados, como já exposto anteriormente, os ambientes internos (indoor) e externos (outdoor). Deste modo, são definidos quatro eventos-topo para as árvores de falhas:

- Impossibilidade de frenagem (Indoor);
- Acionamento não-intencional dos motores (Indoor);
- Impossibilidade de frenagem (Outdoor);
- Acionamento não-intencional dos motores (Outdoor).

Para a definição das taxas de falha dos eventos no topo das árvores de falha, deve-se definir as taxas de falha dos eventos na base das árvores. Por esse motivo, o conjunto de premissas adotadas durante o processo de definição das FTA é apresentado a seguir:

1. Taxa de falha para eventos sistemáticos: As falhas por interferência eletromagnética, assim como aquelas ocasionadas por software, são conhecidas como falhas sistemáticas. De maneira geral, não se define taxas de falha para esse tipo de evento, como é realizado para as falhas de hardware (também denominadas de falhas aleatórias ou de causa atribuível). Entretanto, neste trabalho, como se deseja realizar uma aplicação com avaliação numérica, foram consideradas as seguintes premissas:
    a. Taxas de falhas devido à interferência eletromagnética em ambientes internos (consequências de menor severidade): 10^{-6} [h^{-1}], que representa o limite superior do nível de integridade de segurança (SIL – *Safety Integrity Level*) para funções de segurança de nível 2 (SIL2);
    b. Taxa de falha devido à interferência eletromagnética em ambientes externos (consequências de maior severidade): 10^{-7} [h^{-1}], que representa o limite

superior do nível de integridade de segurança (SIL – *Safety Integrity Level*) para funções de segurança de nível 3 (SIL3);

c. Taxa de falha ocasionada por falhas de software (igual em todos os ambientes): 10^{-7} [h^{-1}], que representa o limite superior do nível de integridade de segurança (SIL – *Safety Integrity Level*) para funções de segurança de nível 3 (SIL3).

Estes valores foram obtidos na norma IEC 61508 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010), já descrita neste trabalho, e que apresenta as faixas de taxas de falhas a serem atingidas por cada uma das funções de segurança operando em modo de alta demanda ou modo contínuo para cada um dos níveis de integridade de segurança, sendo reproduzida na Tabela 18. Observa-se que a escolha dos níveis de integridade de segurança está alinhada com as severidades das consequências dos modos de falha analisados para as respectivas causas.

Tabela 18 – Taxas de falhas para funções de segurança de acordo com nível de integridade esperado para operação contínua (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2010).

Nível de Integridade de Segurança (SIL)	**Frequência média de falha de função de segurança [h^{-1}] (PFH)**
4	$\geq 10^{-9}$ e $< 10^{-8}$
3	$\geq 10^{-8}$ e $< 10^{-7}$
2	$\geq 10^{-7}$ e $< 10^{-6}$
1	$\geq 10^{-6}$ e $< 10^{-5}$

2. Taxa de falha dos componentes principais: Inicialmente, procurou-se por catálogos de fabricantes de componentes específicos para a aplicação de cadeira de rodas motorizadas. Entretanto, nenhum dos fornecedores avaliados apresentavam dados como taxa de falha ou MTTF (do inglês, *Mean Time To Failure*). Desta forma, iniciou-se uma busca por bancos de dados da indústria que poderiam ser utilizados como referência, por exemplo, o OREDA (*Offshore Reliability Data Handbook*) (DNV, 2015). Decidiu-se pela utilização das taxas de falhas apontados no guia IEEE 500 (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 1984), referência utilizada no setor nuclear, que, embora não seja mais uma norma ativa,

apresenta dados históricos de diversos equipamentos elétricos. Abaixo são apresentados os valores assumidos para as taxas de falhas, obtidas em (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, 1984):

a. Controlador: 1,24 falhas / 10^6 horas;
b. Driver (Freios e Motor): 3 falhas / 10^6 horas;
c. Motores: 37 falhas / 10^6 horas;
d. Freios (Assumido igual à dos motores por falta de dados na literatura e por dispositivo ser geralmente acoplado no motor): 37 falhas / 10^6 horas;
e. Joystick: Assumido o valor de 1 falha / 10^5 horas.

Para a criação das árvores de falhas e consecutivo cálculo das taxas de falhas dos eventos no topo das árvores foi utilizado o software *TopEvent FTA* (RELIOTECH, 2020), que possui uma versão gratuita com algumas limitações para implementação, mas suficientes para a realização desta aplicação. O período de missão considerado foi de 1 ano, devido à grande parte dos fabricantes das cadeiras de rodas motorizadas garantirem esse tempo para utilização sem reparos ou manutenção programada.

4.1.5.1 Cenário 1: Impossibilidade de Frenagem (Outdoor)

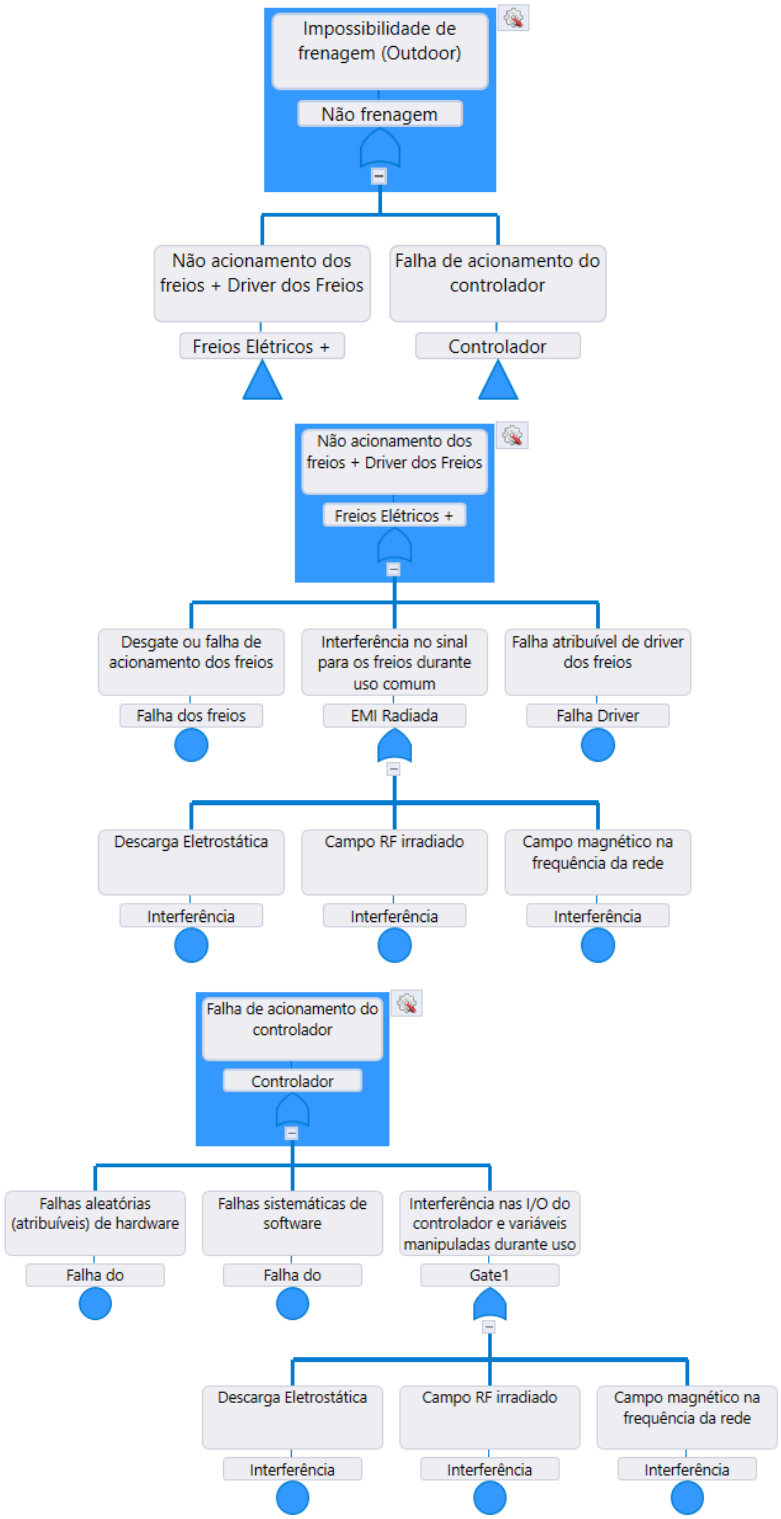
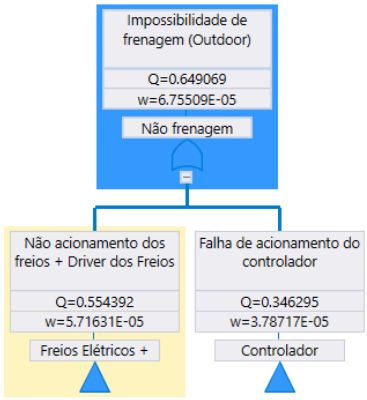


Figura 10: Árvores de falha para cenário 1 – Impossibilidade de frenagem (Outdoor). Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).



	Minimal Cut Set	Order	Unavailability	Contribution
1	Falha dos freios	1	0.276837	0.426513
2	Interferência Radiada 1	1	0.0838727	0.12922
3	Interferência Radiada 2	1	0.0838727	0.12922
4	Interferência Radiada 3	1	0.0838727	0.12922
5	Falha do Controlador 2	1	0.0838727	0.12922
6	Falha Driver	1	0.0259377	0.0399614
7	Falha do Controlador 1	1	0.0108036	0.0166448

Figura 11: Resultados da análise para cenário 1 – Impossibilidade de frenagem (Outdoor).
Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).

4.1.5.2 Cenário 2: Acionamento Não-Intencional dos Motores (Outdoor)

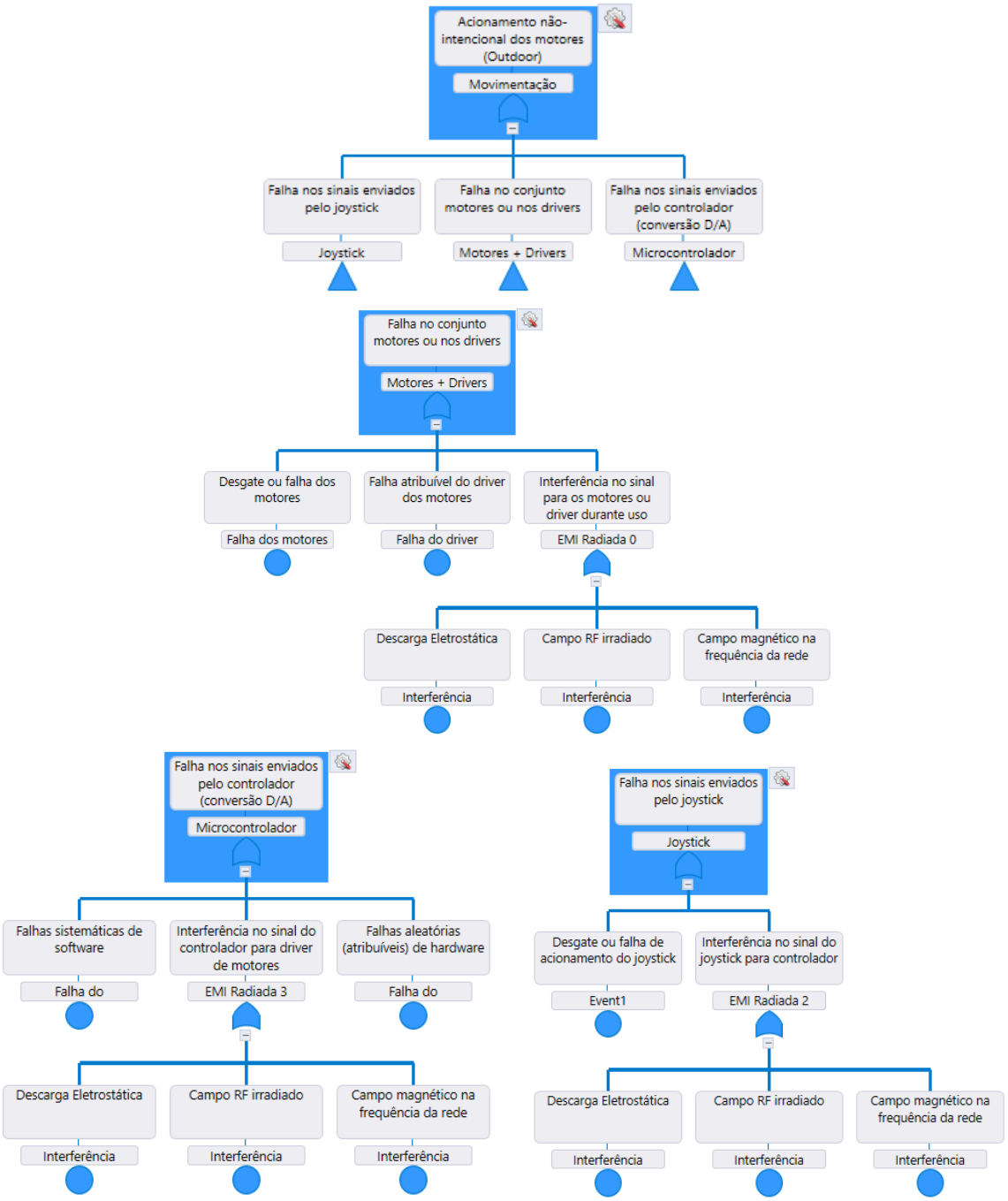
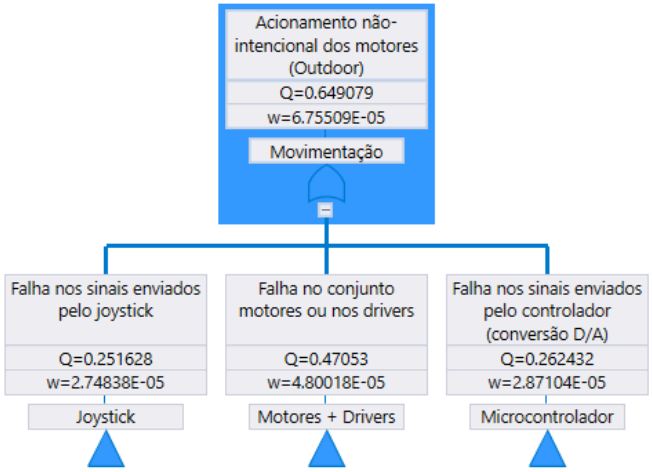


Figura 12: Árvores de falha para cenário 2 – Acionamento não-intencional dos motores (Outdoor). Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).



	Minimal Cut Set	Order	Unavailability	Contribution
1	Falha dos motores	1	0.276837	0.426507
2	Event1	1	0.0838727	0.129218
3	Interferência Radiada 1	1	0.0838727	0.129218
4	Interferência Radiada 2	1	0.0838727	0.129218
5	Falha do Controlador 1	1	0.0838727	0.129218
6	Falha do driver	1	0.0259377	0.0399608
7	Falha do Controlador 2	1	0.0108036	0.0166445
8	Interferência Radiada 3	1	1E-05	1.54064E-05

Figura 13: Resultados da análise para cenário 2 – Acionamento não-intencional dos motores (Outdoor). Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).

4.1.5.3 Cenário 3: Impossibilidade de Frenagem (Indoor)

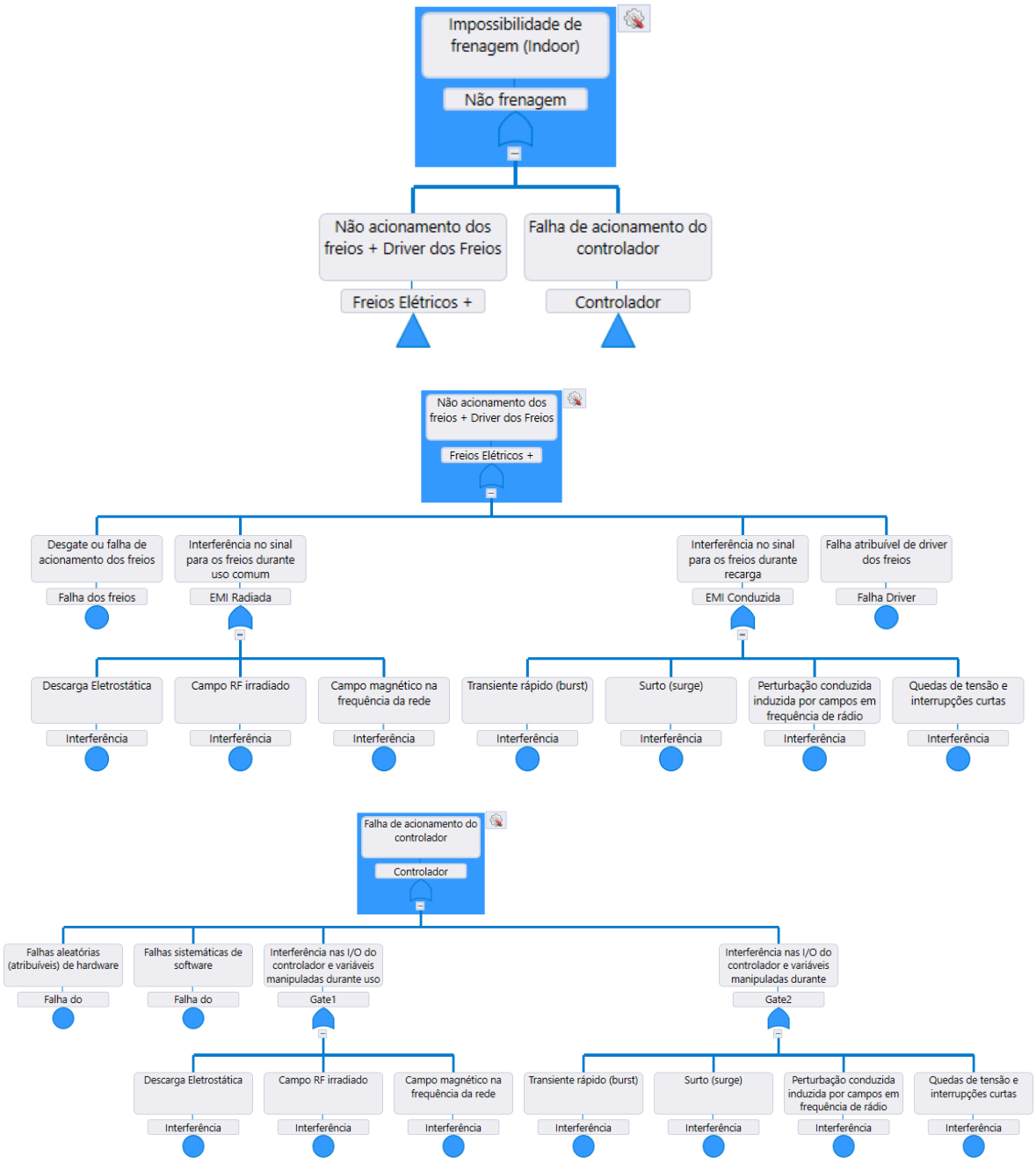
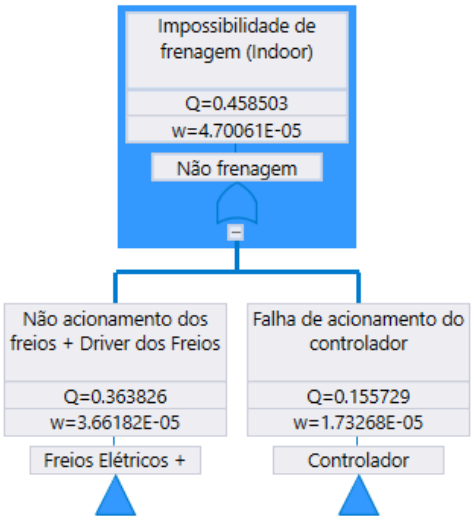


Figura 14: Árvores de falha para cenário 3 – Impossibilidade de frenagem (Indoor). Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).



1 of 1(11 items)

	Minimal Cut Set	Order	Unavailability	Contribution
1	Falha dos freios	1	0.276837	0.603784
2	Falha do Controlador 2	1	0.0838727	0.182927
3	Falha Driver	1	0.0259377	0.0565704
4	Falha do Controlador 1	1	0.0108036	0.0235628
5	Interferência Radiada 1	1	0.00872174	0.0190222
6	Interferência Radiada 2	1	0.00872174	0.0190222
7	Interferência Radiada 3	1	0.00872174	0.0190222
8	Interferência Conduzida 1	1	0.00872174	0.0190222
9	Interferência Conduzida 2	1	0.00872174	0.0190222

Figura 15: Resultados da análise para cenário 3 – Impossibilidade de frenagem (Indoor).
Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).

4.1.5.4 Cenário 4: Acionamento Não-Intencional dos Motores (Indoor)

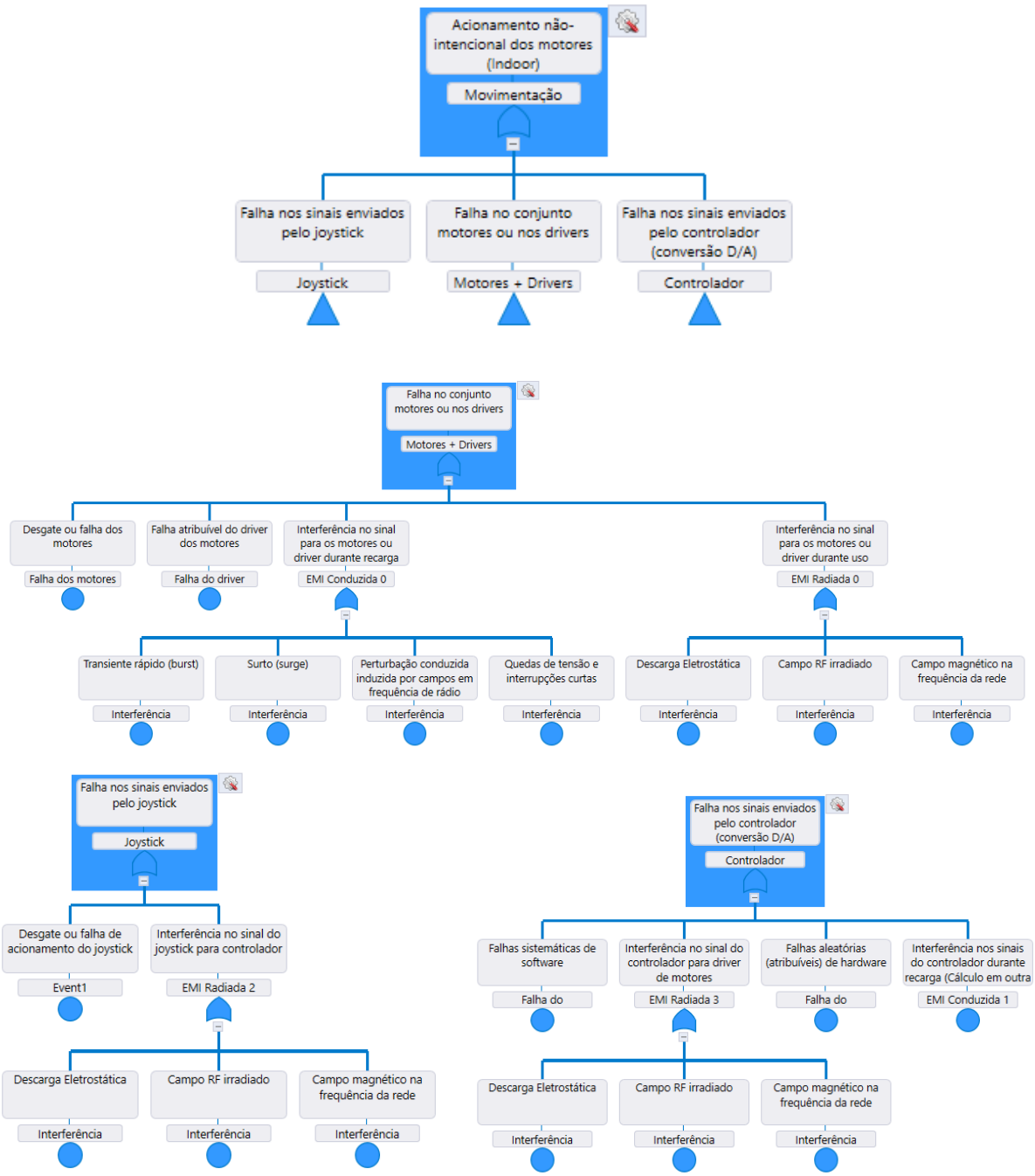
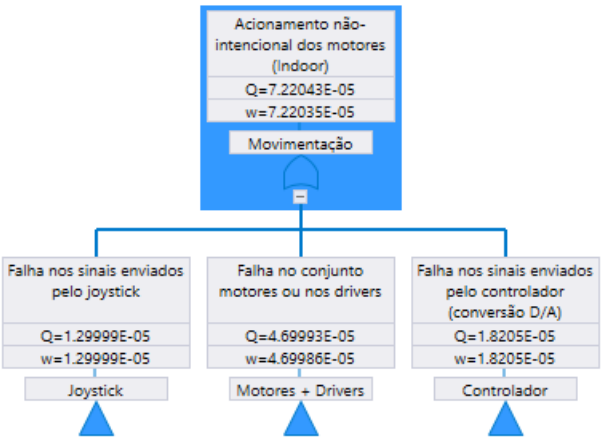


Figura 16: Árvores de falha para cenário 4 – Acionamento não-intencional dos motores (Indoor). Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).



	Minimal Cut Set	Order	Unavailability	Contribution
1	Falha dos motores	1	3.69993E-05	0.512425
2	Event1	1	9.99995E-06	0.138495
3	Falha do Controlador 1	1	9.99995E-06	0.138495
4	EMI Conduzida 1	1	3.9651E-06	0.054915
5	Falha do driver	1	3E-06	0.0415487
6	Falha do Controlador 2	1	1.24E-06	0.0171735
7	Interferência Radiada 1	1	9.99999E-07	0.0138496

Figura 17: Resultados da análise para cenário 4 – Acionamento não-intencional dos motores (Indoor). Fonte: Obtido no software *TopEvent FTA* (RELIOTECH, 2020).

4.1.5.5 Resumo da Aplicação do FTA

Em relação aos conteúdos apresentados nas subseções anteriores, os principais resultados são apresentados de forma sucinta na Tabela 19.

Tabela 19 – Resumo dos resultados das taxas de falha dos eventos nos topos das árvores de falha.

Evento Topo	**Taxa de falha (Falha / 10^6 Horas)**
Impossibilidade de frenagem (Outdoor)	67,55
Acionamento não-intencional dos motores (Outdoor)	67,55
Impossibilidade de frenagem (Indoor)	47

Evento Topo	Taxa de falha (Falha / 10^6 Horas)
Acionamento não-intencional dos motores (Indoor)	77,20

Pode-se observar que, nos cenários relacionados ao ambiente externos (outdoor), devido a consideração de que os eventos de falha devido às perturbações eletromagnéticas eram 10 vezes maiores que aos valores adotados para o caso de ambientes internos, as taxas de falhas dos eventos "Impossibilidade de frenagem (Outdoor)" e "Acionamento não-intencional dos motores (Outdoor)" são semelhantes (diferença a partir da quarta casa decimal), devido ao domínio das perturbações eletromagnéticas diante das taxas de falhas de hardware (dos componentes). Portanto, embora no ambiente externo seja considerado apenas as perturbações irradiadas, tem-se uma maior contribuição das perturbações eletromagnéticas na disponibilidade do evento-topo.

No ambiente interno, por sua vez, foram consideradas as perturbações conduzidas e irradiadas, observando-se que a taxa de falha para o evento-topo "Impossibilidade de frenagem (Indoor)" é menor que "Acionamento não-intencional dos motores (Indoor)" pois, no segundo caso, é maior a quantidade de itens do equipamento que possuem modos de falha que podem ocasionar tal efeito.

4.2 Discussão da Avaliação de Risco com Métodos Tradicionais: Aplicação da Cadeira de Rodas

Durante o desenvolvimento da aplicação da cadeira de rodas e utilização das técnicas de avaliação de risco foram encontradas algumas dificuldades que devem ser ressaltadas:

- Poucos dados de fornecedores sobre taxas de falhas de componentes, tendo que ser utilizado dados de guias de áreas não diretamente relacionadas e que podem ter uma valores distintos aos componentes reais utilizados em cadeiras de rodas motorizadas. Além disso, os valores adotados estão sujeitos às variações de acordo com a evolução tecnológica dos componentes, dispositivos e acessórios utilizados como referência;
- A consideração de falhas sistemáticas nas avaliações numéricas mostra-se problemática, uma vez que suas causas não são facilmente atribuíveis e não pode ser representada por uma taxa de falha, mas tratada no ciclo de vida de segurança, que deve incluir procedimentos para evitar que elas ocorram.

Como melhoria para essa aplicação, recomenda-se, por exemplo, a utilização de taxas de componentes aplicados na indústria de cadeiras de rodas motorizadas.

Observa-se que, uma das dificuldades apontadas consiste no fato da busca de avaliação de ocorrências de falhas sistemáticas, onde abordagens numéricas utilizando os métodos tradicionais de avaliação de risco não são ideais. Deste modo, este exemplo ilustrativo, com a aplicação de métodos tradicionais de determinação de risco, serve para enfatizar a necessidade da busca de métodos de determinação de risco mais adequados a esse propósito, um dos objetivos deste trabalho.

A seguir são apresentados os resultados da revisão sistemática das técnicas e, posteriormente, a aplicação da metodologia de seleção de técnicas de determinação de risco apropriadas para a aplicação.

4.3 Aplicação do Procedimento Proposto de Seleção de Técnicas de Determinação de Risco Adequadas para Resiliência Eletromagnética

Para ilustrar o uso do método descrito na seção 3.1, sua aplicação é apresentada nesta seção. Três métodos de determinação de risco são comparados com os critérios definidos, considerando-se as questões de resiliência eletromagnética, de acordo com o quadro estabelecido na Figura 6.

4.3.1 Revisão Sistemática das Técnicas de Determinação de Risco

A revisão sistemática de técnicas de determinação risco com os critérios estabelecidos na seção 3.3 foi realizada para todas as técnicas descritas na Tabela 20. As técnicas mencionadas estão classificadas em relação a sua aplicabilidade a cada uma das etapas da determinação de risco (identificação, análise e avaliação). Assim, a aplicabilidade às etapas de determinação de risco é classificada como “Aplicável” (A) ou “Não Aplicável” (NA).

Tabela 20 – Métodos avaliados na revisão sistemática.

Técnicas	Identificação de Risco	Análise de risco	Avaliação de risco
Absolute Probability Judgment (APJ) / Direct numerical estimation	A	NA	NA
Accident Hazard Index (AHI)	A	A	A
Accident Sequences Precursor (ASP)	NA	A	A
AcciMap Approach	A	A	NA
Action Error Analysis (AEA)	A	A	A
ALARP, ALARA ou SFAIRP	NA*	NA*	A*
Anticipatory Failure Determination (AFD)	A	A	NA
Barrier and operational risk analysis (BORA)	NA	A	NA
Bayesian statistics or Bayesian Networks / Statistics / Nets / Model	NA*	A*	NA*
Bow-tie analysis/method	NA*	A*	A*
Brainstorming	A*	NA*	NA*
Business impact analysis / assessment (BIA)	A*	A*	A*
Causal Mapping or Causal Map	A*	A*	NA*
Cause-and-consequence analysis (CCA) or diagrams	A*	A*	A*
Cause-and-effect analysis / Cause-effect diagram / Ishikawa Diagram / Fish-bone diagram / Herringbone diagram	A*	A*	NA*
Cindynic Approach	A*	NA*	NA*
Clinical Risk and Error Analysis (CREA)	A	A	A
Cognitive Reliability and Error Analysis Method (CREAM)	A	A	NA
Common cause failure (CCF) analysis	A*	A*	NA*
Concept Hazard Analysis (CHA)	A	NA	NA
Concept Safety Review (CSR)	A	NA	NA
Cost-benefit analysis	A*	A*	A*
Cost-Of-Risk Analysis (CORA)	NA	A	A
Cross Impact Analysis	NA*	A*	NA*
Decision matrix risk-assessment (DMRA)	NA	A	A
Decision tree analysis	NA*	A*	A*
Delphi / Estimate-Talk-Estimate or ETE	A*	NA*	NA*
Event tree analysis (ETA)	A*	A*	A*
External Events Analysis	A	A	NA
Facilitated Risk Analysis and Assessment Process (FRAAP) / Facilitated risk analysis process (FRAP)	A	A	NA
Failure mode effect analysis (FMEA)	A*	NA*	A*

Técnicas	Identificação de Risco	Análise de risco	Avaliação de risco
Failure mode effect and critically analysis (FMECA)	A*	A*	A*
Fault/Functional Hazard Analysis (FHA)	A	A	A
Fault insertion testing / Fault Injection testing	NA	A	NA
Fault tree analysis (FTA)	A*	A*	A*
Fine Kinney method	NA	A	A
FN curves	A*	A*	A*
Functional Resonance Analysis Method (FRAM)	A	A	NA
Game Theory	A*	A*	A*
Goal-Oriented Failure Analysis (GOFA)	A	A	A
Hazard Analyzis and Critical Control Points (HACCP)	A*	A*	A*
Hazard and Operability studies (HAZOP)	A*	A*	A*
Hazard Identification and Ranking (HIRA)	A	A	A
Hazardous Scenario Analysis (HAZSCAN) / Hazard identification (HAZID)	A	A	NA
Hierarchical Task Analysis (HTA) Hierarchical Task Network (HTN)	A	NA	NA
Human Error Assessment and Reduction Technique (HEART)	A*	A*	A*
Human Factor Event Analysis (HFEA)	A*	A*	A*
Human Factors Analysis and Classification System (HFACS)	A*	A*	A*
Incident Review / Incident Report	A	NA	NA
Layer of protection analysis (LOPA) / Barrier Analysis	A*	A*	NA*
Markov analysis	A*	A*	NA*
Master Logic Diagram	A	NA	NA
Maximum Credible Accident Analysis (MCAA)	A	NA	NA
Method Organised Systematic Analysis of Risk (MOSAR - Méthode Organisée et Systémique d'Analyse de Risques)	A	A	NA
Monte Carlo Simulation	NA*	NA*	A*
Normal Accident Theory (NAT)	A	NA	NA
Nuclear Action Reliability Assessment (NARA)	A	A	A
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)	A	A	A
Optimal Risk Assessment (ORA)	A	A	A
Petri Nets (or Time Petri Nets)	A	A	NA
Predictive, Epistemic Approach (PEA)	A	A	A

Técnicas	Identificação de Risco	Análise de risco	Avaliação de risco
Preliminary Hazard Analysis (PHA) / Primary hazard analysis	A*	NA*	NA*
Rapid Risk Analysis Based Design (RRABD) / Rapid Risk Assessment (RRA)	A	NA	NA
Reliability block diagrams (RBD) / Dependence diagram (DD)	NA*	A*	A*
Reliability centred maintenance	A*	A*	A*
Risk and Vulnerability analysis (RVA)	A	A	NA
Risk indices / Risk Level Indicators (RLI) / Key Risk Indicators (KRIs)	NA*	A*	A*
Risk-based Maintenance (RBM)	NA	A	NA
Scenario analysis / Scenario-based design	A*	A*	A*
SEQHAZ Hazard Mapping	A	A	A
Sequentially Timed Event Plotting (STEP)	A	A	NA
Sneak circuit analysis / Sneak Analysis	A*	NA*	NA*
Structure « What if? » (SWIFT)	A*	A*	A*
Structured or semi-structured interviews	A*	NA*	NA*
Success Likelihood Index Methodology / Success Likelihood Index Method (SLIM)	NA*	A*	A*
Swiss Cheese Model (SCM) - SCM-based model - Reason Model (the ATSB accident investigation model)	A	A	NA
System Hazard Identification, Prediction and Prevention (SHIPP)	A*	A*	A*
Systematic Human Error Reduction and Prediction Analysis (SHERPA)	A*	A*	A*
Systems-Theoretic Accident Model and Processes (STAMP = CAST + STPA)	A	A	A
Technique for Human Error Rate Prediction (THERP)	A	A	A
Technique for Human Event Analysis (ATHEANA)	A	A	A
Toxicological risk assessment / Toxicity assessment (TA)	A*	A*	A*
Value at Risk (VaR) / Conditional Value at Risk (CVaR) (CoVaR)	NA*	A*	A*
Weighted risk analysis (WRA)	A	A	A
Worst-case analysis and Worst-case testing	A	NA	NA

Fonte: Itens com asterisco (*) estão de acordo com a norma internacional EIC/ISO 31010 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019).

Foram analisados, ao total, 1459 arquivos técnicos (artigos acadêmicos ou livros) que atendiam os critérios estabelecidos com a aplicação ou análise das 86 técnicas de determinação de risco descritas acima, propostas a partir da revisão bibliográfica deste trabalho.

Inicialmente, avaliou-se, como descrito no item 8 da seção 3.3, o número de artigos incluídos para cada umas das técnicas, podendo ser observado na Figura 18. Observa-se que estão incluídas na figura apenas as técnicas que apresentaram ao menos um artigo dentro dos critérios estabelecidos, embora todas os métodos tenham sido avaliados pela revisão sistemática.

De maneira similar, avaliou-se, como descrito no item 8 da seção 3.3, o número total de citações para cada uma das técnicas, sendo representados os quantitativos na Figura 19. A partir dos valores descritos acima, pode-se realizar o cálculo do A-Fator, C-Fator e R-Fator, sendo este último, apresentado graficamente na Figura 20.

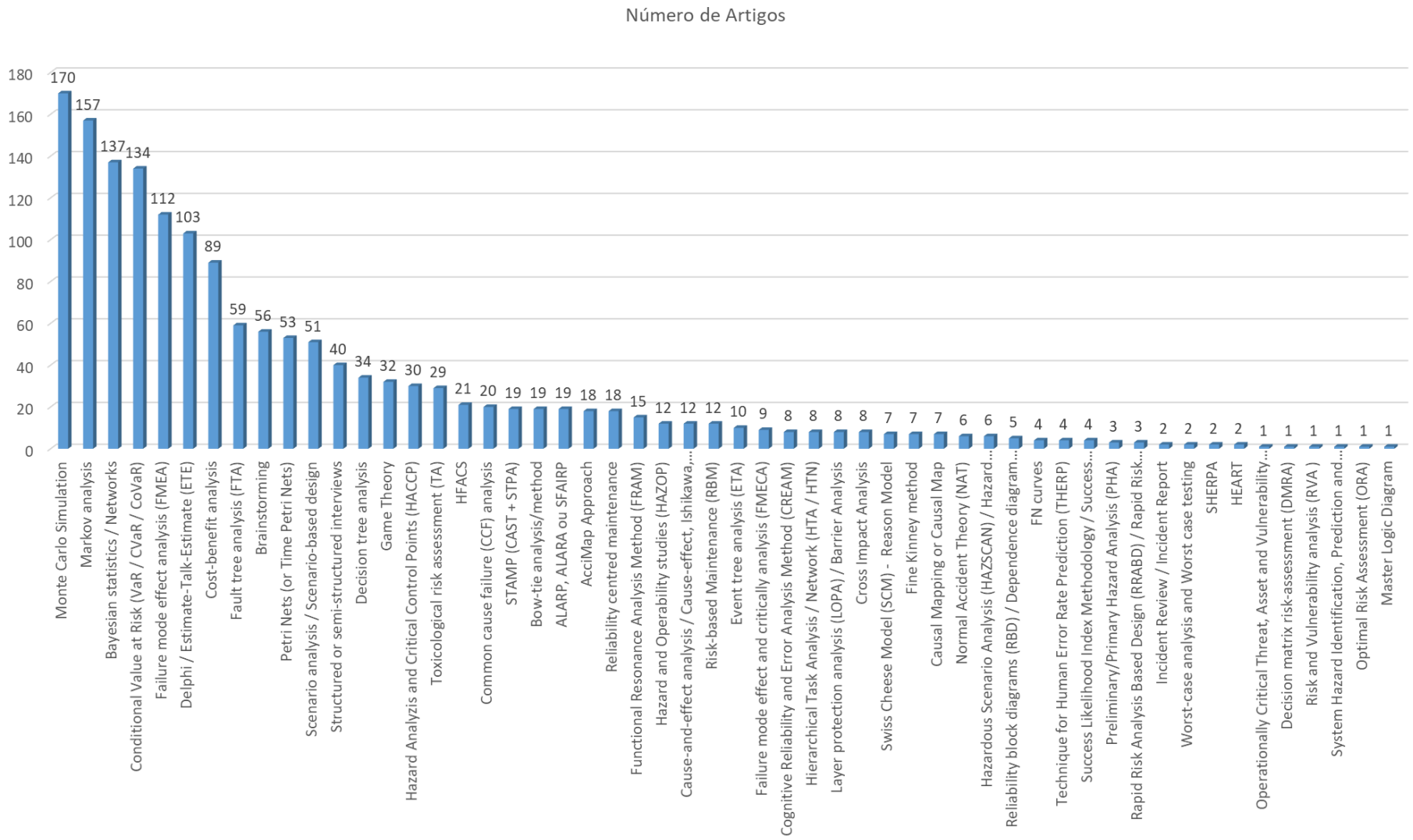


Figura 18: Número de artigos por técnica do processo de avalição de risco obtidas pela revisão sistemática.

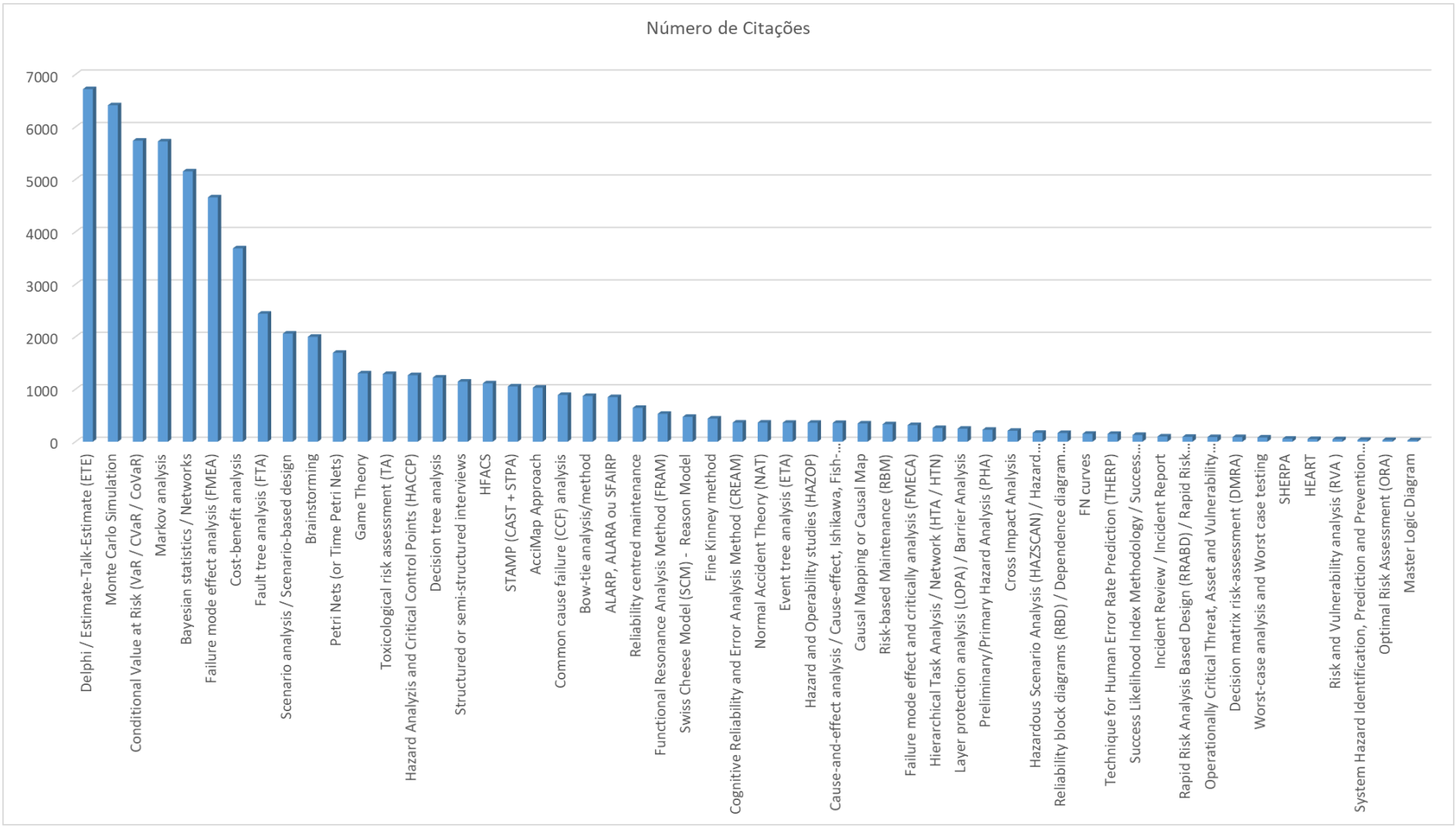


Figura 19: Número de citações por técnica do processo de avalição de risco obtidas pela revisão sistemática.

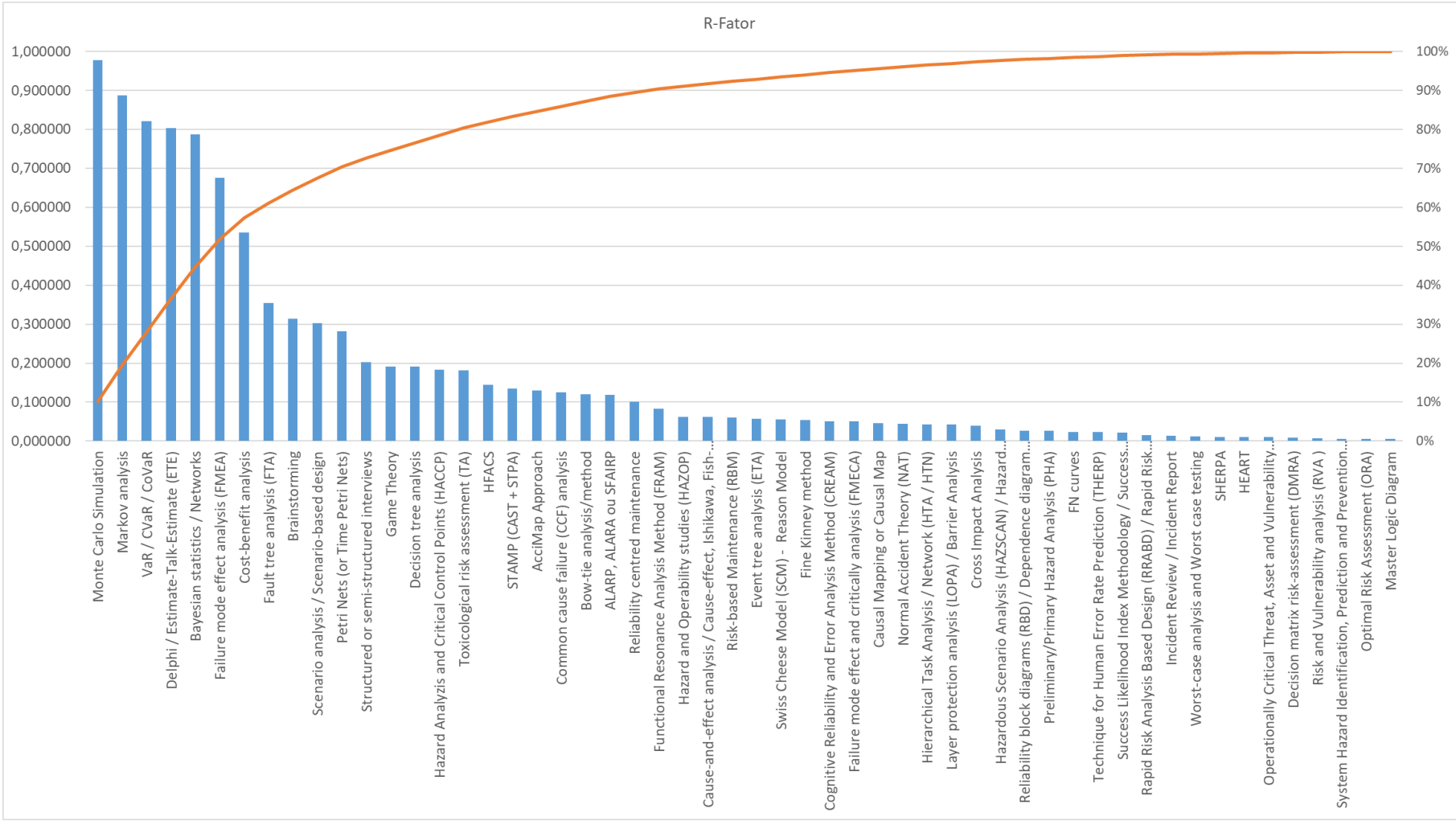


Figura 20: Valores de R-fator obtidas na avaliação de relevância na literatura no período de 2015 a 2020 das técnicas do processo de avalição de risco obtidas pela revisão sistemática.

Os dados compilados da revisão sistemática podem ser visualizados na Tabela 21, onde são apresentados o número de artigos, número de citações e os três fatores (A-fator, C-Fator e R-Fator) para cada uma das técnicas avaliadas. Os dados completos, com descrição de cada um dos artigos selecionados e as técnicas que são abordadas por eles, podem ser visualizados no Anexo A.

Tabela 21 – Resultados da revisão sistemática para os métodos de determinação de risco.

Técnicas	Número de Artigos	A-Fator	Número de Citações	C-Fator	R-Fator
Absolute Probability Judgment (APJ) / Direct numerical estimation	0	0,00	0	0,00	0,00
Accident Hazard Index (AHI)	0	0,00	0	0,00	0,00
Accident Sequences Precursor (ASP)	0	0,00	0	0,00	0,00
AcciMap Approach	18	0,11	1030	0,15	0,13
Action Error Analysis (AEA)	0	0,00	0	0,00	0,00
ALARP, ALARA ou SFAIRP	19	0,11	851	0,13	0,12
Anticipatory Failure Determination (AFD)	0	0,00	0	0,00	0,00
Barrier and operational risk analysis (BORA)	0	0,00	0	0,00	0,00
Bayesian statistics or Bayesian Networks / Statistics / Nets / Model	137	0,81	5154	0,77	0,79
Bow-tie analysis/method	19	0,11	872	0,13	0,12
Brainstorming	56	0,33	2000	0,30	0,31
Business impact analysis / assessment (BIA)	0	0,00	0	0,00	0,00
Causal Mapping or Causal Map	7	0,04	348	0,05	0,05
Cause-and-consequence analysis (CCA) or diagrams	0	0,00	0	0,00	0,00
Cause-and-effect analysis / Cause-effect diagram / Ishikawa Diagram / Fish-bone diagram / Herringbone diagram	12	0,07	358	0,05	0,06
Cindynic Approach	0	0,00	0	0,00	0,00
Clinical Risk and Error Analysis (CREA)	0	0,00	0	0,00	0,00
Cognitive Reliability and Error Analysis Method (CREAM)	8	0,05	365	0,05	0,05
Common cause failure (CCF) analysis	20	0,12	891	0,13	0,13
Concept Hazard Analysis (CHA)	0	0,00	0	0,00	0,00

Técnicas	Número de Artigos	A-Fator	Número de Citações	C-Fator	R-Fator
Concept Safety Review (CSR)	0	0,00	0	0,00	0,00
Cost-benefit analysis	89	0,52	3686	0,55	0,54
Cost-Of-Risk Analysis (CORA)	0	0,00	0	0,00	0,00
Cross Impact Analysis	8	0,05	209	0,03	0,04
Decision matrix risk-assessment (DMRA)	1	0,01	88	0,01	0,01
Decision tree analysis	34	0,20	1223	0,18	0,19
Delphi / Estimate-Talk-Estimate or ETE	103	0,61	6721	1,00	0,80
Event tree analysis (ETA)	10	0,06	362	0,05	0,06
External Events Analysis	0	0,00	0	0,00	0,00
Facilitated Risk Analysis and Assessment Process (FRAAP) / Facilitated risk analysis process (FRAP)	0	0,00	0	0,00	0,00
Failure mode effect analysis (FMEA)	112	0,66	4658	0,69	0,68
Failure mode effect and critically analysis (FMECA)	9	0,05	317	0,05	0,05
Fault/Functional Hazard Analysis (FHA)	0	0,00	0	0,00	0,00
Fault insertion testing / Fault Injection testing	0	0,00	0	0,00	0,00
Fault tree analysis (FTA)	59	0,35	2440	0,36	0,36
Fine Kinney method	7	0,04	442	0,07	0,05
FN curves	4	0,02	151	0,02	0,02
Functional Resonance Analysis Method (FRAM)	15	0,09	532	0,08	0,08
Game Theory	32	0,19	1303	0,19	0,19
Goal-Oriented Failure Analysis (GOFA)	0	0,00	0	0,00	0,00
Hazard Analyzis and Critical Control Points (HACCP)	30	0,18	1268	0,19	0,18
Hazard and Operability studies (HAZOP)	12	0,07	361	0,05	0,06
Hazard Identification and Ranking (HIRA)	0	0,00	0	0,00	0,00
Hazardous Scenario Analysis (HAZSCAN) / Hazard identification (HAZID)	6	0,04	169	0,03	0,03
Hierarchical Task Analysis (HTA) Hierarchical Task Network (HTN)	8	0,05	261	0,04	0,04
Human Error Assessment and Reduction Technique (HEART)	2	0,01	51	0,01	0,01

Técnicas	Número de Artigos	A-Fator	Número de Citações	C-Fator	R-Fator
Human Factor Event Analysis (HFEA)	0	0,00	0	0,00	0,00
Human Factors Analysis and Classification System (HFACS)	21	0,12	1113	0,17	0,14
Incident Review / Incident Report	2	0,01	100	0,01	0,01
Layer of protection analysis (LOPA) / Barrier Analysis	8	0,05	248	0,04	0,04
Markov analysis	157	0,92	5725	0,85	0,89
Master Logic Diagram	1	0,01	26	0,00	0,00
Maximum Credible Accident Analysis (MCAA)	0	0,00	0	0,00	0,00
Method Organised Systematic Analysis of Risk (MOSAR - Méthode Organisée et Systémique d'Analyse de Risques)	0	0,00	0	0,00	0,00
Monte Carlo Simulation	170	1,00	6414	0,95	0,98
Normal Accident Theory (NAT)	6	0,04	364	0,05	0,04
Nuclear Action Reliability Assessment (NARA)	0	0,00	0	0,00	0,00
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)	1	0,01	89	0,01	0,01
Optimal Risk Assessment (ORA)	1	0,01	32	0,00	0,01
Petri Nets (or Time Petri Nets)	53	0,31	1695	0,25	0,28
Predictive, Epistemic Approach (PEA)	0	0,00	0	0,00	0,00
Preliminary Hazard Analysis (PHA) / Primary hazard analysis	3	0,02	229	0,03	0,03
Rapid Risk Analysis Based Design (RRABD) / Rapid Risk Assessment (RRA)	3	0,02	94	0,01	0,02
Reliability block diagrams (RBD) / Dependence diagram (DD)	5	0,03	166	0,02	0,03
Reliability centred maintenance	18	0,11	645	0,10	0,10
Risk and Vulnerability analysis (RVA)	1	0,01	47	0,01	0,01
Risk indices / Risk Level Indicators (RLI) / Key Risk Indicators (KRIs)	0	0,00	0	0,00	0,00
Risk-based Maintenance (RBM)	12	0,07	334	0,05	0,06
Scenario analysis / Scenario-based design	51	0,30	2061	0,31	0,30
SEQHAZ Hazard Mapping	0	0,00	0	0,00	0,00
Sequentially Timed Event Plotting (STEP)	0	0,00	0	0,00	0,00

Técnicas	Número de Artigos	A-Fator	Número de Citações	C-Fator	R-Fator
Sneak circuit analysis / Sneak Analysis	0	0,00	0	0,00	0,00
Structure « What if? » (SWIFT)	0	0,00	0	0,00	0,00
Structured or semi-structured interviews	40	0,24	1146	0,17	0,20
Success Likelihood Index Methodology / Success Likelihood Index Method (SLIM)	4	0,02	129	0,02	0,02
Swiss Cheese Model (SCM) - SCM-based model - Reason Model (the ATSB accident investigation model)	7	0,04	474	0,07	0,06
System Hazard Identification, Prediction and Prevention (SHIPP)	1	0,01	34	0,01	0,01
Systematic Human Error Reduction and Prediction Analysis (SHERPA)	2	0,01	58	0,01	0,01
Systems-Theoretic Accident Model and Processes (STAMP = CAST + STPA)	19	0,11	1054	0,16	0,13
Technique for Human Error Rate Prediction (THERP)	4	0,02	150	0,02	0,02
Technique for Human Event Analysis (ATHEANA)	0	0,00	0	0,00	0,00
Toxicological risk assessment / Toxicity assessment (TA)	29	0,17	1291	0,19	0,18
Value at Risk (VaR) / Conditional Value at Risk (CVaR) (CoVaR)	134	0,79	5739	0,85	0,82
Weighted risk analysis (WRA)	0	0,00	0	0,00	0,00
Worst-case analysis and Worst-case testing	2	0,01	80	0,01	0,01

Após a revisão sistemática, destacam-se as seguintes técnicas, que representam as primeiras técnicas de maior valor de R-fator (princípio de Pareto), em ordem decrescente:

- Simulação de Monte Carlo;
- Análise de Markov;
- *Value at Risk* (VaR);
- Método Delphi;
- Redes e estatística Bayesiana;
- FMEA;
- Análise de Custo-Benefício;

- Análise de árvore de falha (FTA);
- Brainstorming;
- Análise de cenário;
- Redes de Petri;
- Entrevista estruturadas ou semiestruturadas;
- Teoria dos jogos;
- Análise de árvore de decisão;
- Análise de Perigos e Pontos Críticos de Controle (APPCC);
- Avaliação de risco toxicológico;
- Sistema de Análise e Classificação de Fatores Humanos (HFACS);
- Systems-Theoretic Accident Model and Processes (STAMP = CAST + STPA);
- Abordagem AcciMap.

Observa-se também, que os artigos avaliados possuem origem em diversas áreas de pesquisa. No total, foram avaliados artigos que pertenciam a noventa e nove (99) áreas de pesquisa, sendo as principais exibidas na Figura 21. A variedade de diversas áreas dos artigos demonstra a amplitude da revisão sistemática, que abrangeu técnicas utilizadas em diversos campos de conhecimento.

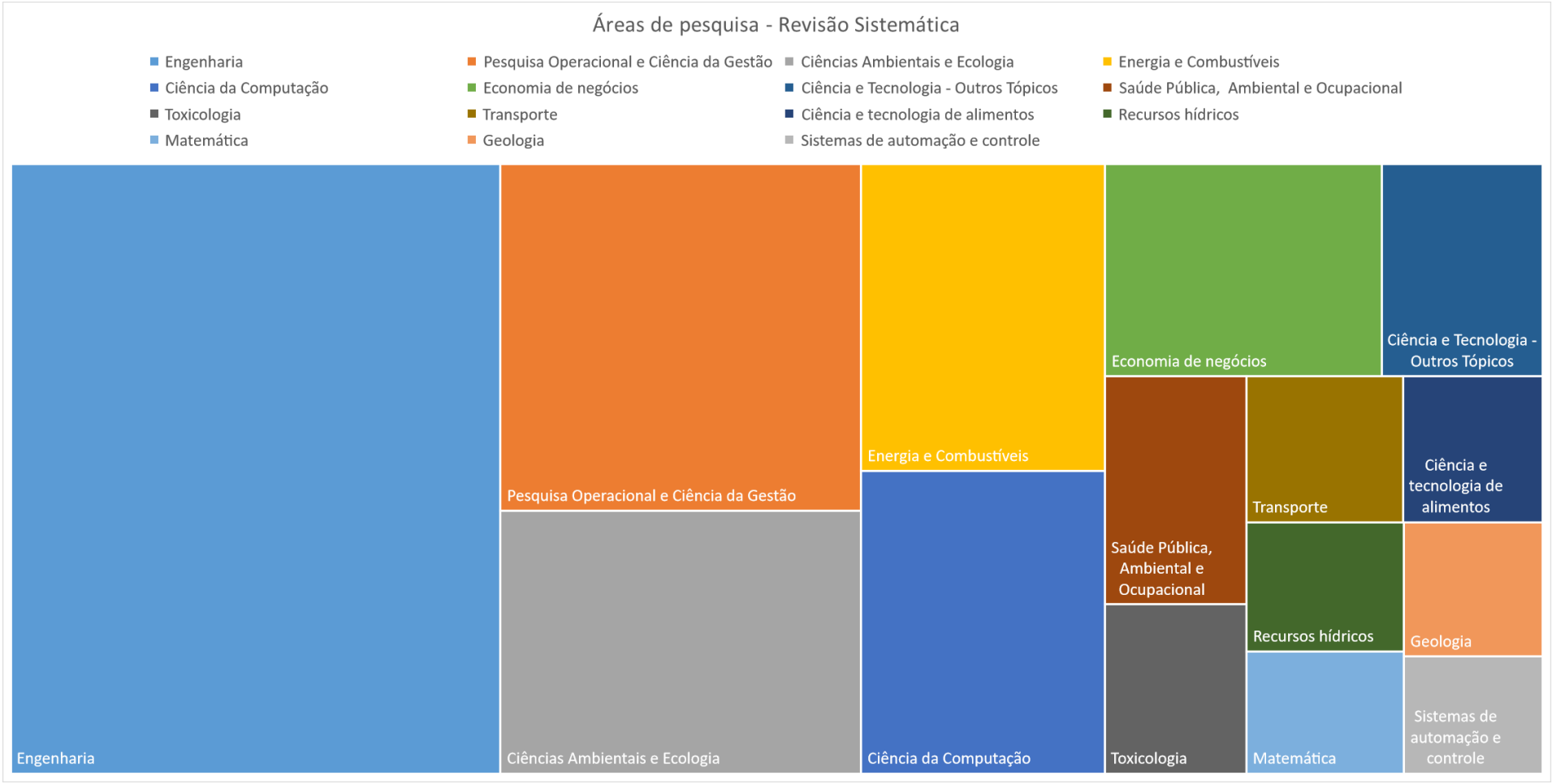


Figura 21: Áreas de pesquisa dos artigos avaliados na revisão sistemática.

4.3.2 Passo 1: Critérios de Seleção Gerais

Enfatiza-se que a escolha da técnica de determinação de risco deve ser adequada para a aplicação no sistema ou processo na qual será utilizada, considerando o nível de importância da avaliação, a complexidade do sistema analisado, as restrições de tempo, de conhecimento prévio para sua utilização, entre outros. Deste modo, deseja-se que as técnicas previamente selecionadas pelos critérios gerais sejam adequadas à aplicação, por exemplo, da cadeira de rodas motorizada. Nota-se que esta aplicação é adotada como base para aplicação neste trabalho.

Os critérios gerais descritos na seção 3.2.1 representam, portanto, os critérios mínimos para aplicação no sistema que deve ser analisado, tendo caráter eliminatório. Deseja-se que a técnica selecionada possa ser utilizada nas três etapas de determinação de risco: identificação, análise e avaliação. A Tabela 22 apresenta os critérios gerais estabelecidos, com base na abordagem apresentada na norma IEC/ISO 31010 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019), as opções para cada um dos critérios e os níveis desejados ou necessários para esta aplicação da cadeira de rodas motorizada.

Tabela 22 – Critérios gerais e níveis desejados para aplicação de cadeira de rodas motorizada.

Critério	**Opções**	**Aplicação: Cadeira de Rodas**
Objetivo	Coletar ideias e visão das partes interessadas e especialistas (F1); Identificação de riscos (F2); Determinação de fontes, causas e iniciadores de riscos (F3); Análise de controles existentes (F4); Entendimento de consequências e probabilidades (F5); Análise de dependências e interações (F6); Mensuração dos riscos (F7); Avaliação de significância dos riscos (F8); Seleção entre opções (F9); Registro e relato das ações (F10).	Identificação: F1, F2, F3; Análise: F2, F3, F4, F5, F6, F7; Avaliação: F1, F8, F9; Possibilidade de avaliação nas três etapas: Identificação, análise e avaliação
Tipo de Análise	Quantitativa; Qualitativa; Semiquantitativo; Ambas.	Ambas
Escopo	Organizacional; Departamental / Projeto; Equipamento ou Processo	Equipamento ou Processo

Critério	Opções	Aplicação: Cadeira de Rodas
Potencial dos riscos envolvidos	Estratégico; Tático; Operacional.	Operacional
Tempo para tomada de decisão	Curto; Médio; Longo; Qualquer.	Curto / Médio
Necessidade de informação prévia	Alto; Médio; Baixo.	Qualquer
Complexidade para aplicação	Baixa: equipamentos isolados / componentes ou consideração apenas de falhas aleatórias; Média: sistemas ou consideração de falhas sistemáticas; Alta: sistemas complexos.	Baixa / Média
Habilidade de pessoal	Baixo (intuitivo) Moderado (treinamento curto) Alto (treinamento significativo)	Qualquer

A Tabela 23 apresenta uma comparação entre as dezenove técnicas pré-selecionadas pela revisão sistemática na seção 4.3.1 e os níveis selecionados para os critérios gerais na aplicação da cadeira de rodas motorizada. Observa-se que as células destacadas em vermelho representam incompatibilidades entre os valores da aplicação de referência (células em verde) e os valores apresentados para cada técnica de determinação de risco para cada um dos critérios estabelecidos. As células destacadas em amarelo apresentam pontos de atenção, entretanto, não são incompatibilidades. As células sem preenchimento em cores, representam compatibilidades entre os valores adotadas de referência e os apresentados por cada técnica. Pela comparação que entre as técnicas pré-selecionadas e verificação dos valores adotados para os critérios gerais, conclui-se que três possuem compatibilidade com os níveis selecionadas para a aplicação deste trabalho:

- FTA;
- FMEA;
- STAMP.

Essas são, portanto, as técnicas a serem comparadas pelo procedimento de seleção de técnicas adequadas aos critérios específicos definidos para alcance da resiliência eletromagnética.

Tabela 23 – Critérios gerais para possíveis técnicas a serem utilizadas na aplicação, com comparação com a aplicação-base.

Técnicas	Objetivo	Tipo de Análise	Escopo	Potencial dos riscos envolvidos	Tempo para tomada de decisão	Informações prévias	Complexidade para aplicação	Habilidade de Pessoal
Baseline – Aplicação Cadeira de Rodas Motorizada	Identificação, Análise e Avaliação	Ambos (Qualitativa e Quantitativa)	Equipamento ou Processo	Operacional	Curto / Médio	Baixo / Médio	Médio	Qualquer
Monte Carlo	Entendimento de consequências e probabilidades (F5)	Quantitativa	Qualquer	Qualquer	Qualquer	Médio	Médio / Alto	Alto
Markov	Entendimento de consequências e probabilidades (F5)	Quantitativa	Equipamento ou Processo	Tático ou Operacional	Qualquer	Médio / Alto	Médio	Alto
Value at Risk (VaR)	Mensuração dos riscos (F7);	Quantitativa	Qualquer	Operacional	Curto ou médio	Alto	Médio	Alto
Delphi	Coletar ideias e visão das partes interessadas e especialistas (F1)	Qualitativa	Qualquer	Qualquer	Qualquer	Nenhuma	Médio	Moderado

Técnicas	Objetivo	Tipo de Análise	Escopo	Potencial dos riscos envolvidos	Tempo para tomada de decisão	Informações prévias	Complexidade para aplicação	Habilidade de Pessoal
Redes e estatística Bayesiana	Entendimento de consequências e probabilidades (F5) Avaliação de significância dos riscos (F8); Seleção entre opções (F9);	Quantitativa	Qualquer	Qualquer	Qualquer	Médio	Médio / Alto	Alto
FMEA FMECA	Identificação de riscos (F2); Avaliação de significância dos riscos (F8);	Ambos	Departamental / Projeto; Equipamento ou Processo	Tático ou Operacional	Qualquer	Depende da aplicação	Depende da aplicação	Moderado
Análise de Custo-Benefício	Seleção entre opções (F9);	Quantitativa	Qualquer	Qualquer	Curto ou Médio	Alto / Médio	Médio / Alto	Moderado / Alto
FTA	Determinação de fontes, causas e iniciadores de riscos (F3); Entendimento de consequências e probabilidades (F5);	Ambas	Departamental / Projeto; Equipamento ou Processo	Tático ou Operacional	Médio	Médio para análise qualitativa / Alto para análises quantitativas	Médio / Alto	Depende da aplicação
Brainstorming	Coletar ideias e visão das partes interessadas e especialistas (F1)	Qualitativa	Qualquer	Qualquer	Qualquer	Nenhuma	Baixo	Baixo / Moderado

Técnicas	Objetivo	Tipo de Análise	Escopo	Potencial dos riscos envolvidos	Tempo para tomada de decisão	Informações prévias	Complexidade para aplicação	Habilidade de Pessoal
Análise de cenário	Identificação de riscos (F2);	Qualitativo	Qualquer	Qualquer	Médio / Longo	Baixo / Médio	Baixo / Médio	Moderado
Redes de Petri	Entendimento de consequências e probabilidades (F5)	Quantitativa	Equipamento ou Processo	Tático ou Operacional	Qualquer	Médio / Alto	Médio	Alto
Entrevista estruturadas	Coletar ideias e visão das partes interessadas e especialistas (F1)	Qualitativa	Qualquer	Qualquer	Qualquer	Baixo	Baixo	Baixo / Moderado
Teoria dos jogos	Seleção entre opções (F9);	Quantitativa	Organizacional	Estratégico ou Tático	Médio	Alto	Médio / Alto	Alto
Análise de árvore de decisão	Seleção entre opções (F9);	Quantitativa	Qualquer	Tático	Qualquer	Baixo / Médio	Médio	Moderado
Avaliação de risco toxicológico	Mensuração dos riscos (F7);	Quantitativa	Processo (Risco Químicos)	Tático ou Operacional	Médio / Longo	Alto	Alto	Alto
Análise de Perigos e Pontos Críticos de Controle (APPCC)	Identificação de riscos (F2); Mensuração dos riscos (F7); Registro e relato das ações (F10);	Qualitativa	Processo (Segurança alimentar)	Tático ou Operacional	Médio / Longo	Alto	Alto	Alto
Sistema de Análise e Classificação de Fatores Humanos (HFACS);	Identificação de riscos (F2) Mensuração de riscos (F7)	Ambos	Processo (Fatores humanos)	Qualquer	Curto / Médio	Médio	Baixa / Média	Moderado

Técnicas	Objetivo	Tipo de Análise	Escopo	Potencial dos riscos envolvidos	Tempo para tomada de decisão	Informações prévias	Complexidade para aplicação	Habilidade de Pessoal
Systems-Theoretic Accident Model and Processes (STAMP = CAST + STPA);	Identificação de riscos (F2) Determinação de fontes, causas e iniciadores (F3) Análise de controles existentes (F4) Análise de dependências e interações (F6) Avaliação de significância dos riscos (F8)	Ambos (Qualitativa e semiquantitativa)	Qualquer	Tático / Operacional	Médio	Médio	Médio / Alto	Moderado
Abordagem AcciMap.	Identificação de riscos (F2) Determinação de fontes, causas e iniciadores (F3)	Qualitativa	Organizacional; Departamental / Projeto	Estratégico; Tático;	Médio	Médio	Médio / Alto	Moderado

4.3.3 Passo 1: Critérios de Seleção Específicos à Resiliência Eletromagnética

Com base nas dificuldades apresentadas na literatura, para o campo de resiliência eletromagnética, que foram sumarizadas na Tabela 9, os seguintes critérios, que são discutidos profundamente no Passo 4 em relação às técnicas selecionadas, são definidos na Tabela 24.

Tabela 24 – Critérios derivados a partir das dificuldades apontadas em literatura na área de resiliência eletromagnética.

Critério	**Medidas Aplicáveis / Critérios Possíveis**
Critério 1	Análise de envelhecimento
Critério 2	Falhas sistemáticas
Critério 3	Avaliação de Confiabilidade Humana (HRA)
Critério 4	Falha de Causa Comum (CCF)
Critério 5	Comportamento hierárquico e dependente do tempo dos sistemas
Critério 6	Análise de incertezas

4.3.4 Passo 2: Definição de Técnicas (Alternativas)

A avaliação das técnicas de maior relevância obtidas por meio da revisão sistemática, realizada na subseção 4.3.1, em relação aos critérios gerais, como descrito na subseção 4.3.2, definiram a seleção de três técnicas para serem comparadas em relação aos critérios específicos relacionados a resiliência eletromagnética na aplicação para cadeira de rodas motorizada: Modo de Falha e Análise de Efeito (FMEA), Análise de Árvore de Falha (FTA) e STAMP (*Systems-Theoretic Accident Model and Processes*). Todos os métodos podem ser aplicados em todas as fases de determinação de riscos (identificação de riscos, análise de riscos e avaliação de riscos) (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2019) e têm sido utilizados nas últimas décadas, contando com diversas aplicações e propostas de melhorias. Esses métodos diferem em suas abordagens analíticas: FMEA é um método indutivo (*bottom-up*), ou seja, uma falha específica é postulada para estabelecer os efeitos na operação do sistema; FTA e STAMP

são método dedutivos (*top-down*), ou seja, uma falha no sistema é postulada, e tem como objetivo determinar as causas ou modos para a ocorrência da falha.

4.3.5 Passo 3: Formulação do Problema de Seleção

No problema de seleção que se encontra representado na Figura 22, o objetivo é encontrar um método adequado para a determinação de risco para apoiar a obtenção da segurança funcional em relação à interferência eletromagnética, isto é, resiliência eletromagnética. Os critérios foram definidos no Passo 1 e as Alternativas no Passo 2.

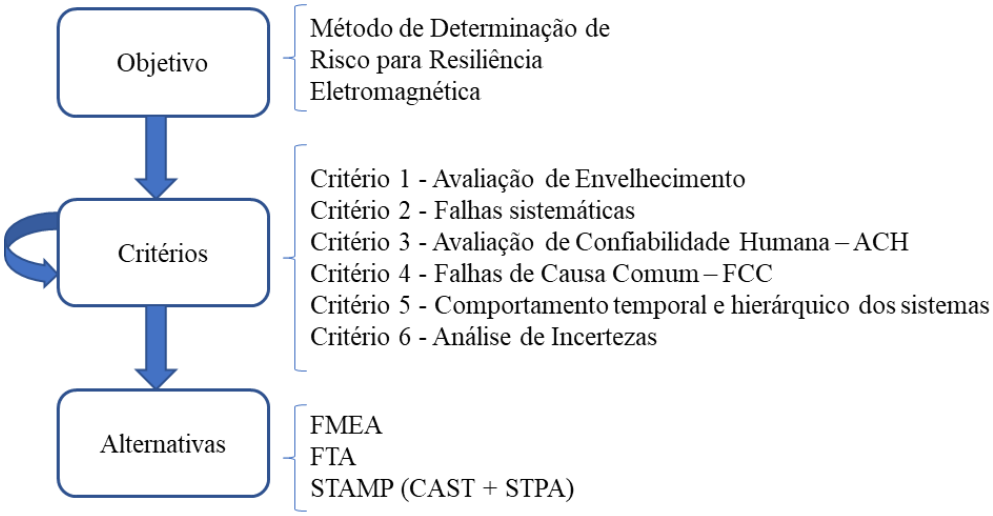


Figura 22: Rede do problema de seleção.

É possível verificar a existência de uma dependência interna no grupo (*cluster*) de critérios, representada pela sua seta em laço (*loop)*.

4.3.6 Passo 4: Método de Apoio à Decisão Multicritério

Embora a apresentação do desenvolvimento detalhado da ANP não seja o principal objetivo deste trabalho, resumidamente, as principais etapas da avaliação de decisão multicritério são descritas a seguir:

- A rede do problema de seleção é criada, com objetivo, critérios e alternativas. Nesta aplicação foi utilizado o software de código aberto *SuperDecisions* (CREATIVE DECISIONS FOUNDATION, 1996), como exibido na Figura 23;

- São estabelecidos os pesos iniciais de cada critério, e definidas as inter-relações entre os critérios e alternativas. Neste passo, é relevante observar que:
    - Inicialmente, todos os critérios recebem pesos idênticos (valor unitário dividido por seis, que representa o número de critérios);
    - Ressalta-se a existência de uma dependência interna no grupo de critérios. Neste contexto, pretende-se determinar a importância relativa dos critérios, uma vez que outro critério dependente já foi avaliado. Na aplicação proposta, os critérios 2, 3 e 4 estão relacionados, uma vez que as falhas sistemáticas são uma fonte significativa de falhas de causa comum e erros humanos podem afetar todo o processo de desenvolvimento do produto, podendo gerar falhas sistemáticas (especificação do projeto, processo de fabricação, instalação etc.). Essa consideração é necessária para evitar a avaliação exagerada de um critério em relação aos outros. Como os critérios 2, 3 e 4 estão relacionados, inseriu-se no *software SuperDecisions* valores para adequar essa consideração (um critério não dependente é duas vezes mais importante que um critério dependente);
- Posteriormente, são realizadas as avaliações pareadas das alternativas, sendo comparadas de duas a duas perante os critérios estabelecidos. A inclusão de dados pode ser realizada pelos avaliadores no *software SuperDecisions* de diversas maneiras: gráfica, verbal, matricial, questionário ou de valores diretos.

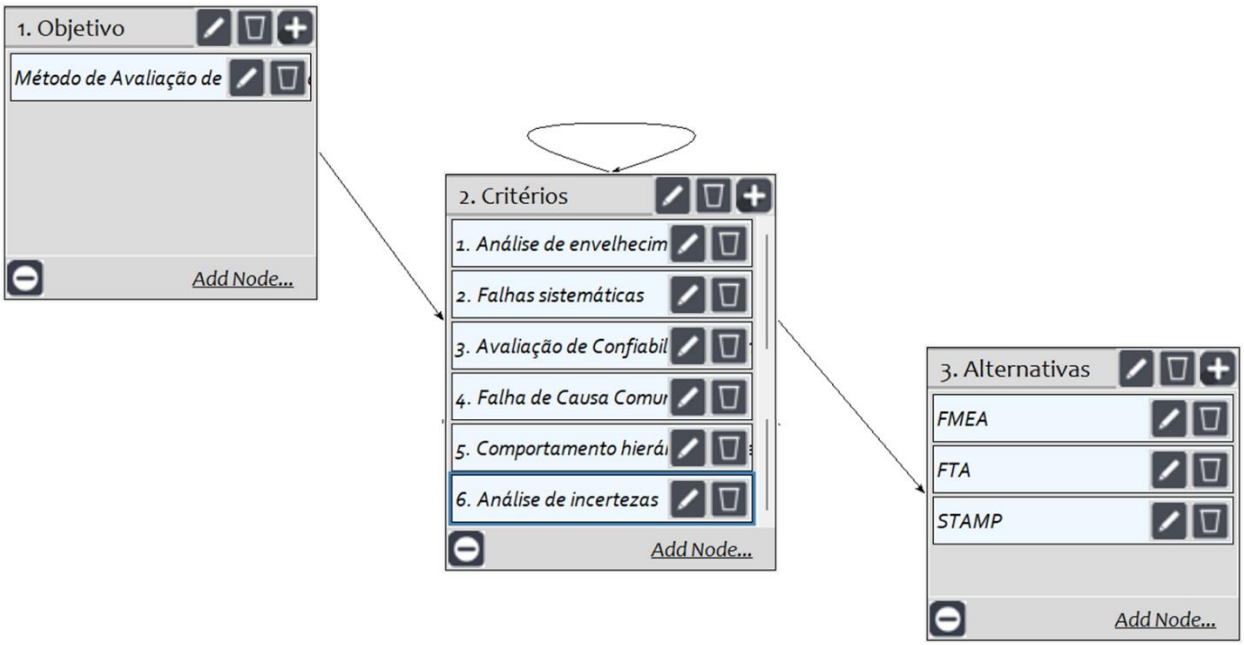


Figura 23: Rede do problema de seleção criado no *software SuperDecisions*.

4.4 Discussão dos Resultados

A aplicação do método ANP gera a denominada supermatriz estocástica, exibida na Tabela 25. Observa-se que essa matriz permite verificar as relações e influências entre critérios, alternativas e o objetivo, permitindo o cálculo final da priorização de cada alternativa. Os valores de prioridades normalizadas foram obtidos através da resolução da supermatrix por meio do *software SuperDecisions.*

Tabela 25 – Supermatriz obtida na aplicação do método de apoio à decisão multicritério ANP com o *software SuperDecisions*.

	Objetivo	Crit. 1	Crit. 2	Crit. 3	Crit. 4	Crit. 5	Crit. 6	FMEA	FTA	STAMP
Objetivo	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
Critério 1	0.16667	0.00000	0.25000	0.25000	0.25000	0.00000	0.00000	0.00000	0.00000	0.00000
Critério 2	0.16667	0.00000	0.00000	0.12500	0.12500	0.00000	0.00000	0.00000	0.00000	0.00000
Critério 3	0.16667	0.00000	0.12500	0.00000	0.12500	0.00000	0.00000	0.00000	0.00000	0.00000
Critério 4	0.16667	0.00000	0.12500	0.12500	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
Critério 5	0.16667	0.00000	0.25000	0.25000	0.25000	0.00000	0.00000	0.00000	0.00000	0.00000
Critério 6	0.16667	0.00000	0.25000	0.25000	0.25000	0.00000	0.00000	0.00000	0.00000	0.00000
FMEA	0.00000	0.40000	0.21092	0.45454	0.10615	0.14286	0.10615	0.00000	0.00000	0.00000
FTA	0.00000	0.40000	0.08414	0.09091	0.70097	0.57143	0.19288	0.00000	0.00000	0.00000
STAMP	0.00000	0.20000	0.70494	0.45454	0.19288	0.28571	0.70097	0.00000	0.00000	0.00000

Considerando o conteúdo exposto nos itens anteriores, a aplicação da ANP resulta que a

STAMP, com prioridade normalizada de 0,403452, é mais adequada do que FTA (prioridade normalizada de 0,374375) e FMEA (prioridade normalizada de 0,222173), considerando os critérios derivados e a avaliação inserida na análise (ANP). Desta maneira, se um método deve ser escolhido, o STAMP seria preferível. Esse resultado pode ser entendido pelo maior domínio do STAMP em lidar com falhas sistemáticas e sua abordagem que considera diversas fontes de incertezas. O FTA, técnica em segundo lugar na hierarquia, destaca-se por lidar com avaliações numéricas quando necessário, e devido à sua estrutura, que permite a consideração de incertezas e dependências.

De maneira simplificada, pode-se entender os resultados obtidos pela comparação entre as técnicas apresentadas na Figura 24. De modo mais detalhado, pode-se discutir as motivações dos resultados para cada um dos critérios estabelecidos:

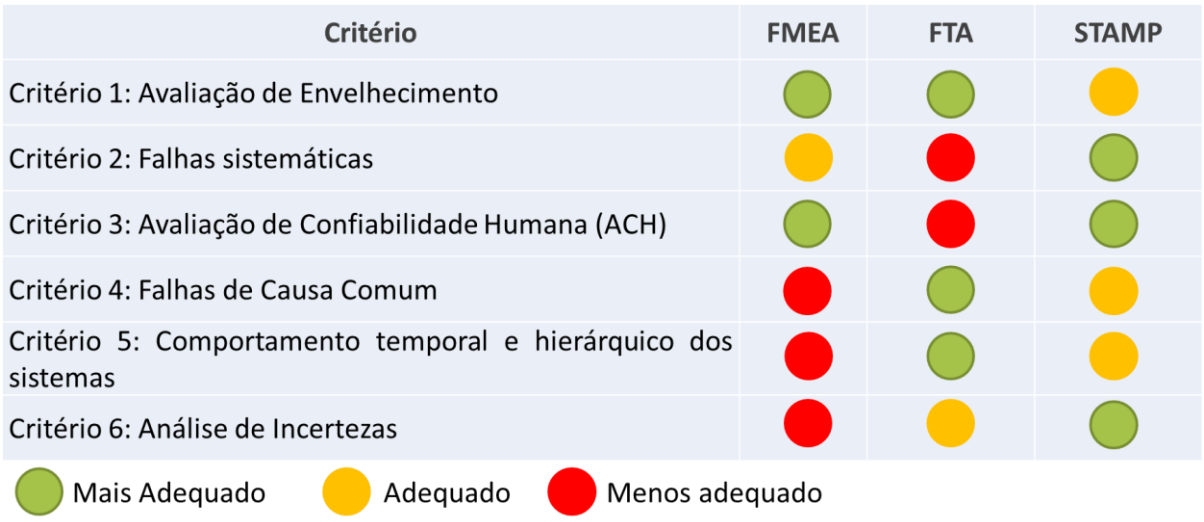


Figura 24: Comparação ilustrativa de técnicas em relação aos critérios específicos.

Critério 1 - Análise e parâmetros de envelhecimento: FMEA pode capturar falhas de mecanismos de envelhecimento e avaliá-los com base em coletas de dados ou experiência especializada. Por exemplo, ela já foi utilizada para analisar o processo de envelhecimento de transformadores de potência (EYUBOGLU, DINDAR e GUL, 2020), fiação e interconexões de aeronaves (MOFFAT, ABRAHAM, *et al.*, 2008) e baterias de íon-lítio para veículos elétricos (SCHLASZA, OSTERTAG, *et al.*, 2014). A FTA pode ser usado para a avaliação da segurança e confiabilidade dos sistemas elétricos e eletrônicos exigidos no gerenciamento do envelhecimento, especialmente quando é necessária uma avaliação numérica. O método já foi usado, por exemplo, no gerenciamento do envelhecimento do sistema de refrigeração do primário de um reator nuclear (DESWANDRI, SUBEKTI e SUNARYO, 2018) e avaliação da

confiabilidade da automação da rede inteligente (HAYATI, AHADI e MIRYOUSEFI AVAL, 2015).

Embora o método STAMP tenha como base a engenharia de sistemas, ao invés da teoria da confiabilidade, ele pode considerar os mecanismos de falha por envelhecimento que levam a ações de controle inseguras (*unsafe control actions*) que poderiam acarretar cenários acidentais ou incidentais. Deve-se ressaltar ainda que uma das etapas finais do STPA (análise de risco proveniente do STAMP) é a consideração de como os controles projetados podem se degradar ao longo do tempo e como construir proteções contra esse fenômeno, criando a necessidade de adição de alterações ou mitigações no projeto (LEVESON, 2011).

Critério 2 - Falhas sistemáticas:

O método FMEA pode, potencialmente, cobrir falhas sistemáticas desde que os especialistas responsáveis as levem em consideração, ainda que seja uma tarefa complexa. Adaptações do método têm sido propostas para analisar o projeto de software (fonte considerável desse tipo de falha), conhecido como software FMEA (SFMEA) (GODDARD, 2000) (STADLER e SEIDL, 2013).

Embora as árvores de falhas clássicas incluam apenas falhas aleatórias, algumas tentativas têm sido feitas para incluir esta categoria em seu processo de construção (SANTIAGO, FAURE e PAPADOPOULOS, 2006), incluindo, por exemplo, em aplicações para software de sistemas de controle automotivo (LI e ZHANG, 2011).

O STAMP é bastante adequado para avaliação de falhas sistemáticas uma vez que seu foco principal está na análise de software e comportamento dinâmico dos sistemas (SULAMAN, BEER, *et al.*, 2019). O método em si foi desenvolvido a partir da teoria de sistemas, partindo do princípio de que as propriedades emergentes dos sistemas surgem por meio da interação entre seus componentes. Como as propriedades emergentes são controladas pela imposição de restrições no comportamento e interações entre componentes, segurança se torna um problema de controle cujo objetivo é fazer cumprir as restrições de controle (LEVESON, 2011). O método tem sido utilizado para avaliação de sistemas eletrônicos e de software nas áreas de aviação (ALLISON, REVELL, *et al.*, 2017), naval (ROKSETH, UTNE e VINNEM, 2017), automotiva (ABDULKHALEQ, LAMMERING, *et al.*, 2017), cuidados à saúde (LEVESON, SAMOST, *et al.*, 2020), entre outras, como já anteriormente apresentado na seção 2.5.8.

Critério 3 - Avaliação de Confiabilidade Humana (HRA):

Embora existam diversos métodos específicos desenvolvidos para a realização de HRA, a FMEA é capaz de lidar com erros humanos que possam causar falhas em sistemas e equipamentos, como método principal ou auxiliar. Já foi aplicado para avaliar possíveis falhas na confiabilidade humana de dispositivos médicos (LIN, WANG, *et al.*, 2014) e para avaliação de acidentes marítimos (WU, YAN, *et al.*, 2016).

No que diz respeito ao HRA, o FTA é mais utilizado como método auxiliar devido à sua abordagem quantitativa. São muitas as possibilidades de aplicações do FTA como método de apoio à HRA, como na análise da confiabilidade do projeto de interação ergonômica de softwares de engenharia (LIU, LIU, *et al.*, 2020).

Umas das etapas do STPA prevê a criação de um modelo da estrutura de controle do sistema onde estejam incluídas as malhas de controle genéricas do sistema, sendo possível antecipar interações complexas e atuações realizadas por operadores (LEVESON e THOMAS, 2018). Deste modo, o método pode fornecer informações sobre causas de erros humanos. Adicionalmente, alguns complementos da técnica foram sugeridos na literatura para abordar os aspectos únicos dos controles humanos (STRINGFELLOW, 2010).

Critério 4 - Falha de Causa Comum (CCF):

A consideração dos riscos de CCF durante a aplicação da FMEA vem sendo considerada há muito tempo, com métodos adaptados especialmente para esse fim (CHILDS e MOSLEH, 1999). É importante ressaltar que a inclusão do CCF na FMEA tradicional pode ser uma tarefa complexa de ser realizada com alta dependência do usuário do método.

Por identificar os conjuntos de corte mínimo e conjuntos de caminho mínimo de falha de causa comum (SHAFIEE, ENJEMA e KOLIOS, 2019), o FTA é uma ferramenta adequada para análise de CCF, ou seja, casos em que um ou mais componentes de nível inferior possam causar um evento indesejado. Portanto, é possível capturar CCF em árvores de falhas, embora a consideração de múltiplos CCF seja complexa e possa demandar muito tempo de projeto, ou até mesmo sendo impossível explicitar todos eles em uma árvore de falhas para sistemas complexos.

As falhas de modo comum podem ser avaliadas no STAMP uma vez que na definição do problema podem ser consideradas os diversos perigos associados a diferentes acidentes (perdas), de modo que a técnica exige que seja mantida uma rastreabilidade entre os perigos e as perdas resultantes. O STPA já foi utilizado, por exemplo, para avaliação de segurança nos

trens de alta velocidade no Japão, em relação aos seus fatores organizacionais e institucionais. O método revelou modos de falha comum entre o operador e o regulador, o que tornava ineficaz sua aparente redundância (BUGALIA, MAEMURA e OZAWA, 2020).

Critério 5 - Comportamento Hierárquico e Dependente do Tempo dos Sistemas:

O FMEA tradicional (usando o número de prioridade de risco - RPN) não é capaz de avaliar interdependências entre os modos de falhas nem é capaz de considerar falhas hierárquicas ou dependentes do tempo. No entanto, muitos pesquisadores têm proposto melhorias para abordar esses recursos, culminando no desenvolvimento de um FMEA hierárquico e dependente do tempo (JANG e MIN, 2019).

O método FTA estabelece naturalmente uma relação hierárquica entre as falhas. Extensões ao convencional foram propostas para incluir a consideração da dependência do tempo, como árvores de falhas dinâmicas usando portas dinâmicas.

No STPA, as ações de controle inadequadas que podem levar o sistema a um estado perigoso são verificadas, considerando os casos em que: uma ação de controle necessária não é fornecida; uma ação de controle insegura (incorreta) é fornecida; uma ação de controle é fornecida muito cedo ou muito tarde (hora ou sequência errada); uma ação de controle foi interrompida muito cedo ou aplicada por muito tempo. Desde modo, as relações temporais são previstas na avaliação no método STPA (SULAMAN, BEER, *et al.*, 2019). Observa-se ainda que as próprias estruturas de controle criadas na execução do método são estruturas hierárquicas em que cada nível impõe restrições nas atividades dos níveis inferiores (LEVESON, 2011).

Critério 6 - Análise de Incertezas (processo e ambiente):

Considerações sobre incertezas podem ser incluídas no FMEA tradicional, entretanto, o desenvolvimento e gerenciamento da propagação das mesmas são bastante impraticáveis no método. Muitos pesquisadores têm proposto melhorias na avaliação de risco executada em FMEA com número de prioridade de risco (RPN), como o uso de conjuntos fuzzy no processo de priorização.

Em relação ao FTA convencional, ele geralmente usa uma probabilidade nítida para cada um dos eventos básicos para calcular a probabilidade de um evento principal. No entanto, as incertezas na probabilidade de falha de componentes ou eventos básicos podem ser assumidas (por exemplo, distribuições de probabilidade) e propagadas para calcular a incerteza no evento principal (FERDOUS, KHAN, *et al.*, 2011).

A técnica STAMP demonstra ser adequado para a análise de risco de sistemas complexos em especial no tratamento da incerteza e surpresas potenciais associadas à operação de tais sistemas (BJERGA, AVEN e ZIO, 2016). Entretanto, as abordagens probabilísticas de avaliação de incertezas não são recomendas pelo método, uma vez que a probabilidade é quase sempre desconhecida, não existindo métodos científicos ou rigorosos que sejam aceitos para obter informações de probabilidade usando dados históricos ou análise no caso de falha sistemáticas e erros de projeto do sistema (LEVESON, 2011). Cenários acidentais com grande grau de incerteza, como o desastre na mina em Soma, considerado o pior acidente de mineração na história da Turquia, também já foram avaliados pelo método CAST (análise de acidente proveniente do modelo STAMP), que demonstrou ser uma ferramenta robusto para estas avaliações (DÜZGÜN e LEVESON, 2018).

Observa-se que, embora a STAMP tenha se mostrado mais adequado, em relação ao FMEA e FTA, para os critérios derivados para uma avaliação que aborde os principais aspectos necessários à avaliação de riscos durante o processo de obtenção da resiliência eletromagnética, é importante notar que essa não cobre todos os aspectos apontados. Portanto, caso seja necessária uma ampla análise, deve ser recomendado, por exemplo, o uso de uma combinação de métodos a fim de garantir que todos os aspectos sejam considerados.

5 Considerações Finais

5.1 Conclusão

Esse trabalho propôs uma metodologia para seleção e aplicação das técnicas de avaliação de risco no processo de obtenção de resiliência eletromagnética.

A partir da revisão bibliográfica, foram propostos, inicialmente, os critérios gerais e específicos de seleção relacionados ao processo de segurança funcional considerando as necessidades de compatibilidade eletromagnética. Realizou-se na sequência, uma revisão sistemática de 86 métodos de determinação de risco, sendo analisados mais de 1400 artigos, de modo a determinar a relevância na utilização das técnicas na literatura recente. A metodologia adotada para hierarquização das técnicas teve como base o método de apoio multicritério à decisão ANP (*Analytical Network Process*), que permite a comparação pareada entre as opções, considerando ainda as dependências entre critérios, subcritérios e alternativas.

Uma avaliação de risco para uma cadeira de rodas motorizada foi desenvolvida, aplicando-se os métodos FMEA e FTA, respectivamente, ilustrando os principais aspectos dos métodos tradicionais na avaliação de risco, em especial as ocorrências relacionadas a falhas sistemáticas, que nos levaram a necessidade da busca de métodos de determinação de risco mais adequados a esse propósito. Realizou-se, então, uma aplicação da metodologia para a comparação das técnicas de determinação de risco com os métodos pré-selecionadas por meio da revisão sistemática anteriormente descrita e da aplicação dos critérios gerais estabelecidos. Deste modo, três técnicas foram consideradas para comparação em relação a seis critérios específicos relacionados a resiliência eletromagnética: Análise de Árvores de Falhas (FTA), Análise de Modos de Falhas e Efeitos (FMEA) e *Systems-Theoretic Accident Model and Processes* (STAMP). Apontaram-se, então, as vantagens e desvantagens de cada método em relação as necessidades, e após a avaliação pelo método de hierarquização ANP, como as características do STAMP demonstraram-se mais adequadas em relação aos critérios estabelecidos.

Cita-se ainda que parte dos resultados dessa dissertação foram publicados e revisados por pares no artigo *"Selection Methodology of Risk Assessment Techniques for Electromagnetic Resilience"*, selecionado para apresentação no simpósio internacional *"2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium"* e publicado na biblioteca digital

"*IEEEXplore"* do "*Institute of Electrical and Electronics Engineers*" (ISBN eletrônico :978-1-6654-4888-8) (ROQUE e SARTORI, 2021).

5.2 Trabalhos Futuros

Algumas melhorias e recomendações para trabalhos futuros podem ser realizadas para aprimoramento do método apresentado, sendo a primeira delas relacionada ao processo de decisão multicritério. A utilização de um grupo maior de especialistas, incluindo, inclusive, a utilização de técnicas para obtenção de um consenso nos valores de entrada nas comparações pareadas do método de apoio multicritério à decisão para as técnicas de avaliação de risco selecionadas como alternativas, pode evitar ou reduzir os efeitos de possíveis resultados sistematicamente imprecisos.

Pode-se citar, também, a possibilidade da utilização da técnica STAMP na avaliação de aplicações como a apresentada no texto, permitindo uma comparação direta e discussão dos resultados a serem obtidos, de forma a verificar a adequação do método na análise de situações em que as falhas sistemáticas são predominantes.

A possibilidade de inclusão de novos critérios específicos de acordo com as aplicações avaliadas poderá, também, ser considerado em trabalhos futuros. A estrutura do procedimento proposto de seleção de técnicas de determinação de riscos mantém-se. Nota-se, no entanto, que dependendo dos sistemas analisados, critérios relacionados às perturbações eletromagnéticas específicas da aplicação podem ser adicionados ou alterados.

Referências

AALIPOUR, M.; AYELE, Y. Z.; BARABADI, A. Human reliability assessment (HRA) in maintenance of production process: a case study. **International Journal of Systems Assurance Engineering and Management**, v. 7, p. 229-238, 2016.

ABBASSI, R. et al. An integrated method for human error probability assessment during the maintenance of offshore facilities. **Process Safety and Environmental Protection**, v. 94, p. 172-179, 2015.

ABDULKHALEQ, A. et al. A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles. **Procedia Engineering**, v. 179, p. 41-51, 2017.

AGENCY, I. A. E. **Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants**. [S.l.]. 2016.

AHN, J.; CHANG, D. Fuzzy-based HAZOP study for process industry. **Journal of Hazardous Materials**, 317, 2016. 303-311.

AKYUZ, E. A hybrid accident analysis method to assess potential navigational contingencies: The case of ship grounding. **Safety Science**, v. 79, p. 268-276, 2015.

AKYUZ, E.; CELIK, M. A methodological extension to human reliability analysis for cargo tank cleaning operation on board chemical tanker ships. **SAFETY SCIENCE**, v. 75, p. 146-155, 2015.

AKYUZ, E.; CELIK, M. A hybrid human error probability determination approach: The case of cargo loading operation in oil/chemical tanker ship. **Journal of Loss Prevention in the Process Industries**, v. 43, p. 424-431, 2016.

ALD SERVICES. Fault Tree Analysis (FTA) Software, 2020. Disponivel em: <https://aldservice.com/Reliability-Products/fta.html>. Acesso em: 13 maio 2020.

ALDEMIR, T. Computer-Assisted Markov Failure Modeling of Process Control Systems. **IEEE Transactions on Reliability**, v. R-36, n. 1, p. 133-144, Abril 1987.

ALLEN, J. G. Radio Interference. **Proceedings of the Institute of Radio Engineers**, 17, Maio 1929. 882 - 891.

ALLISON, C. K. et al. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. **Safety Science**, v. 98, p. 159-166, 2017.

AMERICAN SOCIETY OF SAFETY PROFESSIONALS. **ANSI/ASSP Z590.3: Guidelines For Addressing Occupational Hazards And Risks In Design And Redesign Processes**. [S.l.], p. 80. 2011.

ARMSTRONG, K. EMC-Related Functional Safety (An update), 2002. Disponivel em: <https://www.emcstandards.co.uk/files/emc-related_functional_safety_an_update_emcj_nov_2002.pdf>. Acesso em: 30 Setembro 2020.

ARMSTRONG, K. Review of progress with EMC-related functional safety. **2003 IEEE Symposium on Electromagnetic Compatibility. Symposium Record**, 1, 2003. 454-459.

ARMSTRONG, K. The IET's new guide: EMC for Functional Safety - applying Risk Management to EMC, 2010. Disponivel em: <https://www.emcstandards.co.uk/files/inside_functional_safety_magazine_sent_for_publication_12_mar_10.pdf>. Acesso em: 30 Setembro 2020.

ARMSTRONG, K. **The First Five Hundred "Banana Skins"**. [S.l.]: [s.n.], 2014.

ARMSTRONG, K. **How to Do EM Functional Safety - the Latest Guidance From the IET**. 7th Asia Pacific International Symposium on Electromagnetic Compatibility. Shenzhen, China: [s.n.]. 2016. p. 1018-1020.

ARMSTRONG, K.; DUFFY, A. Reducing the Functional Safety Risks (and other be caused by EMI - new IEEE Standard 1848. **IEEE Letters on Electromagnetic Compatibility Practice and Applications (Early Access)**, 2020. 1-9.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 14971: Dispositivos médicos - Aplicação de gerenciamento de risco a dispositivos médicos**. [S.l.], p. 41. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 7176-21: Cadeira de rodas - Parte 21: Requisitos e métodos de ensaio para compatibilidade eletromagnética de cadeiras de rodas motorizadas e scooters e carregadores de baterias**. [S.l.], p. 22. 2019.

AVEN, T. **Risk Analysis**. [S.l.]: John Wiley & Sons, Ltd, 2015.

BAIG, A. A.; RUZLI, R.; BUANG, A. B. Reliability Analysis Using Fault Tree Analysis: A Review. **International Journal of Chemical Engineering and Applications**, v. 4, n. 3, p. 169-173, 2013.

BAKER, S. P. et al. The Injury Severity Score: a method for describing patients with multiple injuries and evaluating emergency care. **The Journal of Trauma. Lippincott Williams & Wilkins.** , v. 14, n. 3, p. 187–196, 1974.

BANA E COSTA, C. A.; VANSNICK, J. C. The MACBETH Approach: Basic Ideas, Software, and an Application. In: _____ **Advances in Decision Analysis. Mathematical Modelling:** Theory and Applications. Dordrecht: Springer, 1999. p. 131-157.

BASU, S. **Plant Hazard Analysis and Safety Instrumentation Systems**. 1ª edição. ed. [S.l.]: Academic Press, 2016. 1062 p.
BEHZADIAN, M. et al. PROMETHEE: A comprehensive literature review on methodologies and applications. **European Journal of Operational Research**, v. 200 (1), p. 198-215, 2010.
BEHZADIAN, M. et al. A state-of the-art survey of TOPSIS applications. **Expert Systems with Applications**, v. 39 (17), p. 13051-13069, 2012.
BELL , J.; HOLROYD, J. **Review of human reliability assessment methods**. Health and Safety Executive (HSE). [S.l.], p. 90. 2009.
BELL, J. L.; WILLIAMS, J. C. Consolidation of the Generic Task Type database and concepts used in the Human Error Assessment and Reduction Technique (HEART). **Safety and Reliability**, v. 36, p. 245-278, 2016.
BJERGA, T.; AVEN, T.; ZIO, E. Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. **Reliability Engineering & System Safety**, v. 156, p. 203-209, 2016.
BJÖRKLÖF, D. Immunity testing: Examining requirements and test methods". **Compliance Engineering European Edition's- Annual Reference Guide**, p. 51, 1999. Disponivel em: <www.ce-mag.com>.
BOERLE, D. G.; LEFERINK, F. The Jammed Wheelchair: a case study of EMC and functional safety. **IEEE Electromagnetic Compatibility Society newsletter**, v. Fall, p. 63-67, 2004.
BOERLE, D. G.; LEFERINK, F. B. J. The Jammed Wheelchair: a case study of EMC and functional safety. **IEEE Electromagnetic Compatibility Society Newsletter**, v. Fall, p. 61-65, 2004.
BÖRCSÖK, J.; UGLJESA, E.; MACHMUR, D. **Calculation of MTTF values with Markov models for safety instrumented systems**. Proceedings of the 7th Conference on 7th WSEAS International Conference on Applied Computer Science. [S.l.]: World Scientific and Engineering Academy and Society (WSEAS). 2007. p. 30-35.
BORING, R. L. **Fifty Years of THERP and Human Reliability Analysis**. Probabilistic Safety Assessment and Management. Helsinki, Finlândia: [s.n.]. 2012.
BORYS, D.; ELSE, D.; LEGGETT, S. The fifth age of safety: The adaptive age. **Journal of Health Services Research and Policy**, v. 1, p. 19-27, 2009.
BOUTI, A.; KADI, D. A. A State-of-the-Art Review of FMEA/FMECA. **International Journal of Reliability, QUality and Safety Engineering**, v. 01, n. 04, p. 515-543, 1994.
BRANFORD, K. **An investigation into the validity and reliability of the AcciMap approach**. Australian National University. Canberra, p. 341. 2007.
BRANFORD, K. Seeing the big picture of mishaps: Applying the AcciMap approach to analyze system accidents. **Aviation Psychology and Applied Human Factors**, v. 1, n. 1, p. 31-37, 2011.
BRANS, J. P.; VINCKE, P.; MARESCHAL, B. How to select and how to rank projects: The Promethee method. **European Journal of Operational Research**, v. 24 (2), p. 228-238, 1986.
BUGALIA, N.; MAEMURA, Y.; OZAWA, K. Organizational and institutional factors affecting high-speed rail safety in Japan. **Safety Science**, v. 128, p. 104762, 2020.
CALIXTO, E. The safety integrity level as Hazop Risk consistence. The Brazilian risk. **Risk, Reliability and Societal Safety – Aven & Vinnem**, Londres, 2007.
CAN, G. F.; DELICE, E. K. An advanced human error assessment approach: HEART andAV-DEMATEL. **Human Factors and Ergonomics in Manufacturing & Sevice Industries**, v. 30, p. 29-49, 2020.
CARLSSON, A.; LUNDÄLV, J. Acute injuries resulting from accidents involving powered mobility devices (PMDs) - Development and outcomes of PMD-related accidents in Sweden. **Traffic Injury Prevention**, v. 20, p. 484-491, 2019.
CARVALHO, P. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic management system resilience. **Reliability Engineering & System Safety**, 2011. 1482-1498.
CHATTERTON, P. A.; HOULDEN, M. A. **EMC:** Electromagnetic Theory to Practical Design. [S.l.]: Wiley, 1991. 310 p.
CHIB, S. Chapter 57 - Markov Chain Monte Carlo Methods: Computation and Inference. In: HECKMAN, J. J.; LEAMER, E. **Handbook of Econometrics**. [S.l.]: Elsevier, v. 5, 2001. p. 3569-3649.
CHILDS, J. A.; MOSLEH, A. Modified FMEA tool for use in identifying and addressing common cause failure risks in industry. **Proceedings of the Annual Reliability and Maintainability Symposium**, p. 19-24, 1999.
CHIN, K.-S.; CHAN, A.; YANG, J.-B. Development of a fuzzy FMEA based product design system. **The International Journal of Advanced Manufacturing Technology Vol. 36**, Março 2008. 633-649.
CHOI, S. W. et al. Factors associated with injury severity among users of powered mobility devices., v. 8, n. 2, p. 103-110, Junho 2021.
CLARIVATE. Web of Science - Researchers, 2020. Disponivel em: <https://clarivate.com/webofsciencegroup/solutions/researcher/>. Acesso em: 02 set. 2020.
CLERMONT, M.; DYCKHOFF, H. Coverage of Business Administration Literature in Google Scholar: Analysis and Comparison with Econbiz, Scopus and Web of Science. **Bibliometrie - Praxis und Forschung**, v. 1, n. 1, p. 54, 2012.

COLLINS , S. J. et al. Effectiveness of the Surgical Safety Checklist in Correcting Errors: A Literature Review Applying Reason's Swiss Cheese Model. **AORN Journal**, v. 100, p. 65-79, 2014.
COMPLIANCE ENGINEERING. But broken limbs have occurred as a result of such interference, Setembro / Outubro 1994. Disponivel em: <www.ce-mag.com>.
CONGGUANG, M.; CANAVERO, F. System-Level Vulnerability Assessment for EME: From Fault Tree Analysis to BayesianNetworks — Part I: Methodology Framework. **IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY**, v. 58, n. 1, p. 180-187, Fevereiro 2016.
CORBETT, L. J. The radio interference problem and the power company. **Journal of the A.I.E.E.**, v. 44, p. 1057-1063, Outubro 1925.
CORFMAN, T. A. et al. Tips and falls during electric-powered wheelchair driving: effects of seatbelt use, legrests, and driving speed. **Arch Phys Med Rehabil.**, v. 84, n. 12, p. 1797-1802, Dezembro 2003.
COUNCIL OF THE EUROPEAN UNION. **Council directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work**. [S.l.], p. 8. 1989.
COUTINHO, J. S. D. Failure-Effect Analysis. **Transactions of The New York Academy of Sciences**, 26, n. 5, Março 1964. 564-584.
CREATIVE DECISIONS FOUNDATION. Super Decisions CDF, 1996. Disponivel em: <http://www.superdecisions.com/>. Acesso em: 2021 abr. 29.
CZAJA, S. J.; NAIR, S. N. Human Factors Engineering and Systems Design. In: SALVENDY, G. **Handbook of Human Factors and Ergonomics**. 4ª edição. ed. [S.l.]: Wiley, 2012.
DE CICCO, F.; FANTAZZINI, M. L. **Tecnologias Consagradas de Gestão de Risco**. [S.l.]: Risk Tecnologia Editora Ltda, v. Coleção Risk Tecnologia, 2003. 194 p.
DEBRINCAT, J.; BIL, C.; CLARK, G. Assessing organisational factors in aircraft accidents using a hybrid Reason and AcciMap model. **Engineering Failure Analysis**, v. 27, p. 52-60, 2013.
DEPARTMENT OF HEALTH AND HUMAN SERVICES. Letter to Industry, Powered Wheelchair/Scooter or Accessory/Component Manufacturer. **Radio waves may interfere with control of powered wheelchairs and motorized scooters**, 20 Setembro 1994. Disponivel em: <https://www.fda.gov/media/113980/download>.
DESWANDRI; SUBEKTI, M.; SUNARYO, G. R. Reliability Analysis of RSG-GAS Primary Cooling System to Support Aging Management Program. **Journal of Physics: Conference Series**, v. 962, n. 1, p. N° de Artigo: 012002, 2018.
DHILLON, B. S. **Design Reliability:** Fundamentals and Applications. Boca Raton, Florida: CRC Press LLC, 1999.
DNV. **OREDA:** Offshore Reliability Data Handbook. [S.l.]: [s.n.], 2015. 832 p.
DOWELL, A. M. Layer of protection analysis for determining safety integrity level. **ISA Transactions**, v. 37, p. 155-165, 1998.
DUFFIELD, S.; WHITTY, J. Developing a systemic lessons learned knowledge model for organisational learning through projects. **International Journal of Project Management**, v. 33, p. 311-324, 2015.
DUNJÓ, J. et al. Hazard and operability (HAZOP) analysis. A literature review. **Journal of hazardous materials**, 173, Setembro 2009. 19-32.
DÜZGÜN, H. S.; LEVESON, N. Analysis of soma mine disaster using causal analysis based on systems theory (CAST). **Safety Science**, v. 110, p. 37-57, 2018.
ELSEVIER. Scopus - Content Coverage Guide, jan. 2020. Disponivel em: <https://www.elsevier.com/?a=69451>. Acesso em: 02 set. 2020.
ELSEVIER. Scopus: Access and use Support Center, 29 abr. 2020. Disponivel em: <https://service.elsevier.com/app/answers/detail/a_id/15534/supporthub/scopus/#tips>. Acesso em: 02 set. 2020.
EYUBOGLU, O. H.; DINDAR, B.; GUL, O. Risk Assessment by Using Failure Modes and Effects Analysis (FMEA) Based on Power Transformer Aging for Maintenance and Replacement Decision. **Proceedings - 2020 IEEE 2nd Global Power, Energy and Communication Conference**, p. 251-255, 2020.
FERDOUS, R. et al. Fault and event tree analyses for process systems risk analysis: uncertainty handling formulations. **Risk Anal.**, v. 31, p. 86-107, 2011.
FUSSEL, J. B.; POWERS, G. J.; BENNET, R. G. Fault Trees - A State of the Art Discussion. **IEEE Transactions on Reliability**, v. 23, n. 1, p. 51-55, 1974.
GALL, H. Functional safety IEC 61508 / IEC 61511 the impact to certification and the user. **2008 IEEE/ACS International Conference on Computer Systems and Applications**, 2008. 1027-1031.
GAO, T.-T.; WANG, S.-M. Fuzzy Integrated Evaluation Based on HAZOP. **Procedia Engineering**, 211, 2018. 176-182.
GENENDER, E. et al. Fault tree analysis for system modeling in case of intentional EMI. **Advances in Radio Science**, v. 9, p. 297-302, Agosto 2011.

GENENDER, E.; GARBE, H.; SABATH, F. Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level. **IEEE Transactions On Electronic RANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY**, v. 56, n. 1, p. 200-207, Fevereiro 2014.
GILKS, W. R.; RICHARDSON, S.; SPIEGELHALTER, D. **Markov Chain Monte Carlo in Practice**. 1ª. ed. Nova Iorque: Imprint Chapman and Hall/CRC, 1995. 512 p.
GLENDON, A. I.; CLARKE, S.; MCKENNA, E. **Human Safety and Risk Management**. 2ª edição. ed. Boca Raton: CRC Press, 2006.
GODDARD, P. L. **Software FMEA techniques**. Annual Reliability and Maintainability Symposium. Proceedings. International Symposium on Product Quality and Integrity. Los Angeles, CA, USA: [s.n.]. 2000. p. 118-123.
GONÇALVES FILHO, A. P.; JUN, G. T.; WATERSON, P. Four studies, two methods, one accident – An examination of the reliability and validity of Accimap and STAMP for accident analysis. **Safety Science**, v. 113, p. 310-317, 2019.
GONZALEZ, O. R.; GRAY, W. S.; PATILKULKARNI, S. Analysis of memory bit errors induced by electromagnetic interference in closed-loop digital flight control systems. **19th Digital Avionics Systems Conference**, Philadelphia, PA, USA, 1, 2000. 3C5/1-3C5/9.
GOVINDAN, K.; JEPSEN, M. B. ELECTRE: A comprehensive literature review on methodologies and applications. **European Journal of Operational Research**, v. 250 (1), p. 1-29, 2016.
GROOT BOERLE, D. J. **EMC and functional safety, impact of IEC 61000-1-2**. 2002 IEEE International Symposium on Electromagnetic Compatibility. Minneapolis, MN, USA, USA: [s.n.]. 2002.
GUSENBAUER, M. Google Scholar to overshadow them all? Comparing the sizes of 12 academic search engines and bibliographic databases. **Scientometrics**, v. 118, p. 177–214, 2019.
HAASL, D. F. Advanced Concepts in Fault Tree Analy. **System Safety Symposium**, 1965.
HAIMES, Y. Y. **Risk Modeling, Assessment, and Management**. 3ª Edição. ed. Hoboken, New Jersey: John Wiley & Sons, 2008.
HALE, A. R.; HOVDEN, J. Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment. In: FEYER, A. M.; WILLIAMSON, A. **Occupational Injury:** Risk, Prevention, and Intervention. Londres: CRC Press, 1998. p. 320.
HAYATI, H.; AHADI, A.; MIRYOUSEFI AVAL, S. M. New concept and procedure for reliability assessment of an IEC 61850 based substation and distribution automation considering secondary device faults. **Frontiers in Energy,** v. 9, n. 4, p. 387-398, 2015.
HEALTH AND SAFETY EXECUTIVE. **Guidance on the use of programmable electronic systems in safety-related applications**. [S.l.]. 1989.
HEINRICH, H. W. **Industrial Accident Prevention:** a scientific approach. 1ª edição. ed. [S.l.]: McGraw-Hill, 1931. 366 p.
HICKEY, J.; HOMMES, Q. V. E. Effectiveness of accident models: system theoretic model vs. the Swiss Cheese model: a case study of a US Coast Guard aviation mishap. **International Journal of Risk Assessment and Management**, v. 17, p. 46-68, 2013.
HOLLNAGEL, E. **Barriers and Accident Prevention**. 1ª edição. ed. [S.l.]: Routledge, 2004.
HOLLNAGEL, E. **An Applicattion of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change**. Swedish Radiation Safety Authority - SSM. [S.l.]. 2012.
HOLLNAGEL, E.; HOUNSGAARD, J.; COLLIGAN, L. **FRAM - The Functional Resonance Analysis Method - a handbook for the practical use of the method**. [S.l.]: Centre for Quality, 2004.
HOLLNAGEL, E.; WOODS, D.; LEVESON, N. Resilience Engineering: Concepts and Precepts. [S.l.]: CRC Press, 2006. p. 416.
HU, J. et al. An intelligent fault diagnosis system for process plant using a functional HAZOP and DBN integrated methodology. **Engineering Applications of Artificial Intelligence**, v. 45, p. 119-135, 2015.
HUDSON, P. Implementing a safety culture in a major multi-national. **Safety Science**, v. 45, n. 6, p. 697–722, 2007.
HUNT, J. E.; PRICE, C. J.; LEE, M. H. Automating the FMEA process. **Intelligent Systems Engineering**, v. 2, n. 2, p. 119-132, 1993.
HWANG, C.-L.; YOON, K. **Multiple Attribute Decision Making:** Methods and Applications A State-of-the-Art Survey. Nova Iorque: Springer-Verlag Berlin Heidelberg, 1981. 269 p.
IDAHO NATIONAL LABORATORY. **NUREG/CR-6883, "The SPAR-H Human Reliability Analysis Method"**. U.S. Nuclear Regulatory Commission. Washington, DC. 2005.
IEC EMC Players. Disponivel em: <https://www.iec.ch/emc/iec_emc/iec_emc_players_intro.htm>. Acesso em: 15 fev. 2019.
IEEE Electromagnetic Compatibility Magazine. Disponivel em: <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5962381>. Acesso em: 07 jun. 2020.

IEEE Transactions on Power Electronics. Disponivel em: <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=63>. Acesso em: 07 jun. 2020.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 500, "IEEE Guide To The Collection And Presentation Of Electrical, Electronic, Sensing Component, And Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations"**. [S.l.]: IEEE, 1984. 1424 p.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE C62.41.1: IEEE Guide on the Surge Environment in Low-Voltage (1000 V and less) AC Power Circuits**. [S.l.], p. 162. 2002.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE C62.41.2: IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and less) AC Power Circuits**. [S.l.], p. 44. 2002.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE C62.45: IEEE Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000 V and less) AC Power Circuits**. [S.l.], p. 85. 2002.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE C62.48: IEEE Guide on Interactions Between Power System Disturbances and Surge Protective Devices**. [S.l.], p. 20. 2005.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE Std 1848, "Techniques & Measures to Manage Functional Safety and Other Risks With Regard to Electromagnetic Disturbances"**. [S.l.]. 2020.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. IEEE Transactions on Electromagnetic Compatibility. Disponivel em: <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=15>. Acesso em: 07 jun. 2020.

INSTITUTION OF ENGINEERING AND TECHNOLOGY. **Electromagnetic Compatibility for Functional Safety**. Stafford, p. 173. 2008.

INSTITUTION OF ENGINEERING AND TECHNOLOGY. **Overview of Techniques and Measures Related to EMC for Functional Safety**. Shrewsbury, p. 45. 2013.

INSTITUTION OF ENGINEERING AND TECHNOLOGY. **Code of Practice for Electromagnetic Resilience**. [S.l.]: IET Standards, 2017. 134 p.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 60050-161: International Electrotechnical Vocabulary (IEV) - Part 161: Electromagnetic compatibility**. [S.l.], p. 73. 1990.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 1508: Functional Safety: Safety-Related Systems. Parts 1-7**. [S.l.]. 1995.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61165: Application of Markov techniques**. [S.l.], p. 67. 2006.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-2: Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test**. [S.l.], p. 129. 2008.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-8: Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test**. [S.l.], p. 141. 2009.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems - Parts 1 to 7**. [S.l.], p. 127. 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61508-4, "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements"**. [S.l.]. 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations**. [S.l.], p. 68. 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-4: Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test**. [S.l.], p. 140. 2012.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-6: Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields**. [S.l.], p. 168. 2013.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-5: Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test**. [S.l.], p. 334. 2014.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-1-2: Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena**. [S.l.], p. 149. 2016.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61025, "Fault tree analysis (FTA)"**. [S.l.]. 2016.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61025: Fault tree analysis (FTA)**. [S.l.], p. 103. 2016.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61882: Hazard and operability studies (HAZOP studies) - Application guide**. [S.l.], p. 124. 2016.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC TR 61000-4-1: Electromagnetic compatibility (EMC) - Part 4-1: Testing and measurement techniques - Overview of IEC 61000-4 series**. [S.l.], p. 19. 2016.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 60812: Failure modes and effects analysis (FMEA and FMECA)**. [S.l.], p. 165. 2018.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-2-2: Electromagnetic compatibility (EMC) - Environment - Compatibility levels for low-frequency conducted disturbances and signalling in public low-voltage power supply systems**. [S.l.], p. 161. 2018.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **CISPR 16: Specification for radio disturbance and immunity measuring apparatus and methods**. [S.l.], p. 195. 2019.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC/ISO 31010: Risk management - Risk assessment techniques**. [S.l.], p. 264. 2019.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. EMC Explained - EM disturbance phenomena categories, 2020. Disponivel em: <https://www.iec.ch/emc/explained/categories.htm>. Acesso em: 29 ago. 2020.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-11: Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests for equipment with input current up to 16 A per phase**. [S.l.], p. 194. 2020.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-4-3: Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test**. [S.l.], p. 194. 2020.
INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61000-3: Electromagnetic compatibility (EMC) - Part 3: Limit - ALL PARTS**. [S.l.], p. 833. 2022.
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO GUIDE 73, "Risk management — Vocabulary"**. [S.l.]. 2009.
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 9000: Quality Management**. [S.l.]. 2015.
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 31000, "Risk management – Guidelines"**. [S.l.], p. 16. 2018.
ISHIMATSU, T. et al. **Modeling and Hazard Analysis Using STPA**. Proceedings of the 4th IAASS Conference, Making Safety Matter. Huntsville, Alabama: International Association for the Advancement of Space Safety (IAASS). 2010.
ISHIZAKA, A.; NEMERY, P. **Multi-criteria Decision Analysis:** Methods and Software. Chichester: Wiley, 2013. 310 p.
ISLAM, R. et al. Development of a human reliability assessment technique for the maintenance procedures of marine and offshore operations. **Journal of Loss Prevention in the Process Industries**, v. 50, p. 416-428, 2017.
ISOGRAPH LTD. FaultTree+, 2020. Disponivel em: <https://www.isograph.com/software/reliability-workbench/fault-tree-analysis-software/fault-tree-analysis/>. Acesso em: 13 maio 2020.
JANG, H.-A.; MIN, S. Time-dependent probabilistic model for hierarchical structure in failure mode and effect analysis. **Applied Sciences**, v. 9, p. art. no. 4265, 2019.
JORDAN, W. E. **Failure modes, effects and criticality analyses**. Proceedings of Annual Reliability and Maintainability Symposium. São Francisco, Califórnia: Institute of Electrical and Electronics Engineers. 1972. p. 30-37.
KABIR, S. An overview of fault tree analysis and its application in model based dependability analysis. **Expert Systems With Applications**, v. 77, p. 114-135, 2017.
KEENEY, R. L.; RAIFFA, H. **Decisions with multiple objectives:** Preferences and value tradeoffs. Nova Iorque: Cambridge University Press, 1976.
KEISER, B. E. **Principles of electromagnetic compatibility**. [S.l.]: Artech House Microwave Library, 1979.
KIRKCALDY, K. J.; CHAUHAN, D. **Functional Safety in the Process Industry:** A Handbook of Practical Guidance in the Application of IEC61511 and ANSI/ISA-84. [S.l.]: Lulu.com, 2012. 214 p.
KIRWAN, B. The validation of three human reliability quantification techniques — THERP, HEART and JHEDI: Part 1 — technique descriptions and validation issues. **Applied Ergonomics**, v. 26, p. 359-373, 1996.
KIRWAN, B. et al. The validation of three Human Reliability Quantification techniques — THERP, HEART and JHEDI: Part II — Results of validation exercise. **Applied Ergonomics**, v. 28, p. 17-25, 1997.
KIRWAN, B. et al. Nuclear action reliability assessment (NARA): a data-based HRA tool. **Safety and Reliability**, 25, 2005. 38-45.

KLETZ, T. A. An obituary: ICI's contribution to process safety and why it came to an end. **Journal of Loss Prevention in the Process Industries**, v. 23, p. 954-957, 2010.
KOSMOWSKI, K. T. Functional safety concept for hazardous systems and new challenges. **Journal of Loss Prevention in the Process Industries**, 19, 2006. 298-305.
LABIB, A.; READ, M. A hybrid model for learning from failures: The Hurricane Katrina disaster. **Expert Systems with Applications**, 42, n. 21, 2015. 7869-7881.
LAI, Y.-J.; LIU, T.-Y.; HWANG, C.-L. TOPSIS for MODM. **European Journal of Operational Research**, v. 76 (3), p. 486-500, 1994.
LAPA, C. M. F.; GUIMARÃES, A. C. F. Hazard and operability study using approximate reasoning in light-water reactors passive systems. **Nuclear Engineering and Design**, v. 236, p. 1256-1263, 2006.
LEE, W. S. et al. Fault Tree Analysis, Methods, and Applications - A Review. **IEEE Transactions on Reliability**, v. R-34, n. 3, p. 194-203, 1985.
LEGG, J. M. Computerized Approach for Matrix-Form FMEA. **IEEE Transactions on Reliability**, v. R-27, n. 4, p. 254-257, 1978.
LEVESON, N. A New Accident Model for Engineering Safer Systems. **Safety Science**, v. 42, p. 237-270, 2004.
LEVESON, N. et al. A Systems Approach to Analyzing and Preventing Hospital Adverse Events. **Journal of Patient Safety**, v. 16, p. 162-167, 2020.
LEVESON, N. G. **Engineering a Safer World:** Systems Thinking Applied to Safety. 1ª. ed. Cambridge, Massachusetts: The MIT Press, 2011. 560 p.
LEVESON, N. G. Rasmussen's legacy: A paradigm change in engineering for safety. **Applied Ergonomics**, v. 59, p. 581-591, 2017.
LEVESON, N. G. **CAST HANDBOOK: How to Learn More from Incidents and Accidents**. [S.l.], p. 148. 2019.
LEVESON, N. G.; THOMAS, J. P. **STPA Handbook**. [S.l.], p. 188. 2018.
LI, W.; ZHANG, H. A software hazard analysis method for automotive control system. **roceedings - 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE)**, v. 3, p. 744-748, 2011.
LIN, Q.-L. et al. Human reliability assessment for medical devices based on failure mode and effects analysis and fuzzy linguistic theory. **Safety Science**, v. 62, p. 248-256, 2014.
LIU, X. et al. Human Reliability Assessment of Ergonomic Interaction Design for Engineering Software Based on Entropy-FTA-Delphi. **ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering**, v. 6, p. art. no. 04020035, 2020.
LOGHMANPOUR, N. A. et al. A new Bayesian network-based risk stratification model for prediction of short-term and long-term LVAD mortality. **ASAIO Journal**, v. 61, p. 313-323, 2015.
LUNDBLAD, K. et al. FRAM as a risk assessment method for nuclear fuel transportation. **Proceedings of the 4th International Conference Working on Safety**, 2008.
MARRIOTT, R. H. Interference. **Proceedings of the Institute of Radio Engineers**, v. 11, p. 375-388, Agosto 1923.
MARTÍNEZ, R. S. **System Theoretic Process Analysis of Electric Power Steering for Automotive Applications (Thesis)**. Massachusetts, p. 197. 2015.
MATEO, J. R. S. C. Multi-Criteria Analysis. In: _____ **Multi Criteria Analysis in the Renewable Energy Industry**. Londres: Springer, 2012. p. 7-10.
MINISTÉRIO DO TRABALHO E PREVIDÊNCIA SOCIAL. **NR 10 – Segurança em Instalações e Serviços em Eletricidade**. Portaria MTPS n.º 508. [S.l.]. 2016.
MOFFAT, B. G. et al. Failure mechanisms of legacy aircraft wiring and interconnects. **IEEE Transactions on Dielectrics and Electrical Insulation**, v. 15, n. 3, p. 808-822, 2008.
MTL INSTRUMENTS GROUP. **An introduction to Functional Safety and IEC 61508 (AN9025)**. [S.l.], p. 13. 2002.
MULLINEAUX, T. An update on the C63 standards, 2005. Disponivel em: <https://www.evaluationengineering.com/home/article/13002982/an-update-on-the-c63-standards>. Acesso em: 17 Outubro 2021.
NOUVEL, D.; TRAVADEL, S.; HOLLNAGEL, E. Introduction of the Concept of Functional Resonance in the Analysis of a Near-Accident in Aviation. **33rd ESReDA Seminar: Future challenges of accident investigation**, Itália, 2007. 9.
OLAF, P. H. US1765443A, 1928.
OTT, H. W. **Noise Reduction Techniques in Electronic Systems**. 1ª. ed. [S.l.]: Wiley-Interscience, 1976.
OTT, H. W. **Electromagnetic Compatibility Engineering**. 1ª. ed. [S.l.]: Wiley, 2009. 843 p.
PAPADOPOULOS, Y.; PARKER, D.; GRANTE,. A method and tool support for model-based semi-automated failure modes and effects analysis of engineering designs. **In Proceedings of the 9th Australian workshop on Safety critical systems and software**, v. 47, p. 89-95, 2004.

PAPAZOGLOU, I. A.; GYFTOPOULOS, E. P. Markov Processes for Reliability Analyses of Large Systems. **IEEE Transactions on Reliability**, v. R-26, n. 3, p. 232-237, Agosto 1977.
PAUL, C. R. **Introduction to Electromagnetic Compatibility**. 2nd. ed. [S.l.]: Wiley-Interscience, 2006. 1016 p.
PAWLICKI, T. et al. Application of systems and control theory-based hazard analysis to radiation oncology. **Med Phys**, v. 43, p. 1514-1530, 2016.
PEETERS, J. F. W.; BASTEN, R. J. I.; TINGA, T. Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner. **Reliability Engineering and System Safety**, v. 172, p. 36-44, 2017.
PEREZ, R. **The Handbook of Electromagnetic Compatibility**. [S.l.]: Academic Press, 1995.
RASMUSSEN, J. Risk management in a dynamic society: a modelling problem. **Safety Science**, v. 27, p. 183-213, 1997.
RASMUSSEN, N. **WASH-1400, "The Reactor Safety Study"**. Nuclear Regulatory Commission. [S.l.]. 1975.
RAUSAND, M. **Risk Assessment:** Theory, Methods, and Applications. 1ª Edição. ed. Hoboken, New Jersey: Wiley, 2011. 664 p.
REASON, J. **Human Error**. Cambridge: Cambridge University Press, 1990.
REASON, J. The contribution of latent human failures to the breakdown of complex systems. **Philosophical Transactions of the Royal Society**, v. 327, p. 475-484, 1990.
REASON, J. **Managing the risks of organizational accidents**. [S.l.]: Routledge, 1997.
REASON, J. **Managing the Risks of Organizational Accidents**. 1ª. ed. [S.l.]: Ashgate, 1997. 252 p.
REASON, J. Human error: models and management. **BMJ**, v. 320, p. 768-770, 2000.
REASON, J. T. Human error: models and management. **British Medical Journal**, v. 320, p. 768–770, 2000.
REASON, J.; HOLLNAGEL, E.; PARLES, J. Revisiting the « Swiss Cheese » Model of Accidents, Outubro 2016. Disponivel em: <https://www.eurocontrol.int/eec/gallery/content/public/document/eec/report/2006/017_Swiss_Cheese_Model.pdf>. Acesso em: 05 ago. 2020.
RELIASOFT. BlockSim, 2020. Disponivel em: <https://www.reliasoft.com/products/blocksim-system-reliability-availability-maintainability-ram-analysis-software>. Acesso em: 13 maio 2020.
RELIOTECH. TopEvent FTA. **Fault Tree Analysis Software**, 2020. Disponivel em: <https://www.fault-tree-analysis.com/free-fault-tree-analysis-software>. Acesso em: 13 maio 2020.
RELIOTECH S.A.S. TopEvent FTA - Fault Tree Analysis Software. Disponivel em: <https://www.fault-tree-analysis.com/>. Acesso em: 20 Outubro 2021.
ROCKWELL AUTOMATION. **Functional Safety in the Process Industry: Principles, standards and implementation**. [S.l.], p. 168. 2013.
ROKSETH, B.; UTNE, I. B.; VINNEM, J. E. A systems approach to risk analysis of maritime operations. **Journal of Risk and Reliability**, v. 231, p. 53-68, 2017.
ROQUE, A. M.; SARTORI, C. A. F. Selection Methodology of Risk Assessment Techniques for Electromagnetic Resilience. **2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium**, Outubro 2021. 7-12.
ROY, B. The outranking approach and the foundations of electre methods. **Theory and Decision**, v. 31 (1), p. 49-73, 1991.
ROY3, B. Classement et choix en pr´esence de points de vue multiples (la m´ethode ELECTRE). **Revue d'Informatique et de Recherche Op´erationnelle**, v. 2 (8), p. 57–75, 1968.
RUIJTERS, E.; STOELINGA, M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. **Computer Science Review**, v. 15-16, p. 29-62, 2015.
SAATY, T. L. A scaling method for priorities in hierarchical structures. **Journal of Mathematical Psychology**, v. 15 (3), p. 234-281, 1977.
SAATY, T. L. **Decision Making with Dependence and Feedback:** The Analytic Network Process. Pittsburgh, Pennsylvania: RWS Publications, 1996. 370 p.
SAATY, T. L. Fundamentals of the Analytic Network Process - dependence and feedback in decision-making with a single network. **Journal of Systems Science and Systems Engineering**, v. 13, n. 2ª, p. 129-157, 2004.
SAATY, T. L. Fundamentals of the analytic network process—multiple networks with benefits, costs, opportunities and risks. **Journal of Systems Science and Systems Engineering**, v. 13, n. 2, p. 348–379, 2004.
SAATY, T. L. **Theory and Applications of the Analytic Network Process**. Pittsburgh, PA 15213.: RWS Publications, 2005. 352 p.
SABATH, F. EMI Risk Management with the Threat Scenario, Effect, and Criticality Analysis. **Ultra-Wideband, Short-Pulse Electromagnetics 10**, 2014. 265-278.
SAE INTERNATIONAL. **J1739: Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA)**. [S.l.], p. 32. 2009.

SAE INTERNATIONAL. **ARP5580: Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications**. [S.l.], p. 58. 2012.
SALMON, P. et al. Systems-based accident analysis in the led outdoor activity domain: application and evaluation of a risk management framework. **Ergonomics**, v. 53, p. 927-939, 2010.
SALMON, P. M.; CORNELISSEN, M.; TROTTER, M. J. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. **Safety Science**, v. 50, p. 1158-1170, 2012.
SANTIAGO, I. B.; FAURE, J.-M.; PAPADOPOULOS, Y. Including Systematic Faults Into Fault Tree Analysis. **IFAC Proceedings Volumes**, v. 39, n. 13, p. 765-770, 2006.
SAWARAGI, T.; HORIGUCHI, Y.; HINA, A. Safety analysis of systemic accidents triggered by performance deviation. **SICE-ICASE International Joint Conference**, 2006. 1778-1781.
SCHLASZA, C. et al. **"Review on the aging mechanisms in Li-ion batteries for electric vehicles based on the FMEA method**. IEEE Transportation Electrification Conference and Expo: Components, Systems, and Power Electronics - From Technology to Business and Public Policy (ITEC). [S.l.]: [s.n.]. 2014.
SECRETARIA ESPECIAL DE PREVIDÊNCIA E TRABALHO. **Norma Regulamentadora n.º 01 - Disposições Gerais e Gerenciamento de Riscos Ocupacionais**. [S.l.]. 2020. (Portaria SEPRT n.º 6.730).
SHAFIEE, M.; ENJEMA, E.; KOLIOS, A. An Integrated FTA-FMEA Model for Risk Analysis of Engineering Systems: A Case Study of Subsea Blowout Preventers. **Appl. Sci.**, v. 9, p. 1192, 2019.
SHIRLEY, R. B. et al. Validating THERP: Assessing the scope of a full-scale validation of the Technique for Human Error Rate Prediction. **Annals of Nuclear Energy**, v. 77, p. 194-211, 2015.
SIU, N. Risk assessment for dynamic systems: An overview. **Reliability Engineering & System Safety**, 43, n. I, 1994. 43-73.
SLAUSON, W. E. et al. **General Methodologies for Assessing EMI/EMC in Complex Electronic Circuits and Systems**. Military Communications Conference. Boston, MA, USA: MILCOM. 1985. p. 313-314.
SMITH, D. et al. Understanding industrial safety: Comparing Fault tree, Bayesian network, and FRAM approaches. **Journal of Loss Prevention in the Process Industries**, 45, 2017. 88-101.
SMITH, D.; SIMPSON, K. **The Safety Critical Systems Handbook:** A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) & Related Guidance. 4ª. ed. [S.l.]: Elsivier Ltd., 2016. 330 p.
SOSNER, J. et al. Forces, moments, and accelerations acting on an unrestrained dummy during simulations of three wheelchair accidents. **Am J Phys Med Rehabil.**, v. 76, n. 4, p. 304-10, Julho-Agosto 1997.
SPREAFICO, C.; RUSSO, D.; RIZZI, C. A state-of-the-art review of FMEA/FMECA including patents. **Computer Science Review**, 25, Agosto 2017. 19-28.
STADLER, J. J.; SEIDL, N. J. **Software failure modes and effects analysis**. Proceedings - Annual Reliability and Maintainability Symposium. [S.l.]: [s.n.]. 2013.
STOREY, N. R. **Safety Critical Computer Systems**. 1ª. ed. [S.l.]: Addison-Wesley Longman Publishing Co., 1996. 472 p.
STRINGFELLOW, M. **Human and Organizational Factors in Accidents**. [S.l.]: MIT, 2010.
SU, H. et al. An integrated systemic method for supply reliability assessment of natural gas pipeline networks. **Applied Energy**, v. 209, p. 489-501, 2018.
SUJAN, M.-A.; FELICI, M. Combining failure mode and functional resonance analyses in healthcare settings. **International Conference on Computer Safety, Reliability, and Security**, 2012. 364-375.
SULAMAN, S. M. et al. Comparison of the FMEA and STPA safety analysis methods–a case study. **Software Quality Journal**, v. 27, p. 349–387, 2019.
SUTRISNO, A.; LEE, T.-R. Service reliability assessment using failure mode and effect analysis (FMEA): Survey and opportunity roadmap. **International Journal of Engineering, Science and Technology**, v. 3, n. 7, p. 25-38, 2012.
SWAIN, A. D.; GUTTMANN, H. E. **NUREG/CR- 1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications"**. Sandia National Laboratories. [S.l.]. 1983.
SYDOR, M.; KRAUSS, A.; KRAUSS, H. Risk analysis for operating active wheelchairs in non-urban settings. **Ann Agric Environ Med.**, v. 24, p. 532-536, 2017.
TAHERIYOUN, M.; MORADINEJAD, S. Reliability analysis of a wastewater treatment plant using fault tree analysis and Monte Carlo simulation. **Environmental Monitoring and Assessment**, v. 187, n. Número do Artigo: 4186, 2015.
TALEBBERROUANE, M.; KHAN, F.; LOUNIS, Z. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. **Journal of Loss Prevention in the Process Industries**, v. 44, p. 193-203, 2016.
TANG, Z.; DUGAN, J. B. Minimal cut set/sequence generation for dynamic fault tress. **Reliability and Maintainability**, p. 207-213, 2004.
THOMAS, J.; DE LEMOS, F. L.; LEVESON, N. **Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants**. [S.l.], p. 66. 2012. (Research Report: NRC-HQ-11-6-04-0060).

THOMAS, J.; LEVESON, N. A New Approach to Risk Management and Safety Assurance of Digital Instrumentation and Control Systems. **Transactions of the American Nuclear Society**, v. 109, p. 1948, 2013.
TRANSACTIONS on Communications. Disponivel em: <https://www.ieice.org/cs/jpn/EB/index.html>. Acesso em: 07 jun. 2020.
U.S. NUCLEAR REGULATORY. **NUREG-0492: Fault Tree Hanbook**. Washington, p. 209. 1981.
U.S. NUCLEAR REGULATORY COMISSION. **Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems"**. Office of Nuclear Regulatory Research. [S.l.], p. 47. 2003.
U.S. NUCLEAR REGULATORY COMMISSION. **NUREG/CR-6782: Comparison of U.S. Military and International Electromagnetic Compatibility Guidance**. [S.l.], p. 46. 2003.
UNDERWOOD, P.; WATERSON, P. A critical review of the STAMP, FRAM and Accimap systemic accident analysis models. In: STANTON, N. **Advances in Human Aspects of Road and Rail Transportation**. [S.l.]: CRC Press, 2012. p. 385-394.
UNDERWOOD, P.; WATERSON, P. A critical review of the STAMP, FRAM and Accimap systemic accident analysis models. In: STANTON, N. A. **Advances in Human Aspects of Road and Rail Transportation**. [S.l.]: CRC Press, 2012. p. 878.
UNDERWOOD, P.; WATERSON, P. Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. **Accident Analysis & Prevention**, v. 68, p. 75-94, 2014.
US DEPARTMENT OF DEFENSE. **MIL-P-1629: Procedures for performing a failure mode, effects and criticality analysis**. [S.l.], p. 35. 1949.
US DEPARTMENT OF DEFENSE. **MIL-STD-1629A: Procedures For Performing A Failure Mode, Effects, And Criticality Analysis**. [S.l.], p. 79. 1980.
US DEPARTMENT OF DEFENSE. **MIL-STD-1629A: Procedures for Performing a Failure Mode, Effets, and Criticality Analysis**. [S.l.], p. 11. 1980.
US DEPARTMENT OF DEFENSE. **MIL-STD-461G:** Requirements for the control of electromagnetic interference characteristics of subsystems and equipment. [S.l.]: US Military Specs/Standards/Handbooks. 31 Julho 2015.
US DEPARTMENT OF LABOR. **OSHA 3133: Process Safety Management Guidelines for Compliance**. Occupational Safety and Health Administration. [S.l.]. 1994.
VAIDYA, O. S.; KUMAR, S. Analytic hierarchy process: An overview of applications. **European Journal of Operational Research**, v. 169 (1), p. 1-29, 2006.
VILLACOURT, M. **Failure Mode and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry**. [S.l.], p. 25. 1992.
WALLENIUS, J. et al. Multiple criteria decision making, multiattribute utility theory: Recent accomplishments and what lies ahead. **Management Science**, v. 54 (7), p. 1336-1349, 2008.
WANG, H. et al. SDG-based HAZOP analysis of operating mistakes for PVC process. **Process Safety and Environmental Protection**, 87, 2009. 40-46.
WATERSON, P. et al. Defining the methodological challenges and opportunities for an effective science of sociotechnical systems and safety. **Ergonomics**, v. 58, p. 565–599, 2015.
WATERSON, P.; JENKINS, D. P.; SALMO, P. M. 'Remixing Rasmussen': The evolution of Accimaps within systemic. **Applied Ergonomics**, v. 59, p. 483-503, 2017.
WILLIAMS, J. C. **Heart—A Proposed Method for Achieving High Reliability**. Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety. Soutport: [s.n.]. 1985.
WILLIAMS, J. C. **A Proposed Method for Assessing and Reducing Human Error**. In Proceedings of the 9th Advance in Reliability Technology Symposium. Bradford: [s.n.]. 1986. p. B3/R/1 – B3/R/13.
WILLIAMS, J. C. **A Data-based method for assessing and reducing Human Error to improve operational experience**. In Proceedings of IEEE 4th. Conference on Human Factors in power Plants. Monterey, California: [s.n.]. 1988. p. 436-450.
WIRTH, R. et al. Knowledge-based support of system analysis for the analysis of FMs and effects. **Engineering Applications of Artificial Intelligence**, v. 9, p. 219-229, 1996.
WU, B. et al. Quantitative method to human reliability assessment for maritime accident. **Jiaotong Yunshu Xitong Gongcheng Yu Xinxi/Journal of Transportation Systems Engineering and Information Technology**, v. 16, p. 24-30, 2016.
XIANG, H.; CHANY, A. M.; SMITH, G. A. Wheelchair related injuries treated in US emergency departments. **Inj Prev.**, v. 12, n. 1, p. 8-11, 2006.
YANG, K.; TAO, L.; BAI, J. Assessment of Flight Crew Errors Based on THERP. **Procedia Engineering**, v. 80, p. 49-58, 2014.
YAZDI, M.; KABIR, S.; WALKER, M. Uncertainty handling in fault tree based risk assessment: State of the art and future perspectives. **Process Safety and Environmental Protection**, p. 89-104, 2019.

ZHOU, H. et al. **Functional safety analysis and promotion for relay protection device platform**. Proceedings of the 8th International Conference on Informatics, Environment, Energy and Applications (IEEA ’19). Nova Iorque: Association for Computing Machinery. 2019. p. 171-177.
ZHOU, K.; ZAIN, A. M. Fuzzy Petri nets and industrial applications: a review. **Artificial Intelligence Review**, v. 45, p. 405-446, 2016.

Anexo A – Artigos da Revisão Sistemática

O anexo A apresenta os artigos utilizados no processo de revisão sistemática das técnicas de determinação de risco cujo critérios foram definidos na seção 3.3 e os seus resultados apresentados na seção 4.3.1.

Devido a extensão do conteúdo, optou-se pela inclusão de link para acesso ao arquivo em Excel com título “MatrizdeArtigosporTecnica_AcassioRoque.xlsx”:

https://drive.google.com/file/d/1WXWHrxzHR7Cm7ihZvzdhzXtkMeILqxwF/view?usp=sharing

O arquivo apresenta os dados básicos dos artigos ou livros encontrados nos bancos de dados científicos, como título, autores, resumo, ano de publicação, DOI, jornal ou revista de publicação, data da busca, os métodos utilizados nos respectivos artigos e informações adicionais.

Anexo B – Descrição das Técnicas de Determinação de Risco

Neste anexo são apresentadas as técnicas de determinação de risco utilizadas na revisão sistemática com suas principais referências e uma breve descrição da técnica. O objetivo não é detalhar cada uma das técnicas, mas apresentar um breve descritivo inicial sobre cada uma das técnicas avaliadas, permitindo ao leitor dessa dissertação, caso seja do seu interesse, buscar conteúdos mais detalhados. Este conteúdo foi utilizado para a construção da Tabela 10 na seção 3.3.

Tabela 26 – Técnicas de determinação de risco analisadas pela revisão sistemática.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Absolute Probability Judgment (APJ) Direct numerical estimation	Humphreys, P. Human Reliability Assessor's Guide. Human Factors in Reliability Group, 1995. Mary E. Wilkie, Andrew C. Pollock, An application of probability judgement accuracy measures to currency forecasting, International Journal of Forecasting, Volume 12, Issue 1, pp. 25-40, ISSN 0169-2070, 1996. Liu, P., Qiu, Y., Hu, J., Tong, J., Zhao, J., Li, Z. Expert judgments for performance shaping Factors' multiplier design in human reliability analysis (2020) Reliability Engineering and System Safety, 194, art. no. 106343. Grozdanovic, M. Usage of human reliability quantification methods	O julgamento de probabilidade absoluta (APJ) é uma técnica usada no campo da avaliação da confiabilidade humana (HRA), com o propósito de avaliar a probabilidade de um erro humano ocorrer durante a conclusão de uma tarefa específica. A partir de tais análises, podem ser tomadas medidas para reduzir a probabilidade de ocorrência de falhas em um sistema e, portanto, levar a uma melhoria nos níveis gerais de segurança.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	(2005) International Journal of Occupational Safety and Ergonomics, 11 (2), pp. 153-159.	
Accident Hazard Index (AHI)	F.I. Khan, S.A. Abbasi, Accident Hazard Index: A Multi-Attribute Method for Process Industry Hazard Rating, Process Safety and Environmental Protection, Volume 75, Issue 4, 1997, pp. 217-224, ISSN 0957-5820, https://doi.org/10.1205/095758297529093.	O índice de risco de acidente (IAH) representa as consequências de um acidente em uma escala padrão (1 ± 10). O processo começa com a previsão do cenário de acidente mais credível. O cenário de acidente é desenvolvido para estimar o dano potencial, e avalia-se o impacto de outros fatores na gravidade do acidente. Esses fatores influenciam a gravidade de um acidente de duas maneiras: impacto direto e impacto indireto.
Accident Sequences Precursor (ASP)	Holmberg, J. Risk follow-up by probabilistic safety assessment—experience from a Finnish pilot study. Reliability Engineering & System Safety, 53, 3-15, 1996. D. Markberry, C. Hunter, G. DeMoss U.S. Nuclear Regulatory Commission Accidents Sequence Precursor (ASP) Program Summary Description, Washington, DC	A análise de Precursores de Sequências de Acidentes (ASP), uma das metodologias de avaliação de risco quantitativa para eventos operacionais que ocorrem em usinas nucleares, usa avaliação de risco probabilística (PRA) para avaliar sistematicamente a significância do risco de eventos operacionais e para selecionar precursores aplicando critérios quantitativos. Os precursores são os eventos operacionais que podem causar resfriamento inadequado do núcleo ou danos ao núcleo. A gestão sistemática dos precursores selecionados desempenha um papel importante na melhoria da segurança das usinas nucleares.
AcciMap Approach	Jens Rasmussen, Risk management in a dynamic society: a modelling problem, Safety Science, Volume 27, Issues 2–3, 1997, pp. 183-213, ISSN 0925-7535.	É uma técnica de análise de acidentes, baseada em sistemas e apropriada para sistemas técnico-sociais complexos. Para uma fonte de risco específica, devem ser determinadas a estrutura de controle, seus controladores (atores) relevantes, seus objetivos e critérios de performance, suas capabilidades de controle devem ser avaliadas, e as informações disponíveis para eles sobre o estado atual dos sistemas em relação a objetivos de produção e limites de segurança devem ser analisados do ponto de vista da realimentação de controle. 1. Identificar controladores; 2. Objetivos de trabalho; 3. Informação do estado atual das entradas e resposta das ações de controle; 4. Capabilidade e competência dos controladores (tomadores de decisão); 5. Comprometimento: Ação dos controladores (tomadores de decisão).

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Action Error Analysis (AEA)	Rasmussen J., Taylor J. R Notes on Human Factors Problems in Process Plant Reliability and Safety Prediction, Risø-M-1894, 1976. Taylor J R. A Background to Risk Analysis, Risø National Laboratory, Denmark, 1978. Taylor,J.R., Hansen, O.M., Jensen C., Jacobsen O.F., Justesen M., Kjærgård S. Risk Analysis of a Distillation Unit, Risø-M-2319, Risoe National Laboratory, Denmark, 1982.	Action Error Analysis (AEA) analisa interações entre máquina e homens, sendo utilizado para estudar as consequências de potenciais falhas humanas na execução de tarefas relacionadas às funções automáticas de direção. Possui uma abordagem parecida com o FMEA, entretanto, é aplicado em procedimentos humanos (diferentemente de componentes e partes). Qualquer interface automática entre humanos e processos automáticos podem ser avaliadas, como controles de um cockpit, interações com equipamentos etc. Similar ao HAZOP, pode ser utilizada quando essa primeira técnica é aplicada. O método foi validado qualitativamente em um estudo realizado de 1978 a 1991, no qual um reator uretânico e uma unidade de destilação de lotes de vários produtos foram projetadas com ajuda da técnica HAZOP, Action Error Analysis e alguns outros métodos.
ALARP ALARA SFAIRP	Health Service Executive (HSE), HID'S Approach To 'As Low As Reasonably Practicable' (ALARP) Decisions, 2010. HSE, 2010b, Guidance on (ALARP) decisions in control of major accident hazards (COMAH)	O princípio ALARP declara que os riscos residuais devem ser reduzidos ao máximo até onde seja razoavelmente praticável. O termo surgiu na legislação de Saúde e Segurança no Trabalho (*Health and Safety at Work*) no Reino Unido. O método, utilizado para avaliação de risco, define faixas para a classificação dos riscos: 1. Riscos intoleráveis, que não podem ser justificados; 2. Riscos aceitáveis; 3. Riscos na faixa ALARP, onde a redução do risco deve ser realizada até onde seja praticável.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Anticipatory Failure Determination (AFD)	Kaplan, S., Visnepolschi, S., Zlotin, B. and Zusman, A. New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring. Southfield, MI: Ideation International Inc, 1999.	O método AFD é uma abordagem de identificação e análise de riscos e perigos baseado na aplicação do I-TRIZ, método russo desenvolvido para a solução de problemas e projeções derivado do estudo de padrões em invenções da literatura global de patentes. A técnica vai além das perguntas realizadas pelos métodos tradicionais, como "Como a falha ocorreu?" ou "Como essa falha pode ocorrer?", e propõe encontrar os caminhos nos casos em que os avaliadores desejassem provocar a falha. Existem dois tipos de AFD: AFD-1 e AFD-2. AFD-1 se aplica para encontrar causas para falhas que já ocorreram e o AFD-2 é uma análise de predição de falhas. Os passos do AFD-2 são descritos abaixo: Passo 1: Formulação do problema original (como encontrar todas possíveis falhas e eventos de falha do sistema nas fases aplicáveis). Passo 2: Descreve o cenário de sucesso (S0), ou seja, os resultados desejados em cada fase importante. Passo 3: Formulação do problema invertido que é criar ou produzir todos os caminhos possíveis da não ocorrência dos elementos descritos no passo 2. Passo 4: Atribuições de todas possíveis falhas que poderiam levar a ocorrência das formas de insucesso levantadas no item anterior. Devem ser separadas em três partes: eventos iniciais (initiating events - IEs), estados terminais perigosos *(harmful end states* - HESs) e estados intermediários (*mid-states* - MSs).
Barrier and operational risk analysis (BORA)	Aven, T., Sklet, S., Vinnem, J.E. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part I. Method description (2006) Journal of Hazardous Materials, 137 (2), pp. 681-691 Sklet, S., Vinnem, J.E., Aven, T. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part II: Results from a case	BORA é um método quantitativo que foi desenvolvido na Noruega para analisar os cenários de risco de liberação em instalações offshore de petróleo e gás. BORA usa redes bayesianas para ilustrar o efeito de um conjunto de fatores de influência de risco (RIFs) em falhas de barreira e outros eventos críticos. Um procedimento de pontuação e pesagem é usado para determinar quantitativamente o efeito dos vários RIFs para uma instalação específica. Embora o método BORA tenha sido desenvolvido para uma aplicação bastante restrita, seus princípios principais são relevantes em um contexto mais geral.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	study (2006) Journal of Hazardous Materials, 137 (2), pp. 692-708	
Bayesian statistics Bayesian Networks Bayesian Nets (BN) Bayes network (NB) Bayes Model Bayesian Model	Pearl, J. A constraint propagation approach to probabilistic reasoning. Proceedings of the Second Conference on Uncertainty in Artificial Intelligence, pp.357-370, 1986.	Rede Bayesiana é um modelo gráfico estatístico que representa um conjunto de variáveis ou eventos e suas relações de dependência. Os eventos são representados por nós e as conexões causais são representadas por setas. O objetivo é determinar a probabilidade de evento (resultado) a partir das probabilidades e distribuições conhecidas, sendo seguida a estatística bayesiana (atribuída ao Reverendo Thomas Bayes) cuja principal diferença em relação a estatística clássica é que todos os parâmetros das distribuições sejam fixos).
Bow tie analysis Bow-Tie method	CCPS. (2018). Bowties in risk management. Hoboken, NJ: John Wiley. CIEHF. (2016). Human factors in barrier management. Loughborough, UK: Chartered Institute of Ergonomics and Human Factors. Reason, J. (1998) Managing the Risks of Organisational Accidents, Ashgate Publishing Ltd., Aldershot. Health and Safety Executive Reports (as RR637 Research Report - Optimising hazard management by workforce engagement and supervision)	É um método de avaliação de risco que descreve e analisa os diferentes caminhos entre causas e consequências, revisando ainda os métodos de controle (barreiras para as causas e as mitigações para as consequências). Deste modo, a análise bow-tie apresenta um resumo visual de acidentes possíveis e identifica as medidas de controle dos cenários. O nome do método provém da forma do diagrama formado, onde causas são exibidas do lado direito e as consequências do lado esquerdo, unidas por um nó central, onde estará a falha sistémica ou perda de função de segurança. O método pode ser visto como uma combinação lógica de uma árvore de falha (lado direito) analisando a causa de um evento (nó) e uma árvore de eventos analisando as consequências. A origem do método é incerta, acreditando-se que tenha surgido na década de 1970. Entretanto, o grupo Shell foi a primeira grande companhia a realizar sua integração nas práticas empresariais, tendo desenvolvido o primeiro bow-tie software chamado THESIS na década de 90. Até há alguns anos, não existia nenhum guia de boas práticas com reconhecimento internacional. O Center for Chemical Process Safety (CCPS) publicou, em 2018, o primeiro guia com reconhecimento da indústria com boas práticas para conduzir e usar a análise de bow-tie nas indústrias de

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		processo, química e de gás e óleo. O *Chartered Institute of Ergonomics and Human Factors* (CIEHF) do Reino Unido publicou, em 2016, um guia de boas práticas de gerenciamento de barreiras para fatores humanos e organizacionais em geral, sendo o método bow-tie apontado em particular.
Brainstorming	Alex F. Osborn Applied Imagination. Charles Scribner's Sons. 1st edition. 317 pp. January 1, 1953.	Brainstorming é uma técnica que estimula e encoraja a conversação entre um grupo de pessoas para identificar potenciais modos de falha e perigos associados, riscos, critérios de decisão e opções de resolução de problemas. O termo foi popularizo por Alex Faickney Osborn em seu livro "*Applied Imagination*", embora já apresentasse as bases da técnica em 1948 em seu livro "Your Creative Power" (capítulo 33 - "*How to Organize a Squad to Create Ideas*"). Embora seja utilizado de forma mais genérica para representar uma discussão em grupo, verdadeiros brainstormings envolvem técnicas para tentar assegurar que a imaginação das pessoas seja despertada por pensamentos e frases de outros membros ou pré-estabelecidas. Pode ser utilizada em conjunto com outras técnicas de avaliação de risco. Dentre as evoluções nesta área, se encontra o desenvolvimento do "*Brain storm optimization (BSO)*", algoritmo de inteligência de enxame que simula a processo de brainstorming humano para diversas aplicações. As técnicas de brainstorming são geralmente utilizadas nas etapas de identificação de riscos, sendo uma técnica de suporte antes da aplicação de outras avaliações de risco.
Business impact analysis (BIA) Business impact assessment	ISO TS 22317, Societal security – Business continuity management systems – Guidelines for Business Impact Analysis, 2015. ISO 22301, Societal security – Business continuity management systems – Requirements, 2012.	Processo sistemático para determinar e avaliar os efeitos potenciais de riscos disruptivos de uma interrupção para as operações críticas como um resultado de um desastre, acidente ou emergência. O método aborda: - Identificação e criticidade dos processos chaves de negócio, funções e recursos associados e as interdependências entre as funções e processos; - Eventos disruptivos que afetarão a capacidade de atingir os objetivos de negócio; - Avaliação para recuperação da organização após a ocorrência dos eventos.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Causal Mapping Causal Map	John M. Bryson, Fran Ackermann, Colin Eden, Charles B. Finn. Visible Thinking: Unlocking Causal Mapping for Practical Business Results. Wiley, 396 pp., 2004. B. Chaib-draa. Causal maps: theory, implementation, and practical applications in multiagent environments. IEEE Transactions on Knowledge and Data Engineering, Volume: 14, Issue: 6, pp. 1201-1217, 2002.	É uma abordagem de estruturação de problemas (do inglês, *problem structuring approaches* - PSM). O método captura percepções individuais em forma de cadeia de argumentos em gráfico direto para avaliação e análise. Eventos, causas e consequências podem ser descritos no método.
Cause and consequence analysis (CCA) Cause-consequence diagrams	Nielsen, D.S. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis. Tech. Rep., Danish Atomic Energy Commission, Roskilde, Denmark, 1971.	Uma combinação de árvore de falha e árvores de eventos, incluindo atrasos de tempo, analisando causas e consequências simultaneamente. Um evento crítico é inicialmente considerado e as consequências são analisadas a partir de uma combinação de portas binárias (sim ou não) onde são descritas as condições necessárias para sua ocorrência. As causas das condições são analisadas por meio de árvores de falha (relações com portas lógicas). A técnica foi desenvolvida nos laboratórios RISO na década de 1970 para auxiliar na análise de confiabilidade de plantas nucleares nos países Escandinavos. A sua aplicação é mais comum para sistemas que onde os estados dos sistemas podem sofrer alteração com o tempo, pois ele conta com blocos de atraso.
Cause-and-effect analysis Cause-effect diagram Ishikawa Diagram Fish-bone diagram Herringbone diagram	The Cause Consequence Diagram Method as a Basis for Quantitative Accident Analysis. B. S. Nielsen, Riso-M-1374, 1971	O método modela, de forma diagramática, a sequência de eventos que podem se desenvolver em um sistema como consequência de combinações de eventos básicos. Pode ser considerado uma combinação dos métodos árvore de falha e árvore de eventos, portanto combina os métodos dedutivo (*top-down*) e indutivo (*bottom-up*).

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Cindynic Approach	Kervern, G-Y. Elements fondamentaux des cindyniques, Economica, 110 pp., 1995. Kervern, G-Y.; Boulenger, P. Cindyniques – Concepts et mode d'emploi, Economica, 102 pp., 2007.	O método considera metas, valores, regras, dados e modelos de partes interessadas e identifica inconsistências, ambiguidades e omissões. Estes formam fontes e impulsionadores dos riscos a serem avaliados.
Clinical Risk and Error Analysis (CREA)	Trucco P, Cavallin M. A quantitative approach to clinical risk assessment: The CREA method. Safety Science. 2006; 44(6). doi:10.1016/j.ssci.2006.01.003.	O CREA (*Clinical Riskand Error Analysis*) implementa não apenas uma análise quantitativa de risco dos modos de falha, mas também uma avaliação quantitativa de fatores organizacionais críticos que afetam a segurança do paciente, com base na estrutura de Vincent, fornecendo um método consistente para a integração de análise de dados e julgamento de especialistas. O CREA apresenta um nível mais alto de precisão e confiabilidade em relação aos métodos FMEA / FMECA ou HFMEA para aplicações clínicas.
Cognitive Reliability and Error Analysis Method (CREAM)	Erik Hollnagel, Cognitive Reliability and Error Analysis Method (CREAM), 1998, 287 pp.	O Método de Análise de Confiabilidade e Erro Cognitivo (CREAM) é um método HEI / HRA desenvolvido recentemente pelo autor em resposta a uma análise de abordagens de HRA existentes. CREAM pode ser usado de forma preditiva, para prever o erro humano em potencial, e retrospectivamente, para analisar e quantificar o erro. A técnica CREAM consiste em um método, um esquema de classificação e um modelo. De acordo com Hollnagel (1998), o CREAM permite ao analista atingir os seguintes objetivos: - Identificação das partes do trabalho, tarefas ou ações que requerem ou dependem da cognição humana e que, portanto, podem ser afetadas por variações na confiabilidade cognitiva; - Determinação das condições sob as quais a confiabilidade da cognição pode ser reduzida e, portanto, onde as ações podem constituir uma fonte de risco; - Fornece uma avaliação das consequências do desempenho humano na segurança do sistema, que pode ser usado em PRA / PSA;

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		- Desenvolvimento e especificação de modificações que melhorem essas condições e, portanto, sirvam para aumentar a confiabilidade da cognição e reduzir o risco. CREAM usa um modelo de cognição, o Modelo de Controle Contextual (COCOM). O COCOM se concentra em como as ações são escolhidas e assume que o grau de controle que um operador tem sobre suas ações é variável e que o grau de controle que um operador possui determina a confiabilidade de seu desempenho. O COCOM descreve quatro modos de controle, controle embaralhado, controle oportunista, controle tático e controle estratégico. De acordo com Hollnagel (1998), quando o nível de controle do operador aumenta, o mesmo ocorre com a confiabilidade de seu desempenho.
Common cause failure (CCF) analysis	IEC 62340:2007 - Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF) IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 Annex D EC 61508-7:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures Item C.6.3 L. Xing, L. Meshkat, S. Donohue. Reliability analysis of hierarchical computer-based systems subject to common-cause failures. Reliability	Falha de cause comum (CCF) é uma falha onde duas ou mais partes de um mesmo sistema falham ao mesmo tempo devido a uma mesma causa. Existem diferentes definições nas normas para a CCF. De acordo com a IEC (IEC60050), CCF corresponde a falhas de diferentes itens, resultantes de um único evento, onde essas falhas não são consequência uma da outra. De acordo com a NRC (*Nuclear Regulatory Comission*), CCF é uma falha dependente em que dois ou mais estados de falha de componentes existem simultaneamente, ou em um curto período, e são resultados diretos de uma causa compartilhada. É muito importante diferenciar falha de causa comum do termo falha de modo comum. Falhas de modo comum ocorrem quando dois componentes ou duas partes diferentes do sistema, falham da mesma maneira e com a mesma causa. Falhas de causa comum englobam as falhas de modo comum, uma vez que uma causa comum pode resultar na falha em dispositivos idênticos ou similares usados no sistema. Após a invenção das árvores de falha nos anos de 1960 nos laboratórios Bell, as falhas de modo comum tem sido foram utilizadas também durante a análise probabilística de riscos (APR) dos sistemas Apollo pela NASA, incluindo também

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	Engineering & System Safety Volume 92, Issue 3, March 2007.	Falhas de causa comum tem sido considerada na análise probabilística de risco (APR) de plantas nucleares desde o início dos anos de 1970 (NUREG-75/014, 1975). Essa indústria, desde então, tem tido um foco contínuo nas CCFs e foi umas das forças motoras para o desenvolvimento de métodos e modelos de CCF (fator beta, fator alpha, *multiple Greek letter*). A indústria da aviação também deu grande atenção para este tipo de falha; e a indústria de oléo e gás offshore, desde a década de 1980, focou nas CCFs relacionadas à avaliação de confiabilidade de sistemas instrumentados.
Concept Hazard Analysis (CHA)	Wells, G. Hazard identification and risk assessment. Institute of Chemical Engineers, 302 p., 1996.	Concept Hazard Analysis (Análise de Riscos Conceituais) identifica áreas de preocupação específica por meio de uma revisão abrangente da literatura de incidentes anteriores. É idealmente incorporado nas fases de conceito e projeto que requerem fluxograma de processo com os principais sistemas adicionais de segurança. Perigos observados devem ser combinados com soluções adequadas para mitigar ou minimizar o risco. Apresenta resultados qualitativos e sua aplicação demanda pouco tempo.
Concept Safety Review (CSR)	Wells, G., Wardman, M., Whetton, C. Preliminary Safety Analysis, Journal of Loss Prevention in the Process Industry, v6, n1, p. 47-60, 1993. Wells, G., Hazard Identification and Risk Assessment, Institution of Chemical Engineers, 1996.	É um método que pode ser aplicado durante o PSA (Preliminar Safety Analysis). Uma revisão conceitual de segurança deve ser realizada o mais rápido possível durante a fase de conceito do processo. Sua aplicação deve definir os objetivos e o escopo do projeto e identificar os principais perigos presentes. A revisão também deve estabelecer todos os critérios que a planta deve aderir para cumprir a legislação específica. Vantagens da revisão de segurança de conceito: • Boa base para estudos futuros. Este estudo identifica áreas que requerem investigação adicional no início do ciclo de vida do processo para auxiliar no desenvolvimento de uma planta mais inerentemente segura. • Auxilia na produção de um processo mais inerentemente seguro. A identificação de perigos no início do ciclo de vida do processo permite que o perigo seja eliminado ou a adição de medidas extras de segurança. Desvantagens da revisão de segurança de conceito:

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		• Revisão inicial identificando apenas perigos graves. A técnica é realizada quando apenas informações mínimas estão disponíveis e apenas os perigos graves são evidentes para os investigadores.
Cost/benefit analysis Cost-benefit analysis	HM Treasury and Government Finance Function The Green book, Appraisal and Evaluation in Central Government, 2013. Andoseh, S., Bahn, R.,Gu, J. The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects, Food Policy. 44, 10. 2013.	A análise de custo / benefício pode ser usada para avaliação de risco onde os custos totais esperados são avaliados contra os benefícios totais esperados para escolher a melhor ou mais lucrativa opção. É uma parte implícita de muitos sistemas de avaliação de risco. Pode ser qualitativo ou quantitativo ou envolver uma combinação de elementos quantitativos e qualitativos.
Cost-Of-Risk Analysis (CORA)	International Security Technology Inc (IST Inc). Managing risks using CORA, PowerPoint presentation. www.ist-usa.com, 2000. International Security Technology Inc (IST Inc). CORA: What it is, what it does, how it helps, PowerPoint presentation. http://www.ist-usa.com, 2002. International Security Technology Inc (IST Inc). A brief history of CORA, Word document. http://www.ist-usa.com, 2002. Vorster, Anita & Labuschagne, Les. (2005). A framework for comparing different information security risk analysis methodologies, pp. 95-103.	Desenvolvido pela International Security Technology, Inc. (IST), o modelo de risco CORA usa dados coletados sobre ameaças, funções e ativos, e as vulnerabilidades das funções e ativos às ameaças para calcular as consequências, ou seja, as perdas devido às ocorrências das ameaças. É uma metodologia onde os parâmetros de risco são expressos quantitativamente e onde as perdas são expressas em termos quantitativos monetários. CORA usa um processo de duas etapas para apoiar o gerenciamento de riscos. Parâmetros para ameaças, funções e os ativos são validados e refinados até que os melhores valores sejam determinados. CORA então calcula o SOL (perdas de ocorrência única, do inglês, *Single Occurrence Lossess*) e ALE (Expectativa de perdas anuais, do inglês, *Annual Loss Expectancy*), para cada uma das ameaças identificadas. Ele estima um único valor de perda para uma ameaça a uma organização e, em seguida, multiplica esse valor pela frequência da ocorrência da ameaça.
Cross Impact Analysis	Gordon, T. J., Cross Impact Method, Wayback Machine, United Nations University, Millennium Project, 1994, 18 pp. https://web.archive.org/web/20110713182749/http://www.lampsacus.com/documents/CROSSIMPACT.pdf	A análise de impacto cruzado é uma metodologia desenvolvida por Theodore Gordon e Olaf Helmer em 1966. O primeiro passo em uma análise de impacto cruzado é definir os eventos a serem incluídos no estudo. Este primeiro passo pode ser crucial para o sucesso do exercício. A maioria dos estudos inclui entre 10 e 40 eventos.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		Uma vez determinado o conjunto de eventos, o próximo passo é estimar a probabilidade inicial de cada evento. Essas probabilidades indicam a probabilidade de que cada evento ocorra em algum ano futuro. O próximo passo na análise é estimar as probabilidades condicionais. Normalmente, os impactos são estimados em resposta à pergunta: "Se o evento 'm' ocorrer, qual é a nova probabilidade do evento 'n'?" Toda a matriz de impacto cruzado é completada fazendo esta pergunta para cada combinação de evento ocorrido e evento impactado. Uma vez que a matriz de impacto cruzado foi estimada, um programa de computador é usado para realizar uma execução de calibração da matriz. Uma execução da matriz consiste em selecionar aleatoriamente um evento para teste, comparar sua probabilidade com um número aleatório para decidir sua ocorrência ou não e calcular os impactos em todos os outros eventos devido à ocorrência ou não do evento selecionado.
Decision matrix risk-assessment (DMRA)	Marhavilas, P.K., Koulouriotis, D., Gemeni, V. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009, Journal of Loss Prevention in the Process Industries, Volume 24, Issue 5, 2011, pp. 477-523. Marhavilas, P.K., Koulouriotis, D. A risk-estimation methodological framework using quantitative assessment techniques and real accidents' data: Application in an aluminum extrusion industry, Journal of Loss Prevention in the Process Industries, Volume 21, Issue 6, 2008, pp. 596-603.	A técnica de avaliação de risco de matriz de decisão (DMRA) é uma abordagem sistemática amplamente utilizada na avaliação de risco de Saúde e Segurança Ocupacional (OHS). Em uma abordagem de método de matriz típica, uma medida de valor de risco é obtida avaliando dois fatores de risco como a probabilidade de um perigo e a gravidade do perigo quando ele surge. Obtemos uma medida do valor de risco (R) pelo auxílio da relação em gravidade (S) e probabilidade (P) como: R = S * P

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Decision tree analysis	Quinlan, J. R. Induction of Decision Trees. Machine Learning, vol. 1, no. 1, 1986, pp. 81–106. Jensen, Finn B., and Thomas Graven-Nielsen. Bayesian Networks and Decision Graphs. 2001. Rokach, Lior, and Oded Maimon. Data Mining with Decision Trees: Theory and Applications. 2007.	Uma árvore de decisão tem o objetivo de representar as alternativas e as consequências em uma maneira sequencial, tendo em consideração as incertezas dos resultados. Apresenta similaridade com a árvore de eventos por iniciar com um evento iniciador ou uma decisão inicial, modelando na sequência os diversos caminhos e resultados de acordo com as diferentes decisões que devem ser feitas. Por ser uma representação visual clara dos detalhes da tomada de decisão e permitir o cálculo de probabilidades (juntamente com custos ou qualquer outro parâmetro desejado) para cada resultado, possui grande aplicabilidade para comunicação de decisões. Em contrapartida, pode levar a simplificações ou não ser viável para execução em casos muitos complexos.
Delphi Estimate-Talk-Estimate ETE	Harold A. Linstone; Helmer, O., The Delphi Method Techniques and Applications, Editora Addison-Wesley Educational Publishers Inc; 620 pp., First Edition (December 1975); Second Edition (2002), ISBN-10: 0201042932. Dalkey, N.; Helmer, O. An Experimental Application of the Delphi Method to the use of experts. Management Science. 9 (3): 458–467, 1963. Adler, Michael & Erio Ziglio (1996) Gazing Into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health, (Jessica Kingsley Publishers, 1996)	É um método estruturado para processos de previsão em que os resultados são baseados em múltiplas rodadas de questionários enviados para um quadro de especialistas. É um processo estruturado, permitindo o processo de comunicação em grupo de modo que o processo seja efetivo na solução de processo complexo, ou na identificação, avaliação de consequência e probabilidade de riscos. O processo deve ser realizado de modo anônimo pelo grupo de especialistas para evitar viés, sendo um membro externo responsável por compilar as respostas a cada etapa e enviar novamente os questionários e resultados, e permitir então o ajuste de respostas dos especialistas. O objetivo é, portanto, atingir as respostas desejadas por meio do consenso do grupo. A técnica foi concebida nos anos 1950 por Olaf Helmer e Norman Dalkey da Rand Corporations. O nome fazia referência ao Oráculo dos Delfos (Oracle of Delphi), templo que abrigava sacerdotes e sacerdotisa de Apolo, na Grécia antiga, conhecidos por suas profecias.
Event tree analysis (ETA)	IEC 62502:2010 Analysis techniques for dependability - Event tree analysis (ETA)	Análise de árvores de eventos é um procedimento indutivo para modelar os possíveis resultados obtidos a partir de um dado evento inicial, assim como para identificar e avaliar a frequência ou probabilidade dos resultados. É importante observar que o método tem a lógica binária como base, ou seja, representa sequências mutualmente exclusivas de eventos. O método foi desenvolvido durante o estudo de segurança da planta nuclear

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		WASH-1400, ao perceberem que as árvores de falha ficariam muito grandes e de difícil análise. Criaram, então, as árvores de evento para condensar a análise em um documento de melhor gerenciamento. Os principais passos para execução da técnica são: 1) Definição do sistema ou da atividade de interesse; 2) Identificação dos eventos iniciadores; 3) Identificação dos fatores de mitigação e fenômenos físicos; 4) Definição das sequências e resultados com suas quantificações; 5) Análise dos resultados; 6) Uso dos resultados da árvore de eventos. Os principais pontos positivos da técnica são: - Aplicável a todos os tipos de sistemas; - É visual e de fácil construção; - Permite a partição da árvore em diversas partes, tornando o processo menos complexo e mais gerenciável; - Permite a visualização da falha e do sucesso simultaneamente; - Análise qualitativas e quantitativas são possíveis; As principais limitações são: - Os eventos iniciais devem ser levantados anteriormente, não fazendo parte da análise; - Dependências não visíveis do sistema podem não ser avaliadas e estimativas otimistas podem ser obtidas.
External Events Analysis	Knochenhauer M., Louko P. Guidance for External Events Analysis. In: Spitzer C., Schmocker U., Dang V.N. (eds) Probabilistic Safety Assessment and Management. Springer, London, 2004. https://doi.org/10.1007/978-0-85729-410-4_241	O objetivo da Análise de Eventos Externos é analisar os eventos adversos que estão fora do sistema, operação ou processo em estudo. São eventos que podem ocorrer fora dos limites do processo e / ou podem ser o resultado de um ato malicioso ou intencional, que pode ter um impacto deletério no processo, resultando, por exemplo, em uma liberação acidental de uma substância regulamentada. Também inclui riscos internos, como inundações internas e incêndios.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Facilitated Risk Analysis and Assessment Process (FRAAP) Facilitated risk analysis process (FRAP)	Thomas R. Peltier, Facilitated Risk Analysis Process (FRAP), Available in http://ittoday.info/AIMS/DSM/85-01-21.pdf. Accessed on May 5th, 2020. Peltier Associates, "Facilitated Risk Analysis Process (FRAP)". URL: http://www.peltierassociates.com/frap.htm	O FRAP é um processo eficiente e disciplinado para garantir que os riscos relacionados à segurança da informação para as operações de negócios sejam considerados e documentados. O processo envolve a análise de um sistema, aplicativo ou segmento de operação de negócios por vez e a formação de uma equipe de indivíduos que inclui gerentes de negócios que estão familiarizados com as necessidades de informações de negócios e equipe técnica que tem uma compreensão detalhada das vulnerabilidades potenciais do sistema e controles relacionados. As sessões, que seguem uma agenda padrão, são facilitadas por um membro do escritório de projetos ou equipe de proteção de informações, que é responsável por garantir que os membros da equipe se comuniquem com eficácia e cumpram a agenda.
Failure mode effect analysis (FMEA)	IEC 60812, "Failure modes and effects analysis (FMEA and FMECA)", International Electrotechnical Commission, 2018.	A FMEA é uma técnica que identifica os modos e mecanismos de falhas com seus respectivos efeitos, abordando ainda os meios para evitar ou mitigar as falhas. É classificado como um método 'bottom-up' (indutivo) devido a ordem adotada na análise, iniciada com as possíveis falhas de componentes do sistema e avalia posteriormente seus efeitos nas funções executados pelo sistema. É um processo interativo, possuindo três tipos principais: Functional FMEA, DFMEA (design) e PFMEA (process). Foi desenvolvida inicialmente pelas Forças Armadas Americanas em 1949 para análise dos sistemas de controle de voo. Pontos positivos: - Aplicável para grande variedade de sistemas (humanos, computacionais, etc.) e processos; - Consegue antecipar problemas em fases posteriores de projetos e evita retrabalhos; - Metodologia bem-definida. Pontos negativos: - Consume bastante tempo para desenvolvimento;

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		- As versões mais simplificadas são baseadas apenas no conhecimento de especialistas, podendo não cobrir todas as possíveis falhas em sistemas complexos.
Failure mode effect and critically analysis (FMECA)	IEC 60812, "Failure modes and effects analysis (FMEA and FMECA)", International Electrotechnical Commission, 2018.	É uma variação do FMEA, sendo adicionado uma análise crítica para definir a significância de cada modo de falha. Em geral, a análise crítica pode ser baseada em uma classificação dos modos de falha em relação a severidade, ocorrência e detecção, ou então, pode ser obtida pelas taxas de falhas e de confiabilidade de cada modo. Essa análise é, portanto, geralmente qualitativa ou semiquantitativa, podendo ser quantitativa se utilizada as taxas de falha reais, embora essa abordagem seja mais incomum.
Fault Hazard Analysis Functional Hazard Analysis (FHA)	Vincoli, J.W. Fault or Functional Hazard Analysis. In Basic Guide to System Safety, J.W. Vincoli (Ed.), 2014. https://doi.org/10.1002/9781118904589.ch11	A FHA é um método dedutivo de análise que pode ser usado exclusivamente como um método qualitativo ou, se desejado, expandida para uma quantitativa. Ela requer uma investigação detalhada dos subsistemas para determinar os modos de risco do componente, as causas desses riscos e os efeitos resultantes para o subsistema e sua operação. Este tipo de análise é uma forma de uma família de análises de confiabilidade denominada análise de efeitos e modos de falha (FMEA). A principal diferença entre o FMEA / FMECA e a FHA encontra-se na profundidade da análise. Enquanto o FMEA ou FMECA analisa todas as falhas e seus efeitos, a FHA possui foco apenas nos efeitos que estão relacionados à segurança. A FHA de um subsistema é uma análise de engenharia que responde a uma série de perguntas, como: O que pode falhar? Como isso pode falhar? Com que frequência isso vai falhar? Quais são os efeitos do fracasso? Qual a importância, do ponto de vista da segurança, dos efeitos da falha? Passos: 1. O sistema é dividido em módulos (geralmente funcionais ou particionados) que podem ser manipulados efetivamente; 2. Os diagramas funcionais, esquemas e desenhos para o sistema e cada subsistema são então revisados para determinar suas inter-relações. Esta revisão pode ser feita pela preparação e uso de diagramas de blocos;

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		3. Para análises realizadas até o nível do componente, uma lista completa de componentes com suas respectivas funções é preparada para cada módulo. Para aqueles casos em que as análises devem ser realizadas no nível funcional ou de particionamento, esta lista é para o nível de análise mais baixo; 4. Estresses operacionais e ambientais que afetam o sistema são revisados; 5. Mecanismos de falhas significativas que podem ocorrer e afetar os componentes são determinados a partir de análise dos desenhos de engenharia e diagramas funcionais. Os efeitos das falhas do subsistema são então considerados; 6. Os modos de falha de componentes individuais que levariam às várias falhas possíveis os mecanismos do subsistema são então identificados. Basicamente, é a falha do componente que produz a falha de todo o sistema. No entanto, uma vez que alguns componentes podem ter mais de um modo de falha, cada modo deve ser analisado quanto ao seu efeito na montagem e, em seguida, no subsistema. Isso pode ser feito tabulando todos os modos de falha e listando os efeitos de cada um; 7. Todas as condições que afetam um componente ou montagem devem ser listadas para indicar se há períodos especiais de operação, estresse, ação pessoal ou combinações de eventos que aumentariam as probabilidades de falha ou danos; 8. A categoria de risco deve ser atribuída; 9. São listadas medidas preventivas ou corretivas para eliminar ou controlar os riscos; 10. As taxas de probabilidade iniciais são inseridas; 11. Uma análise de criticidade preliminar pode ser realizada como uma etapa final.
Fault insertion testing Fault Injection testing Implemented Fault Injection Software	Carreira, J. V., Costa, D., Silva, J. G. Fault Injection Spot-Checks Computer System Dependability, IEEE Spectrum, pp. 50–55, 1999.	A técnica de Teste de Injeção de Falha (do inglês, *Fault Insertion Testing* - FIT) é uma técnica de teste que ajuda a entender como o sistema [virtual / real] se comporta quando estressado de maneiras incomuns. Esta técnica é baseada no resultado de simulação ou experimento, portanto pode ser mais válida (ou mais próxima da realidade) em comparação com métodos estatísticos. Ela tem sido desenvolvida desde a década de 1970 quando foi utilizada para

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Implemented Fault Injection (SWIFI) Hardware Implemented Fault Injection (HWIFI) Fault Simulation for Control Systems		induzir falhas em hardware. Como uma técnica de teste não tradicional, ela desempenha um papel muito importante na melhoria da qualidade do software, eliminando falhas de software e melhorando o processo de software desenvolvimento.
Fault tree analysis (FTA)	IEC 61025 - Fault tree analysis (FTA)	É um método dedutivo que representa graficamente as condições e outros fatores que causam ou que contribuem para a ocorrência de determinados eventos, falhas ou catástrofes. O início da AAF ocorre com a definição de um evento indesejado ou uma falha, chamado de evento inicial (em inglês, top event) e determina todas as formas de sua ocorrência por meio de símbolos gráficos em um diagrama lógico, relacionando os eventos por meio de portas lógicas para estabelecer critérios de dependências entre eles. O método foi desenvolvido em 1961 pelos Laboratórios Bell Telephone quando eles estavam realizando uma avaliação de segurança, a pedido da Força Aérea Americana, para uso no sistema de controle do míssil balístico Minuteman. É um método muito versátil, permitindo a realização de análises de vários fatores de forma qualitativa ou quantitativa, podendo ser utilizada em diversos campos de aplicação. Embora seja efetiva para gerenciamentos de riscos, para sistemas mais complexos, a árvore de falhas cresce e exige grandes esforços de tempo, além de dificultar a verificação se todos os modos de falha estão cobertos.
Fine Kinney method	A. Kokangül, U. Polat, C. Dağsuyu A new approximation for risk assessment using the AHP and Fine Kinney methodologies. Saf. Sci., 91 (2017), pp. 24-32 Muhammet Gul, Busra Guven, Ali Fuat Guneri, A new Fine-Kinney-based risk assessment framework using FAHP-FVIKOR incorporation, Journal of Loss	O método Fine-Kinney é um método abrangente para avaliações quantitativas para auxiliar no controle de riscos. Tem como base o método de classificação de risco Fine-Kinney desenvolvido pela Marinha dos Estados Unidos na década de 1970. Diversas variações foram desenvolvidas ao longo do tempo. Neste método de avaliação de risco, o valor do risco é calculado considerando os parâmetros da consequência de um acidente (C), a exposição ou frequência de ocorrência de um evento de perigo que poderia levar a um acidente (E) e a probabilidade de um perigo evento (P). O método clássico Fine-Kinney tem

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	Prevention in the Process Industries, Volume 53, 2018, pp. 3-16.	uma limitação na medida em que atribui um peso igual a esses três parâmetros.
FN curves	Center for Chemical Process Safety Guidelines for Developing Quantitative Safety Risk Criteria, 2009; Wiley Online Library; ISBN:9780470261408, DOI:10.1002/9780470552940. Societal Risk: Initial briefing to Societal Risk Technical Advisory Group Prepared jointly by the Health and Safety Laboratory and the Health and Safety Executive 2009	Curvas FN são uma maneira de representar os resultados da análise de risco graficamente. O nível de risco é representado por uma linha que descreve uma faixa de valores que relacionam frequência de ocorrência (F) no eixo das ordenadas, e consequência (N) no eixo das abcissas, geralmente em escala logarítmica. Técnica muito utilizada para avaliação de riscos sociais, que expressam o risco cumulativo para grupos de pessoas que podem ser afetadas por eventos de incidentes ou acidentes.
Functional Resonance Analysis Method (FRAM)	Hollnagel, Erik. Barriers and Accident Prevention, Routledge, 242 p., 2016. Hollnagel, Erik. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems, 142 p., 2012.	FRAM é um método que utiliza os princípios e conceitos de engenharia de resiliência que descreve falhas de sistemas (eventos adversos) como um resultado da ressonância funcional vinda da variabilidade da performance normal dos sistemas, isto é, os eventos são o resultado do aumento de amplitude de uma ou mais funções devido a interação de diversas pequenas variações de partes do sistema. O método foi primeiramente descrito por Erik Hollnagel e tem sido aplicado em diversas áreas como saúde, gerenciamento de tráfico aéreo, aviação e operações marítimas.
Game Theory	Myerson, Roger B. Game Theory: Analysis of Conflict, Harvard University Press, 568p., 1991. Smith, J. M. Evolution and Theory of Games, Cambridge University Press, 234 p., 1st edition, 1982. Rosenhead, J. (Editor), Mingers, J. (Editor)	A teoria dos jogos é uma forma de modelar as consequências de diferentes decisões possíveis, dada uma série de possíveis situações futuras. As situações futuras podem ser determinadas por um tomador de decisão diferente (por exemplo, um concorrente) ou por um evento externo, como sucesso ou falha de uma tecnologia ou teste. Por exemplo, suponha que a tarefa seja determinar o preço de um produto levando em consideração as diferentes decisões que podem ser tomadas por diferentes tomadores de decisão (chamados de jogadores) em momentos diferentes. O pagamento para cada jogador envolvido no jogo, relevante para o período em questão, pode ser calculado e

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	Rational Analysis for a Problematic World Revisited: Problem Structuring Methods for Complexity, Uncertainty and Conflict, 2nd edition, Wiley, 382 p., 2001.	a estratégia com o pagamento ideal para cada jogador selecionado. A teoria dos jogos também pode ser usada para determinar o valor das informações sobre o outro jogador ou os diferentes resultados possíveis (por exemplo, sucesso de uma tecnologia).
Goal-Oriented Failure Analysis (GOFA)	International Atomic Energy Agency (IAEA) IAEA-TECDOC-856, Development of safety related expert systems, Final report of a coordinated research programme 1991-1994, 264 p., 1996.	GOFA uma técnica de identificação de perigo usando recursos selecionados do FMEA e do FTA para identificar as causas do falhas relacionadas as metas definidas, que podem ser descritas por uma declaração de intenção prescritiva para ser satisfeita pelo projetista de um sistema. Um GOFA típico é uma análise top-down usando o diagrama do sistema para identificar as causas da falha. As seguintes etapas costumam ser executadas: 1. Definição da meta de falha de um sistema; 2. Desenvolvimento de um diagrama de sistema que mostre os subsistemas e componentes; 3. Determinação dos modos de falha para cada componente em cada subsistema do diagrama do sistema; 4. Escolha de um componente para estudo detalhado; 5. Escolha de um modo de falha para este componente; 6. Identifique os mecanismos de falha para o modo de falha escolhido 7. Escolha de um mecanismo de falha; 8. Identificação das causas da falha para este mecanismo de falha. Estes podem ser externos ao diagrama do sistema ou internos se causados por outros componentes; 9. Repita as etapas acima até que todos os componentes sejam avaliados.
Hazard Analysis and Critical Control Points (HACCP)	ISO 22000:2018 Food Safety Management Systems - Requirements for Any Organization in The Food Chain	A análise de perigos e pontos críticos de controle, ou HACCP, é uma abordagem preventiva sistemática para a segurança alimentar de perigos biológicos, químicos, físicos e, mais recentemente, riscos radiológicos nos processos de produção que podem tornar o produto inseguro, com objetivo de reduzir esses riscos a um nível adequado de segurança. Desta forma, o HACCP tenta evitar perigos ao invés de tentar inspecionar os produtos acabados para avaliar os efeitos dos riscos existentes. Princípio 1: Conduzir uma análise de perigos;

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		Princípio 2: Determinar os pontos críticos de controle (CCP's); Princípio 3: Estabelecer limites críticos; Princípio 4: Estabelecer procedimentos de monitoramento; Princípio 5: Estabelecer ações corretivas; Princípio 6: Estabelecer procedimentos de verificação; Princípio 7: Estabelecer procedimentos de documentação e manutenção de histórico. [https://www.fda.gov/food/hazard-analysis-critical-control-point-haccp/haccp-principles-application-guidelines]
Hazard and Operability studies (HAZOP)	IEC 61882:2016 Hazard and operability studies (HAZOP studies) - Application guide	HAZOP é avaliação estruturada e sistemática de produtos, processos, procedimentos ou sistemas. É uma análise qualitativa que tem como base o uso de palavras chaves (guide words) que questionam como as condições de projeto ou de operação podem não ser alcançadas em cada etapa do sistema ou processo avaliado. É uma técnica semelhante ao FMEA, porém se diferencia pois o time de analistas iniciará o procedimento buscando por variações e resultados indesejados a partir dos resultados esperados. Foi desenvolvido por Bert Lawley, inventor do HAZOP, que publicou seus primeiros resultados em 1976. Inicialmente foi desenvolvida para sistemas que envolvem o tratamento de um meio fluido ou outro fluxo de material nas indústrias de processo, porém possui aplicações diversas. Embora seja uma técnica de fácil aplicação e bastante útil para detectar fraquezas em sistemas, possui algumas limitações que incluem a falta de garantia de identificação de todas as fontes de risco, não possuir abordagem para identificação de riscos provenientes de interação das partes do sistema ou processo, e depender diretamente do conhecimento da equipe de análise.
Hazard Identification and Ranking (HIRA)	Khan, F.I., Abbasi, S.A. Multivariate Hazard Identification and Ranking System, Process Safety Progress, 17 (3), pp. 157-170, 1998.	HIRA é um termo coletivo que abrange todas as atividades envolvidas na identificação de perigos e avaliação de riscos nas instalações, ao longo de seu ciclo de vida, para garantir que os riscos aos funcionários, ao público ou ao meio ambiente sejam controlados de forma consistente dentro da tolerância ao risco da organização. Esses estudos geralmente abordam três questões de risco principais em um nível de detalhe compatível com os objetivos da

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		análise, estágio do ciclo de vida, informações disponíveis e recursos, sendo elas: Perigo -O que pode dar errado? Consequências - O quão ruim poderia ser? Probabilidade - Com que frequência isso pode acontecer?
Hazardous Scenario Analysis (HAZSCAN) Hazard identification (HAZID)	Crawley, F. Offshore loss prevention, Chemical Engineer, 592, pp. 24-25, 1995. Frank Crawley, 5 - HAZID, Editor(s): Frank Crawley, A Guide to Hazard Identification Methods (Second Edition), Elsevier, pp. 37-48, 2020 ISBN 9780128195437	O método de avaliação de risco HAZID (Identificação de Perigos) ou HAZSCAN (Análise de Cenários Perigosos) são mais adequados para as fases iniciais do projeto, onde são identificados os perigos mais significativos, bem como os problemas que podem afetar o projeto. O HAZID originou-se do HAZOP e era originalmente conhecido como '3D HAZOP', pois o principal objetivo, naquela época, era determinar a interação de potenciais 'riscos' em um espaço tridimensional típico de instalações offshore. Após 4 anos de evolução, tornou-se conhecido como HAZID. Enquanto o HAZOP é impulsionado pela 'causa', HAZID é conduzido pela 'consequência'. Tal como acontece com as novas técnicas, levou tempo e uso para desenvolvê-lo em todo o potencial. Inicialmente, era baseado em uma matriz HAZID, que tinha três tópicos: Efeito, Para / Sobre e Causa.
Hierarchical Task Analysis (HTA) Hierarchical Task Network (HTN)	Stanton, N.A., Hierarchical task analysis: Developments, applications, and extensions, Applied Ergonomics, 37 (1 SPEC. ISS.), pp. 55-79, 2006.	A Análise Hierárquica de Tarefas tem disso utilizada desde a década de 1960 ou mesmo antes. É mais adequada para analisar tarefas que têm uma estrutura bem definida - ou seja, tarefas que tendem a ser executadas de maneira semelhante todas as vezes (sem estrutura muito flexível). A HTA envolve a descrição da tarefa em termos de uma hierarquia tarefa-subtarefa e um conjunto de planos que definem em que ordem as subtarefas podem ser executadas ou sob que circunstâncias determinadas subtarefas são executadas.
Human Error Assessment and Reduction Technique (HEART)	Williams, J.C. HEART – A Proposed Method for Achieving High Reliability in Process Operation by means of Human Factors Engineering Technology. In Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society, 16 September 1985, Southport.	A Técnica de Avaliação e Redução de Erro Humano (do inglês, *Human Error Assessment and Reduction Technique* – HEART) é um método de avaliação de confiabilidade humana (ACH) que tem como base a literatura de performance humana para o desenvolvimento de tarefas. No HEART, a probabilidade de erros humanos é definida com base na: - Classificação das tarefas a serem desenvolvidas em nove grandes grupos (Tipos Genéricos de Tarefas, do inglês, *Generic Task Types* – GTTs), sendo

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	Williams, J.C. A proposed Method for Assessing and Reducing Human error. In Proceedings of the 9th Advance in Reliability Technology Symposium, University of Bradford, pp. B3/R/1 – B3/R/13, 1986.	cada uma delas relacionada a um Potencial de Erro Humano (do inglês, *Human Error Potential* – HEP); - Identificação das condições que podem influenciar na produção de erros (*Error-Producing Conditions* – EPCs), sendo essas já estabelecidas em lista pré-definida com 38 condições. A técnica foi desenvolvida na década de 1980 por J. C. Williams, sendo lançada em 1985, quando este publicou um artigo com seus resultados iniciais, enquanto trabalhava no Corpo de Geração Central de Energia do Reino Unido.
Human Factor Event Analysis (HFEA)	Yang, D., Liu, H. Application of THERP HCR model for valve overhaul in nuclear power plant, AIP Conference Proceedings, 1839, art. no. 020045, 2017. Zhang, L., Huang, S.-D., Huang, X.-R. THERP+HCR-based model for human factor event analysis and its application, Hedongli Gongcheng / Nuclear Power Engineering, 24 (3), pp. 272-276, 2003.	A análise de evento de fator humano (HFEA) é utilizada para a avaliação da confiabilidade do sistema, especialmente para a avaliação probabilística de risco (PRA) em usinas nucleares. Existem dois métodos analíticos, THERP (Técnica para Predição da Taxa de Erro Humano) e HCR (Confiabilidade Cognitiva Humana), que geralmente são usados separadamente no HFEA. Esses métodos têm seus próprios recursos. O método HCR é melhor para determinar erros humanos durante o estágio de diagnóstico de um acidente, enquanto o THERP fornece um modelo de árvore de eventos humanos e uma grande quantidade de dados para determinar erros operacionais de pessoal. Como existem duas fases, ou seja, diagnósticos e manipulações em um evento de fator humano, é necessário que o THERP com HCR seja integrado em um novo modelo de HFEA.
Human Factors Analysis and Classification System (HFACS)	Wiegmann, D.A., Shappell, S.A. A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System, Ashgate Publishing, pp. 1-165, 2012. Wiegmann, D.A., Shappell, S.A. Human error analysis of commercial aviation accidents: Application of the human factors analysis and	O Sistema de Análise e Classificação de Fatores Humanos (HFACS) foi desenvolvido pelo Dr. Scott Shappell e pelo Dr. Doug Wiegmann. É uma ampla estrutura de avaliação de erro humano, tendo sido originalmente utilizada pela Força Aérea dos Estados Unidos para investigar e analisar aspectos de fatores humanos da aviação.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	classification system (HFACS), Aviation Space and Environmental Medicine, 72 (11), pp. 1006-1016, 2001. Shappell, S.A., Wiegmann, D.A. Applying Reason: The human factors analysis and classification system (HFACS), Human Factors and Aerospace Safety: An International Journal: No.1, 1, pp. 59-86, 2017.	
Incident Review (based on Incident Reporting / Incident Report)	Carl Macrae, Analyzing Near-Miss Events: Risk Management in Incident Reporting and Investigation Systems, Centre for Analysis of Risk and Regulation at the London School of Economics and Political Science, Londres, 2007.	Um relatório de incidente é uma ferramenta que documenta qualquer evento que pode ou não ter causado ferimentos a uma pessoa ou danos a um ativo da empresa. Ele é usado para capturar lesões e acidentes, quase acidentes, danos materiais e equipamentos, questões de saúde e segurança, quebras de segurança e más condutas no local de trabalho. Um relatório de incidente pode ser usado na investigação e análise de um evento. Inclui a causa raiz e as ações corretivas para eliminar os riscos envolvidos e evitar ocorrências futuras semelhantes. Os relatórios de incidentes também podem ser usados como documentos de segurança que indicam riscos potenciais e perigos não controlados encontrados no local de trabalho.
Layer of protection analysis (LOPA) Barrier Analysis	IEC 61508 (all parts): 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems, Ed. 2.0 IEC 61511 (all parts): 2016 Functional safety – Safety instrumented systems for the process industry sector, Ed. 2.0	A análise de camadas de proteção (LOPA) é um método semi-qualitativo que tem como objetivo avaliar as medidas de proteção para os pares de causas e consequências para sistemas e equipamentos. A LOPA embora possua uma abordagem numérica, essa abordagem é simplificada, sendo um método localizado entre o HAZOP e uma análise quantitativa de risco. O método tem como objetivo evitar que riscos com consequências indesejadas possam ocorrer com frequência maior do que as frequências permitidas. Sendo assim, o método costuma ser aplicadas em indústrias que possuem alvos específicos de risco para atingir ou que desejam reduzir riscos até onde seja razoável na prática de projetos (ALARP). LOPA fornece ainda a base para a determinação dos níveis de integridade de segurança para sistemas instrumentados, como definido na série de normas IEC 61508 e IEC 61511.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		Pode ser utilizada ainda para ajudar na alocação efetiva dos recursos de redução de risco.
Markov analysis	IEC 61165:2006 Application of Markov techniques	A análise de Markov é uma técnica utilizada para análise de confiabilidade, segurança e disponibilidade de sistemas, utilizando diagramas de transição de estado. Realiza a modelagem do comportamento de sistemas em relação ao tempo, sendo que nesses sistemas o estado futuro depende apenas do estado presente. A técnica ganhou esse nome devido ao matemático russo Andrei Andreyevich Markov, pioneiro no estudo de processos estocásticos.
Master Logic Diagram	I.A Papazoglou, O.N Aneziris Master Logic Diagram: method for hazard and initiating event identification in process plants, Journal of Hazardous Materials, Volume 97, Issues 1–3, pp.11-30, 2003, ISSN 0304-3894.	MLD é um diagrama lógico que se assemelha a uma árvore de falhas, mas sem as propriedades matemáticas formais da última. O MLD começa com um Evento Principal “Perda de Contenção” e o decompõe em eventos de contribuição mais simples
Maximum Credible Accident Analysis (MCAA)	Khan, F.I., Abbasi, S. A criterion for developing credible accident scenarios for risk assessment, Journal of Loss Prevention in the Process Industries, 15 (6), pp. 467-475, 2002.	A análise de acidentes máximos credíveis é realizada para encontrar a distância de perigo para o pior cenário. O Acidente Máximo Credível (MCA) é um acidente provável com distância máxima de dano. Na prática, a seleção de cenários de acidentes para MCAA é realizada com base no julgamento de engenharia e na análise de acidentes anteriores. O MCAA não inclui a quantificação da probabilidade de ocorrência de um acidente. O risco envolve a ocorrência potencial de algum acidente consistindo em um evento ou sequência de eventos. A liberação acidental de óleo e gás para a atmosfera de um poço ou equipamento de processamento é estudada por meio da visualização de cenários com base em suas propriedades e os impactos são calculados em termos de distâncias de danos. Uma situação desastrosa é o resultado de incêndio ou explosão do gás liberado, além de outras causas naturais, o que eventualmente leva à perda de vidas, danos ao desequilíbrio

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		patrimonial e / ou ecológico. Dependendo dos atributos de perigo efetivos e seus impactos, o efeito máximo para os arredores pode ser avaliado.
OMethod Organised Systematic Analysis of Risk (MOSAR - Méthode Organisée et Systémique d'Analyse de Risques)	Perilhon, P., MOSAR: Présentation de la méthode, Technique de l'Ingénieur, traité, sécurité et gestion des risques, article SE 4060, 2000. Ayrault, N., Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs (DRA-039), Rapport Oméga 10 – Evaluation des barrières techniques de sécurité, INERIS, France, 2005.	O método MOSAR (do francês, *Méthode Organisée et Systémique d'Analyse de Risques*) foi desenvolvido por uma equipe de especialistas do *Institute National des Sciences et Techniques Nucléaires* (INSTN CEA Grenoble). Trata-se de uma estrutura de dez etapas para o exame de segurança. O MOSAR avalia uma variedade de subsistemas em interação e as tabelas são fornecidas pela equipe de avaliação. Devem ser realizadas: - Identificação de perigo; - Adequação da Prevenção; - Interdependência; - Estudo de segurança operacional usando FMEA ou HAZOP; - Árvores Lógicas; - Tabela de Gravidade; - Vinculando a gravidade com os objetivos de proteção; - Barreiras tecnológicas (sem barreiras humanas); - Barreiras de utilização (incluindo intervenção humana); - Tabela de aceitabilidade para risco residual.
Monte Carlo	ISO/IEC Guide 98-3:2008/Suppl 1 Uncertainty of measurement – Part 3: Guide to the expression of uncertainty in measurement (GUM 1995) – Propagation of distributions using a Monte Carlo method	Método estatístico que permite a geração de resultados numéricos a partir da utilização de amostragens massivas de distribuições (mesmo nos casos para distribuições com formatos conhecidos), em geral, para modelos em que não é possível ou viável obter uma solução analítica. Podem utilizados na análise de risco para a propagação de incertezas em modelos analíticos ou cálculos probabilísticos quando técnicas analíticas não são possíveis.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Normal Accident Theory (NAT)	Perrow, Charles. Normal Accidents: Living with High-Risk Technologies, Basic Books, 1st ed., 386 pp., 1984.	"*Normal Accidents: Living with High-Risk Technologies*" é um livro de 1984 do sociólogo de Yale Charles Perrow, que fornece uma análise detalhada de sistemas complexos de uma perspectiva sociológica. Foi o primeiro a "propor um quadro de caracterização de sistemas tecnológicos complexos como o tráfego aéreo, o tráfego marítimo, as centrais químicas, as barragens e, sobretudo, as centrais nucleares de acordo com o seu risco". Perrow argumenta que falhas múltiplas e inesperadas são incorporadas aos sistemas complexos e fortemente acoplados da sociedade. Esses acidentes são inevitáveis e não podem ser planejados. O argumento de Perrow, baseado em características sistêmicas e erro humano, é que grandes acidentes tendem a aumentar, e a tecnologia não é o problema, mas as organizações. Cada um desses princípios ainda é relevante hoje. O primeiro passo é reduzir a complexidade onde quer que ela possa ser encontrada. A segunda etapa é garantir que, onde houver um acoplamento acelerado, os sistemas projetados para gerenciá-lo possam reagir a uma velocidade semelhante a qualquer incidente em potencial.
Nuclear Action Reliability Assessment (NARA)	B. Kirwan, H. Gibson, R. Kennedy, J. Edmunds, G. Cooksley e I. Umbers, Nuclear action reliability assessment (NARA): a data-based HRA tool, Safety and Reliability, vol. 25, pp. 38-45, 2005. J. Bell e J. Holroyd, Review of human reliability assessment methods, HSE Books, 2009.	O método NARA é uma versão específica do HEART para a área nuclear, que foi desenvolvido, em 2005, para atender as necessidades das avaliações probabilísticas de segurança das plantas nucleares no Reino Unido, sendo uma ferramenta de propriedade da companhia British Energy.
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)	Christopher J. Alberts, Sandra Behrens, Richard D. Pethia, William R. Wilson Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0, Technical report, 1999.	A abordagem de Avaliação de Ameaça, Ativo e Vulnerabilidade Operacionalmente Crítica (OCTAVE®) foi desenvolvido em 2001 na Carnegie Mellon University (CMU), para o Departamento de Defesa dos Estados Unidos e define uma avaliação estratégica baseada em riscos e uma técnica de planejamento para segurança. OCTAVE é uma abordagem autodirigida, o que significa que as pessoas de uma organização assumem a

Método	Referências Principais / Abordagens Iniciais	Breve descrição
	Christopher J. Alberts and Audrey Dorofee. Managing Information Security Risks: The Octave Approach, Addison-Wesley Longman Publishing Co., Inc., USA. 471 pp., 2002.	responsabilidade por definir a estratégia de segurança da organização. OCTAVE-S é uma variação da abordagem adaptada aos meios limitados e às restrições exclusivas normalmente encontradas em pequenas organizações (menos de 100 pessoas). OCTAVE-S é liderado por uma pequena equipe interdisciplinar (três a cinco pessoas) do pessoal de uma organização que coleta e analisa informações, produzindo uma estratégia de proteção e planos de mitigação com base nos riscos de segurança operacional exclusivos da organização. Para conduzir OCTAVE-S de forma eficaz, a equipe deve ter amplo conhecimento dos processos de negócios e segurança da organização, para que seja capaz de conduzir todas as atividades por conta própria.
Optimal Risk Assessment (ORA)	Khan, F.I. and Abbasi, S.A. Risk Assessment in Chemical Process Industries: Advance Techniques, Discoverv Publishing House, India, 376 pp, 1998. Khan, F.I. and S.A. Abbasi, Techniques for Risk Analysis of Chemical Process Industries, Journal of Loss Prevention in Process Industries, 11 (21, pp. 91-102, 1998.	ORA foi criado para ser utilizado na indústria petroquímica como um framework para a avaliação de risco, envolvendo quatro etapas: i) identificação de perigo e triagem; ii) avaliação de risco (ambos qualitativos e probabilística); iii) quantificação de perigos ou análise de consequências; e iv) estimativa de risco.
Petri Nets (or Time Petri Nets)	IEC 62551:2012 Analysis techniques for dependability - Petri net techniques	Redes de Petri são uma ferramenta gráfica para a representação e análises de interações entre componentes e eventos de um sistema. Nelas são representados: - Lugares (usualmente representados como círculos) que representam as condições em que o sistema pode ser encontrado; - Transições (representados por barras) que representam os eventos que podem mudar de uma condição para outra; - Arcos (representados por setas) que conectam lugares a transições e transições a lugares e representam conexões lógicas admissíveis entre condições e eventos. Além de oferecerem uma notação gráfica como em outras linguagens industriais, as redes de Petri possuem uma teoria matemática bem desenvolvida para análise de processos.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Predictive, Epistemic Approach (PEA)	Apeland, S., Aven, T., Nilsen, T., Quantifying uncertainty under a predictive, epistemic approach to risk analysis, Reliability Engineering and System Safety, 75 (1), pp. 93-102, 2002.	Na PEA, o foco está em prever as quantidades observáveis, como, por exemplo, a ocorrência ou não de um evento acidental, ou o número de natalidade ou a magnitude da perda financeira em um período de tempo. Quantidades observáveis expressam estados do `mundo ', ou seja, quantidades da realidade física ou da natureza; eles são desconhecidos no momento da análise, mas se tornarão (ou poderão se tornar) conhecidos no futuro.
Preliminary Hazard Analysis (PHA) Primary hazard analysis	Military Standard - Department of Defense MIL-STD882 - System Safety Program Requirements, USA, 1969.	A análise preliminar de risco (PHA) é um método indutivo simples de análise semiquantitativa cujo objetivos são: 1. Identificar todos os perigos potenciais e eventos acidentais que podem levar a um acidente; 2. Classificar os eventos acidentais identificados de acordo com seus gravidade; 3. Identifique os controles de perigo necessários e ações de acompanhamento. Diversas variantes de PHA são usadas, com diferentes nomes como: - Classificação rápida de risco; - Identificação de perigo (HAZID).
Rapid Risk Analysis Based Design (RRABD) Rapid Risk Assessment (RRA)	European Centre for Disease Prevention and Control (ECDC) Operational guidance on rapid risk assessment methodology, 2011, 68 pp.	A análise / avaliação rápida de risco (RRA) típica leva cerca de 30 minutos. Não é uma revisão de segurança, um modelo de ameaça completo, uma avaliação de vulnerabilidade ou uma auditoria. No entanto, esses tipos de atividades podem seguir um RRA, se considerado apropriado ou necessário. O principal objetivo do RRA é compreender o valor e o impacto de um serviço na reputação, finanças, produtividade do projeto ou negócio. Baseia-se nos dados processados, armazenados ou simplesmente acessíveis pelos serviços. Observe que o RRA não se concentra em enumerar e analisar os controles de segurança. O processo RRA se destina a analisar e avaliar serviços, não processos ou controles individuais.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Reliability block diagrams (RBD) Dependence diagram (DD)	IEC 61078:2016 Reliability block diagrams	É uma técnica para modelagem do conjunto de eventos que devem ser realizados ou condições que devem ser preenchidas para operação correta de um sistema ou tarefa. RBDs podem ser convertidos em árvores de falha e são semelhantes a análise de Markov, entretanto RBDs são devem ser utilizados para modelos que apresentam dependência de ordem ou de tempo, sendo outros métodos devem ser utilizados (Markov ou redes de Petri, por exemplo). Para sua realização deve-se considerar seus princípios básicos: apenas dois estados são permitidos aos blocos (em operação e falha ou em reparação); a falha de um bloco não pode afetar a probabilidade de falha de outro bloco modelado no sistema.
Reliability centred maintenance	IEC 60300-3-11 Ed. 2.0 b:2009 Dependability Management - Part 3-11: Application Guide - Reliability Centred Maintenance	A Manutenção Centrada na Confiabilidade (Reliability Centred maintenance - RCM) é um método para identificar as políticas que deveriam ser implementadas para gerenciar falhas para atender de modo eficiente e efetivo os requisitos de segurança, disponibilidade e econômicos das operações de todos os tipos de equipamento. É uma metodologia aprovada, reconhecida e utilizada em uma grande gama de indústrias. Esforços para entender os padrões de falha de componentes de aeronaves não estruturais levaram a Stanley Nowlan e a Howard Heap, ambos da United Airlines, a desenvolver uma nova abordagem para manutenção. Eles documentaram sua metodologia para desenvolver políticas de gerenciamento de consequências de falhas em um relatório publicado pelo Departamento de Defesa dos EUA em 1978.
Risk and Vulnerability analysis (RVA)	Financial Supervisory Authority of Norway Risk and Vulnerability Analysis (RVA) 2020, 82 pp., 2020.	A análise de risco e vulnerabilidade (RVA) pode beneficiar o processo de prevenção e preparação para desastres, tanto ao gerar uma base para a tomada de decisões quanto ao aumentar a consciência de risco, a cultura de segurança e a capacidade de resposta por meio do próprio processo de RVA.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Risk indices Risk Level Indicators (RLI) Key Risk Indicators (KRIs)	MacKenzie, C.A. Summarizing Risk Using Risk Measures and Risk Indices. Risk Analysis, 34: 2143-2162, 2014. https://doi.org/10.1111/risa.12220	Um índice de risco é uma medida semiquantitativa de risco que é uma estimativa derivada de uma abordagem de pontuação usando escalas ordinais. Os índices de risco podem ser usados para classificar uma série de riscos usando critérios semelhantes para que possam ser comparados. As pontuações são aplicadas a cada componente de risco, por exemplo, características do contaminante (fontes), a gama de possíveis vias de exposição e o impacto nos receptores. Os índices de risco são essencialmente uma abordagem qualitativa para classificar e comparar riscos. Embora os números sejam usados, isso é simplesmente para permitir a manipulação. Em muitos casos em que o modelo ou sistema subjacente não é bem conhecido ou não pode ser representado, é melhor usar uma abordagem mais abertamente qualitativa.
Risk-based Maintenance (RBM)	Arunraj, N.S., Maiti, J. Risk-based maintenance—Techniques and applications, Journal of Hazardous Materials, Volume 142, Issue 3, 2007, pp. 653-661. Faisal I. Khan, Mahmoud M. Haddara Risk-based maintenance (RBM): a quantitative approach for maintenance/inspection scheduling and planning, Journal of Loss Prevention in the Process Industries, Volume 16, Issue 6, 2003, pp. 561-573.	A manutenção baseada em risco (RBM) prioriza os recursos de manutenção em relação aos ativos que apresentam maior risco caso venham a falhar. É uma metodologia para determinar o uso mais econômico dos recursos de manutenção. Isso é feito para que o esforço de manutenção em uma instalação seja otimizado para minimizar qualquer risco de falha. Uma estratégia de manutenção baseada em risco é baseada em duas fases principais: - Avaliação de risco; - Planejamento de manutenção com base no risco. O tipo e a frequência da manutenção são priorizados com base no risco de falha. Os ativos que apresentam maior risco e consequência de falha são mantidos e monitorados com mais frequência. Os ativos que apresentam um risco menor estão sujeitos a programas de manutenção menos rigorosos. Implementar um processo de manutenção baseado em risco significa que o risco total de falha é minimizado em toda a instalação da maneira mais econômica.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Scenario analysis Scenario-based design	Ringland, G. Scenarios in business, Wiley, 288 pp., 2002. Van der Heijden, K. Scenarios: The art of strategic conversation, Wiley, 384 pp., 2011 Chermack, Thomas J. Scenario planning in organizations: How to Create, Use, and Assess Scenarios, Berrett-Koehler, 272 pp., 2011.	Análise de cenário é o nome dado a uma série de técnicas que envolvem o desenvolvimento de modelos de como o futuro pode ser. Em termos gerais, consiste em definir um cenário plausível e trabalhar o que pode acontecer, dados os vários desenvolvimentos futuros possíveis. Para escalas de tempo relativamente curtas, pode envolver a extrapolação do que aconteceu no passado. Para escalas de tempo mais longas, a análise de cenário pode envolver a construção de um cenário imaginário, mas confiável, e então explorar a natureza dos riscos dentro desse cenário. É mais frequentemente aplicado por um grupo de partes interessadas com diferentes interesses e especialidades. A análise de cenário envolve a definição de alguns detalhes do cenário ou cenários a serem considerados e a exploração das implicações do cenário e do risco associado.
SEQHAZ Hazard Mapping	Björkhem, D. HAZOP and SEQHAZ® methods as input data producers to Safety Integrity Level evaluations, Report 5250, ISSN: 1402-3504, 111 pp., 2008. E. Korjusiommi, R. Salo, R. Taylor Hazard analysis for batch processes and for special operations, In proceeding from 9th International Symposium Loss Prevention and Safety Promotion in the Process Industries, 422-431, 1998.	O método foi desenvolvido em 1995-1997 pela *Neste Engineering* (atualmente *Neste Jacobs*) em um projeto especial que foi realizado em cooperação com a Neste Oil Oyj, a Neste Chemicals Division e o Instituto Dinamarquês de Análise de Sistemas Técnicos. SEQHAZ® é aplicável a todos os tipos de objetos industriais e pode ser modificado para se adequar a outros tipos de sistemas também. Ele serve melhor como uma análise preliminar de risco no projeto conceitual ou básico, ou como um método grosseiro para objetos de médio ou baixo risco. Ele também se mostrou adequado para objetos de alto risco, quando o objetivo é obter um amplo entendimento dos riscos. Se houver experiência operacional considerável disponível, o método também se adequa a uma análise detalhada de projeto de objetos de alto risco.
Sequentially Timed Event Plotting (STEP)	Hendrick K., Benner L. Investigating accidents with STEP, Ed. M. Dekker, New York/Basel, 454 pp. 1986.	A técnica STEP fornece uma reconstrução do processo traçando a sequência de eventos e ações que contribuíram para o acidente. Os principais conceitos no STEP são a iniciação do acidente por meio de um evento ou mudança que interrompeu o sistema, os agentes que intervêm para controlar o sistema (por exemplo, equipamentos, sistemas de monitoramento, trabalhadores, controladores automáticos) e os "blocos de construção de eventos" elementares". O acidente é comumente desenvolvido em diferentes planos (eventos multilineares) que se referem a diferentes agentes e situações

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		simultâneas; sendo todos os eventos logicamente conectados durante o processo.
Sneak circuit analysis Sneak Analysis	Ericson, Clifton A. Hazard Analysis Techniques for System Safety, Wiley, 499 pp., 2005. Savakoor, Devyani S., Bowles, John B., Bonnell, Ronald D. Combining sneak circuit analysis and failure modes and effects analysis, Proceedings of the Annual Reliability and Maintainability Symposium, pp. 199-205, 1993. Rankin, John P. Sneak-Circuit Analysis, Nuclear Safety, 14 (5), pp. 461-469, 1973.	É uma metodologia para identificar erros de projeto. Uma condição furtiva (*sneak condition)* é uma condição latente de hardware, software ou condição integrada que pode fazer com que um evento indesejado ocorra ou pode inibir um evento desejado e não é causado por falha de componente. Essas condições são caracterizadas por sua natureza aleatória e capacidade de escapar da detecção durante os mais rigorosos testes de sistema padronizados. Condições furtivas podem causar operação inadequada, perda de disponibilidade do sistema, atrasos no programa ou mesmo morte ou ferimentos ao pessoal. Foi desenvolvido pela NASA nos anos de 1960 para verificação da integridade e funcionalidade dos seus projetos.
Structured « What if? » (SWIFT)	Card, Alan J., et al. Beyond FMEA: The Structured What-If Technique (SWIFT), Journal of Healthcare Risk Management, vol. 31, no. 4, pp. 23–29, 2012.	É um tipo de método estruturado de brainstorming similar ao HAZOP. Utiliza palavras-chaves ou títulos em combinação de questões levantadas pelos participantes (geralmente iniciadas com "E se..." ou "Como poderíamos...") para explorar o comportamento de sistemas e identificar e analisar perigos e riscos. Geralmente é suportado por listas de verificação para evitar que sejam negligenciados riscos ou perigos, e pode ser estendido em uma análise DELPHI. Não há uma abordagem padrão para o SWIFT (embora alguns artigos científicos indiquem possíveis abordagens), sendo flexível para utilização em diversas áreas de aplicação.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Structured or semi-structured interviews	Harrell, M.C., Bradley, M.A. Data Collection Methods: Semi-Structured Interviews and Focus Groups. Santa Monica, CA: RAND Corporation, 2009. Gill, J., Johnson, P. Research methods for managers, SAGE Publications Ltd, 288 pp., 2010.	Em uma entrevista estruturada, os entrevistados individuais respondem a um conjunto de perguntas preparadas. Uma entrevista semiestruturada é semelhante, mas permite mais liberdade para uma conversa para explorar os problemas que surgem. Em uma entrevista semiestruturada, a oportunidade é explicitamente fornecida para explorar áreas que o entrevistado pode desejar cobrir. As perguntas devem ser abertas sempre que possível, simples e em linguagem apropriada para o entrevistado, e cada pergunta deve abranger apenas um assunto. Possíveis perguntas de acompanhamento para buscar esclarecimentos também são preparadas.
Success Likelihood Index Methodology Success Likelihood Index Method (SLIM)	Embrey, D.E., Humphreys, P.C., Rosa, E.A., Kirwan, B., Rea, K. SLIM-MAUD: An approach to assessing human error probabilities using structured expert judgement, NUREG/CR-3518. US Nuclear Regulatory Commission: Washington D.C., 1984. Shokoufeh Abrishami, Nima Khakzad, Seyed Mahmoud Hosseini, Pieter van Gelder BN-SLIM: A Bayesian Network methodology for human reliability assessment based on Success Likelihood Index Method (SLIM), Reliability Engineering & System Safety, Volume 193, 2020.	O Método do Índice de Probabilidade de Sucesso (SLIM) é uma técnica utilizada na área de Avaliação da Confiabilidade Humana (HRA), com o objetivo de avaliar a probabilidade de ocorrência de um erro humano ao longo da realização de uma tarefa específica. A partir de tais análises, medidas podem ser tomadas para reduzir a probabilidade de falhas ocorridas dentro de um sistema e, portanto, levar a uma melhoria nos níveis gerais de segurança. A técnica consiste em dois módulos: MAUD (decomposição de utilidade multi-atributo), que dimensiona a probabilidade relativa de sucesso na execução de uma série de tarefas, dados os PSFs que provavelmente afetam o desempenho humano; e SARAH (Abordagem Sistemática para a Avaliação de Confiabilidade de Humanos), que calibra essas pontuações de sucesso com tarefas com valores HEP conhecidos, para fornecer um número geral.
Swiss Cheese Model (SCM) SCM-based model Reason Model	Reason J. Human error: models and management, BMJ (Clinical research ed.), vol. 320, pp. 768–70, 2000.	O modelo do queijo suíço é uma ferramenta de avaliação e gerenciamento de riscos que oferece um entendimento profundo de camadas de proteção. Entende-se por uma camada de proteção, uma ação preventiva que reduz a chance de um acidente ocorrer ou uma ação de mitigação que diminua a severidade de um acidente. O nome da técnica tem origem ao se relacionar os sistemas humanos a múltiplas fatias de queijo suíço, empilhados lado a lado. Nessa comparação, cada fatia representa uma camada de proteção do sistema e as aberturas no queijo são as fragilidades do sistema. Para a ocorrência de ume evento indesejado, é necessário o alinhamento das fragilidades de cada

Método	Referências Principais / Abordagens Iniciais	Breve descrição
		uma das camadas de proteção. O método é também conhecido por modelo de Reason, devido ao nome do seu criador.
System Hazard Identification, Prediction and Prevention (SHIPP)	Samith Rathnayaka, Faisal Khan, Paul Amyotte, "SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description", Process Safety and Environmental Protection, Volume 89, Issue 3, 2011, pp. 151-164. Samith Rathnayaka, Faisal Khan, Paul Amyotte, "SHIPP methodology: Predictive accident modeling approach. Part II. Validation with case study", Process Safety and Environmental Protection, Volume 89, Issue 2, 2011, pp. 75-88.	O SHIPP é uma metodologia sistemática para identificar, avaliar e modelar o processo de acidentes passados, prevendo e prevenindo futuros acidentes em uma instalação de processo. Nesta metodologia, os riscos relacionados a acidentes do processo são modelados usando barreiras de segurança. O modelo tem como base o histórico do processo, as informações do precursor do acidente e na modelagem da causa do acidente. As técnicas de análise de árvore de falhas e árvore de eventos são usadas para aprimorar o modelo de acidente e para representar uma imagem holística do mecanismo de causa-consequência do processo de acidente. A análise quantitativa tem dois aspectos: atualização e previsão. O modelo é capaz de capturar o comportamento operacional do processo e atualizar a probabilidade de acidentes. O modelo preditivo prevê a probabilidade de uma série de eventos anormais ocorrerem no próximo intervalo de tempo.
Systematic Human Error Reduction and Prediction Analysis (SHERPA)	Embrey, D.E. SHERPA: A systematic human error reduction and prediction approach (Originally:1986). Contemporary Ergonomics 1984-2008: Selected Papers and an Overview of the Ergonomics Society Annual Conference. 113-119, 2009.	A SHERPA foi desenvolvida por David Embrey em 1986 como uma técnica de previsão de erros humanos que também analisa tarefas e identifica possíveis soluções para erros de forma estruturada. A técnica é baseada em uma taxonomia do erro humano e, em sua forma original, especifica o mecanismo psicológico implicado no erro.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Systems-Theoretic Accident Model and Processes (STAMP) STAMP = CAST + STPA	Nancy G. Leveson A New Accident Model for Engineering Safer Systems, Safety Science Volume: 42, Issue: 4, pp. 237-270, 2004, Massachusetts Institute of Technology.	STAMP é um modelo de causalidade de acidentes inspirado na teoria de sistemas. Nesta técnica, os sistemas são vistos como componentes interrelacionados mantidos em um estado de equilíbrio dinâmico por malhas de realimentação por realimentação, sendo tratados como processos dinâmicos que estão continuamente se adaptando para atingir seus resultados e para reagir as mudanças internas e do ambiente ao redor. O método foi desenvolvido por Nancy Levenson em 2004, tendo como conceitos básicos as restrições impostas ao sistema, as malhas de controle, os modelos de processos, e os níveis de controle. As duas ferramentas mais utilizadas hoje que tem como base o STAMP são o STPA (do inglês, System Theoretic Process Analysis) e o CAST (do inglês, Causal Analysis based on System Theory).
Technique for Human Error Rate Prediction (THERP)	Swain, A.D., Guttmann, H.E. Handbook of human reliability analysis with emphasis on nuclear power plant applications. US Nuclear Regulatory Commission), Washington, DC. NUREG/CR-1278, 1983. Kirwan, B. The validation of three human reliability quantification techniques, THERP, HEART and JHEDI: Part 1 technique descriptions and validation issues. Applied Ergonomics, 27, (6), 359-373, 1996. Kirwan, B., Kennedy, R., Taylor-Adams, S. and Lambert, B. The validation of three human reliability quantification techniques, THERP, HEART and JHEDI: Part II – results of validation exercise. Applied Ergonomics, 28 (1), 17-25, 1997.	THERP (do inglês, *Technique for Human Error Rate Prediction*) é um método de Avaliação de Confiabilidade Humana - ACH (do inglês, Human Reliability Assessement – HRA) que tem por objetivo definir a probabilidade de erro humano ao realizar uma ou um conjunto de tarefas, de modo que medidas possam ser tomadas para a redução da chance de ocorrência desses erros analisados. A primeira versão do método THERP foi apresentada em 1962 em um simpósio durante a Sexta Reunião Anual da Sociedade de Fatores Humanos. O método foi desenvolvido pelo Dr. Alan Swain, sendo considerado o primeiro método formal de ACH. Os principais elementos para completar o processo de quantificação são descritos por Kirwan et al (1997): • Decomposição de tarefas em elementos; • Atribuição de HEPs (*human error probabilities*) nominais a cada elemento; • Determinação dos efeitos do PSF (Performance Shaping Factors) em cada elemento; • Cálculo dos efeitos da dependência entre tarefas; • Modelagem em uma árvore de eventos para HRA (*Human Reliability Assessment*); • Quantificação da tarefa total HEP.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Technique for Human Event Analysis (ATHEANA)	Cooper, S.E. et al. NUREG/CR-6350: A Technique for Human Error Analysis (ATHEANA), 114 pp., 1996. Forester J. et al. NUREG-1624, Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). Rev. 1, 2000.	Técnica para Análise de Evento Humano (ATHEANA) é uma técnica utilizada no campo da avaliação da confiabilidade humana (HRA). O objetivo do ATHEANA é avaliar a probabilidade de erro humano durante a execução de uma tarefa específica. A partir de tais análises, medidas preventivas podem ser tomadas para reduzir erros humanos dentro de um sistema e, portanto, levar a melhorias no nível geral de segurança.
Toxicological risk assessment Toxicity assessment (TA)	World Health Organization (WHO) Human health risk assessment toolkit – chemical hazards, 1st ed., 87 pp., 2010. U.S. Environmental Protection Agency (US EPA) Guidelines for ecological risk assessment, 1998.	A avaliação de risco no contexto de riscos para plantas, animais, domínios ecológicos e humanos como resultado da exposição a uma variedade de perigos ambientais envolve as seguintes etapas. Riscos para plantas, animais, domínios ecológicos e humanos podem ser causados por agentes físicos, químicos e / ou biológicos, resultando em danos ao DNA, defeitos de nascença, disseminação de doenças, contaminação das cadeias alimentares e contaminação da água. A avaliação de tais riscos pode exigir a aplicação de uma variedade de técnicas durante as seguintes etapas: a) Formulação de Problemas; b) Identificação e Análise de perigos; c) Avaliação de dose de resposta; d) Avaliação de exposição; e) Caracterização de risco.
Value at Risk (VaR) Conditional Value at Risk (CVaR) (CoVaR)	Chance, D., Brooks, R. An introduction to derivatives and risk management, 0 Cengage Learning, 652 pp., 2010. Thomas J. and Pearson Neil D. Value at risk. Financial Analysts Journal, Vol. 56, pp. 47-67, 2000.	O VaR é amplamente utilizado no setor financeiro para fornecer um indicador do valor da possível perda em uma carteira de ativos financeiros ao longo de um período específico dentro de um determinado nível de confiança. Perdas maiores que o VaR são sofridas apenas com uma pequena probabilidade. A distribuição de lucros e perdas geralmente é derivada de uma de três maneiras: - A simulação de Monte Carlo é usada para modelar os impulsionadores da variabilidade no portfólio e derivar a distribuição; - Modelos de simulação histórica fazem projeções com base em olhar para os resultados e distribuições observados; - Os métodos analíticos são baseados em suposições de que os fatores de mercado subjacentes têm uma distribuição normal multivariada.

Método	Referências Principais / Abordagens Iniciais	Breve descrição
Weighted risk analysis (WRA)	Shahid Suddle The weighted risk analysis, Safety Science, Volume 47, Issue 5, pp. 668-679, 2009.	A análise de risco ponderada é uma ferramenta interessante que compara diferentes riscos, como investimentos, perdas econômicas e a perda de vidas humanas, em uma dimensão (por exemplo, dinheiro), uma vez que tanto os investimentos quanto os riscos podem ser expressos apenas em dinheiro.
Worst-case analysis Worst-case testing	U.S. Department of Defense MIL-STD-785B, Military Standard: Reliability Program for Systems and Equipment Development and Production, 1980.	A análise de pior caso é usada para identificar os componentes mais críticos que afetarão o desempenho do circuito. Inicialmente, uma análise de sensibilidade é executada em cada componente individual que possui uma tolerância atribuída. O valor do componente é efetivamente empurrado para ambos os limites de tolerância por uma pequena porcentagem de seu valor para ver qual limite teria o maior efeito na saída do pior caso. Uma análise de pior caso é então realizada definindo todos os valores de componentes para seus limites de tolerância finais que deram uma indicação dos resultados de pior caso. Para reduzir o número de execuções de simulação, as funções de intercalação podem ser usadas para detectar diferenças da saída de pior caso nominal, como diferenças mínimas, máximas ou de limite.

Anexo C – Mapa de Produto: Cadeira de Rodas Motorizada

Este anexo apresenta o mapa de produto da cadeira de rodas motorizada desenvolvido para avaliação na seção 4.1.3.