**ANÁLISE COMPARATIVA INTERSETORIAL DA AVALIAÇÃO QUALITATIVA E QUANTITATIVA DE RISCO**

Guilherme Conceição Rocha1, Instituto Tecnológico de Aeronáutica (ITA)

Salvador Jorge da Cunha Ronconi2, KONATUS

**RESUMO**

Este trabalho faz uma análise comparativa dos métodos, processos e ferramentas empregados na avaliação qualitativa e quantitativa de risco nos setores da aviação, espacial, automotivo, saúde, petróleo e gás, nuclear, mineração e indústria de transformação. Para tanto, analisa-se a base normativa, contexto operacional, taxonomias de cada domínio, bem como estado da prática no uso de recursos tecnológicos para apoiar a avaliação e gerenciamento de riscos em tais setores.

1. **INTRODUÇÃO**

O processo de avaliação qualitativa e quantitativa de riscos é feito tanto no projeto de sistemas quanto durante a operação do mesmo e consiste em pilar básico para assegurar operações com boas margens de segurança.

Para atender a esse propósito, diferentes setores industriais utilizam diferentes métodos, processos e ferramentas, bem como usam taxonomias distintas no que diz respeito ao gerenciamento de riscos.

Nesse contexto, realizou-se uma análise comparativa intersetorial, destacando semelhanças e diferenças de métodos, processos, ferramentas e taxonomias, utilizando como base do estudo as referências normativas mais utilizadas em tais setores.

1. **PANORAMA HISTÓRICO**

A sistematização do processo de avaliação qualitativa e quantitativa de riscos está coadunada com a criação de órgãos normativos e agências reguladoras em território nacional. Tais entidades contribuíram bastante para a definição de uma base regulatória e estabelecimento meios de cumprimento aceitáveis para gerenciamento de riscos no projeto e na operação de sistemas. A definição da base regulatória inspira-seem regras e normas adotadas por países desenvolvidos com as devidas adaptações para o cenário brasileiro, por meio da participação ativa da comunidade prática via consultas públicas.

A lista a seguir contém as datas de criação das principais agências reguladoras e órgãos normativos nacionais.

* CNEN - Comissão Nacional de Energia Nuclear, agosto de 1962 (Lei 4.118)
* ANEEL - Agência Nacional de Energia Elétrica, dezembro de 1996 (Lei 9.427)
* ANATEL - Agência Nacional de Telecomunicações, junho de 1997 (Lei 9.472)
* ANP - Agência Nacional do Petróleo, Gás Natural e Biocombustíveis, agosto de 1997 (Lei 9.478)
* ANVISA – Agência Nacional de Vigilância Sanitária, janeiro de 1999 (Lei 9.782)
* ANTT - Agência Nacional de Transportes Terrestres, junho de 2001 (Lei 10.233)
* ANAC - Agência Nacional de Aviação Civil, setembro de 2005 (Lei 11.182)
* ANM - Agência Nacional de Mineração, julho de 2017 (Medida provisória 791)

1. **NORMAS SETORIAIS**

Cada setor econômico possui um conjunto específico de normas que estabelecem métodos, processos e ferramentas empregados na avaliação qualitativa e quantitativa de risco. A seguir faz-se um resumo das principais normas de cada setor.

* 1. **Aeronáutico**

SAE-ARP-4761

Essa é uma norma que estabelece processos e ferramentas de análise de segurança recomendados durante a fase de projeto de sistemas aeronáuticos.

Nessa norma, destacam-se as seguintes ferramentas [1]:

* FHA (FunctionalHazards Assessment): Processo sistemático de identificar e avaliar a criticidade de condições de falha com efeito na aeronave, tripulação e seus passageiros;
* FMEA (FailureModeandEffectAnalysis): Ferramenta que permite identificar modos de falhas de componentes que compõem o sistema, avaliar efeitos de tais falhas no sistema e na aeronave, bem como identificar meios de verificação da existência da referida falha;
* FTA (FaultTreeAnalysis): Avaliação quantitativa da probabilidade de ocorrência de eventos associados a condições de falhas, baseada na combinação booleana de eventos básicos, bem como avaliação do nível de redundância de determinado sistema e quantificação do risco residual de falhas simples;
* CMA (Common ModeAnalysis): Processo sistemático para avaliar o potencial de modos comuns de falha em sistemas aeronáuticos;
* PRA (Particular Risk Analysis): Avaliação do impacto na segurança da aeronave, tripulação e passageiros de situações particulares de risco tais como fogo a bordo, estouro de pneu, rompimento de palheta de motor, dentre outros;
* ZSA (Zonal Safety Analysis): Processo de se avaliar o efeito de interface entre sistemas que localizados próximos, numa mesma região da aeronave, tal como o potencial de ocorrência de falhas em cascata.

RTCA/DO-178C

Essa norma prescreve objetivos processuais de desenvolvimento de software embarcado tão mais rigorosos quanto mais crítica for a falha do referido software [2]. Desse modo, existe uma relação direta entre o rigor processo de desenvolvimento de software prescrito e a avaliação qualitativa de risco associada ao mesmo.

A tabela a seguir contém um breve histórico de revisões dessa norma.

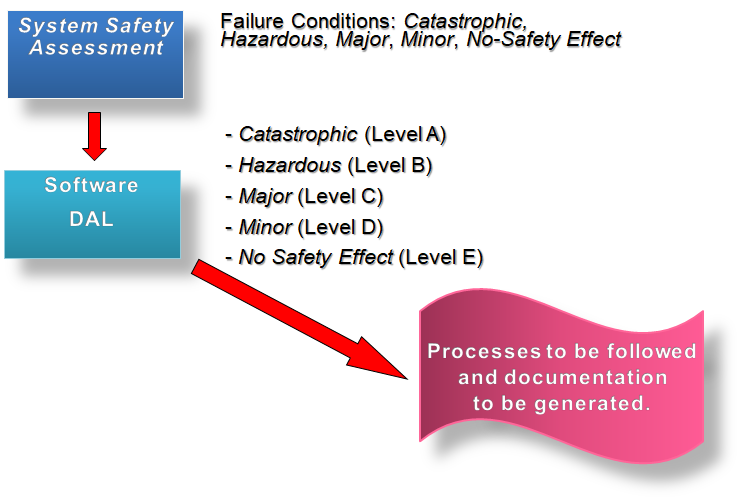
**Tab.1** – Histórico de revisões da norma RTCA/DO-178

|  |  |  |
| --- | --- | --- |
| **Documento** | **Conteúdo** | **Data** |
| DO-178 | * Definição da documentação mínima de certificação | 1980 |
| DO-178ª | * Aderência aos princípios de Engenharia de Software * Introdução do conceito de Verificação e Validação | 1985 |
| DO-178B | * Detalha os objetivos do processo de desenvolvimento (“O que”), mas não detalha o “Como” atingir tais objetivos. | 1992 |
| DO-178C | * Inclusão de suplementos que abordam o “Como” | 2011 |

Os suplementos referenciados na norma RTCA/DO-178 C encontram-se listados a seguir [2]:

* RTCA/DO-330 Software Tool Qualification Considerations
* RTCA/DO-331 Model-Based Development and Verification Supplement to DO-178C and DO-278A
* RTCA/DO-332 Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A
* RTCA/DO-333 Formal Methods Supplement to DO-178C and DO-278A

A figura a seguir mostra esquematicamente como o nível de rigor de desenvolvimento de software (DAL – *Design AssuranceLevel*) está associado à condição de falha do sistema e à demanda por evidências de certificação.



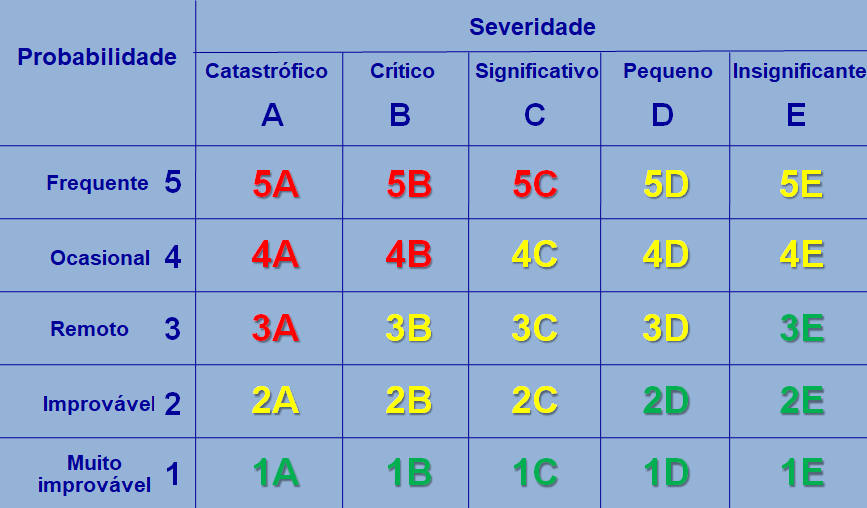
|  |
| --- |
|  |
| **Fig.1** – Processo de alocação de DAL da norma RTCA/DO-178C |

ICAO Anexo 19

O anexo 19 da ICAO, lançado em 2013 estabelece um processo sistemático de gerenciamento de riscos a ser executado durante a operação de aeronaves. Esse processo baseia-se em quatro pilares básicos, a saber [3]:

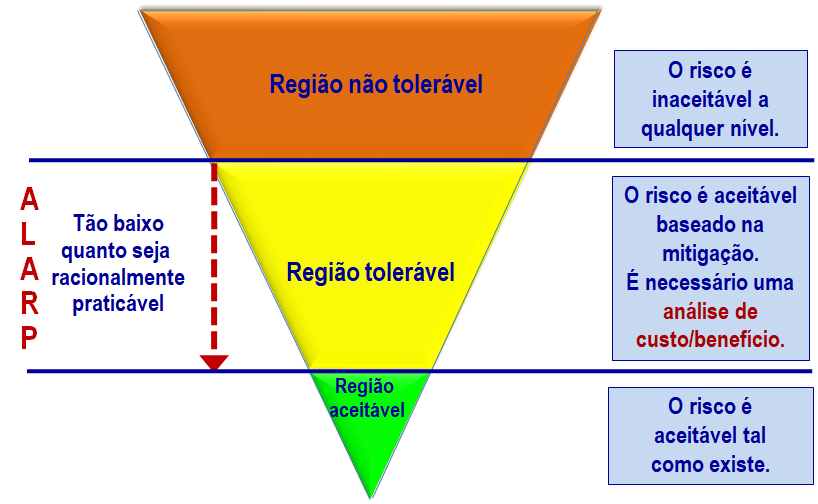
* Definição de políticas de segurança
* Gerenciamento de risco
* Garantia do sistema
* Promoção da segurança

Em termos de ferramentas, a principal ferramenta sugerida pelo Anexo 19 é a matriz de avaliação de risco. Trata-se de uma matriz que permite avaliar qualitativamente se um risco é aceitável, tolerável ou não tolerável, a partir da estimativa de severidade e probabilidade [3].



|  |
| --- |
|  |
| **Fig.2** – Matriz de avaliação do risco |

A figura a seguir expõe de modo esquemático as três regiões anteriormente descritas e identificadas pela cor verde (aceitável), amarelo (tolerável) e vermelho (não tolerável) [3].



|  |
| --- |
|  |
| **Fig.3** – Processo de avaliação do risco conforme Anexo 19 da ICAO |

* 1. **Petróleo e Gás**

N-2595

Essa norma [4], elaborada pela Petrobras com base na norma IEC 61511 [5], estabelece condições mínimas requeridas para projeto, operação e manutenção de sistemas instrumentados de segurança utilizados na indústria de Petróleo e Gás e denominados SIS (*Safety Instrumented Systems*).

A norma N-2595 baseia-se na seguinte taxonomia [4]:

* **Safety Instrumented System - SIS**

Sistema instrumentado utilizado para implementar uma ou mais funções de segurança. Tal sistema é composto por um conjunto de sensores, processadores lógicos e atuadores.

* **Independent Protection Layer - IPL**

Uma camada de proteção independente (IPL) consiste em um recurso de projeto capaz de manter sua função preventiva ou de mitigação de forma totalmente autônoma, independentemente do cenário operacional ou mesmo de outras camadas de proteção.

* **Falha (fault)**

Condição anormal que pode causar a redução ou perda da capacidade de um dispositivo desempenhar a sua função desejada.

* **Estado Seguro (safe state)**

Estado de um processo ou de operação de um equipamento cujo risco encontra-se dentro de um limite considerado tolerável.

* **Safety Instrumented Function - SIF**

Função de proteção implementada por um SIS para atingir ou manter um estado Seguro de um processo ou operação de equipamento por meio de uma ação de automação específica a partir de um determinado desvio operacional.

* **Falhasistemática (systematic failure)**

Falha relacionada com uma causa conhecida e que evolui de forma determinística.

* **Redundância**

Existência de mais de uma maneira de se desempenhar a mesma função, normalmente associada ao aumento da confiabilidade e disponibilidade do sistema. A redundância pode ser implementada por meio de dispositivos idênticos (redundância idêntica) ou diferentes (redundância diversa ou dissimilar).

* **Risco**

Combinação da probabilidade (frequência esperada) de um evento perigoso com a severidade de tal evento. O risco pode ser expresso matematicamente pelo produto da frequência esperada pela severidade do evento (Risco = frequência X severidade). A frequência esperada é tipicamente expressa pelo número de eventos por ano, enquanto a severidade o é em valores monetários e/ou números de fatalidades.

* **Riscotolerável (tolerable risk)**

Risco estabelecido como aceitável em um determinado contexto.

Os processos e ferramentas que a norma N-2595 recomenda são [4]:

* **Layers of Protection Analysis - LOPA**

Técnica semi-quantitativa utilizada para avaliar a redução de risco alcançável pelo uso de camadas de proteção no sistema.

* **Process Hazard Analysis - PHA**

Esforço sistemático e organizado para identificar e avaliar a relevância de perigos em potencial associados com o processamento e manuseio de produtos perigosos, focando no equipamento, instrumentação, ações humanas e condições externas que podem afetar o processo.

* **Hazards and Operability Study - HAZOP**

Técnica indutiva e estruturada para identificar qualquer processo perigoso e problemas operacionais potenciais, associando um conjunto de palavras chave às variáveis de processo e para cada desvio operacional identificado, suas causas, consequências, meios de detecção, proteções de segurança existentes e recomendações de medições adicionais quando aplicável.

* **Definição do Safety Integrity Level - SIL**

O SIL (*Safety IntegrityLevel*) é um indicador de desempenho do SIF e expresso numa escala inteira de 1 a 4. Para se estimar o SIL, faz-se necessário:

1. Estimar a probabilidade média de uma determinada camada de proteção falhar quando demandada num determinado intervalo de tempo (*PFDavg - AverageProbabilityofFailure on Demand*).
2. Estimar o fator de redução do risco (*RRF - Risk Reduction Factor*) como sendo RRF = 1/ PFDavg.
3. Definir o SILcom a norma IEC 61508. Quanto maior o RRF requerido para uma SIF, maior deverá ser o SIL associado a ela.

De modo sumarizado, a norma N-2595 preconiza as seguintes etapas processuais [4]:

* **Hazard Analysis**

Identificação das condições perigosas feita por um time muiti-disciplinar de profissionais nas áreas de processos, instrumentação e controle, operações industriais e segurança. Nessa etapa recomenda-se o uso da ferramenta HAZOP.

* **Risk Evaluation**

Para cada condição perigosa, determina-se o risco conforme estimativa de frequência e severidade. Em seguida avalia-se se o risco é tolerável ou não.

* **Protection Layers**

Caso a avaliação anterior indique que o risco é superior a um limite tolerável, deve-se buscar reduzir a expectativa de frequência ou severidade do evento associado por meio da introdução de camadas de proteção no sistema.

* **SIS Design**

Especificar uma solução lógica compatível com as análises anteriores e demonstrar atendimento aos requisitos da norma IEC 61508 para os SIL (Safety IntegrityLevel) de cada uma das funções de proteção (SIF).

* **Factory Acceptance Test**

Especificar e realizar um teste de aceitação do sistema a ser realizado após a conclusão do projeto e antes da instalação e comissionamento. O FAT deve ser exaustivo, cobrindo todas as SIFs e todas as possíveis combinações lógicas de cada SIF. O objetivo desse teste é verificar atendimento aos requisitos das SIFs.

* 1. **Industrial e automotivo**

IEC 61508

Essa norma estabelece um processo de desenvolvimento de dispositivos eletro-eletrônicos programáveis que podem colocar em risco a segurança do sistema [6]. Existe uma adaptação dessa norma para aplicação no setor automotivo que consiste na ISO 26262 [7].

Quanto mais crítica a programação (software embarcado), maior o rigor processual demandado, o que implica em um SIL (Safety IntegrityLevel) maior. Desse modo, para um software mais crítico, espera-se uma probabilidade média de falhas mais baixa, um fator de redução de risco (RRF – Risk Reduction Factor) mais alto e um SIL maior.

As tabelas a seguir mostram a relação entre SIL e RRF para itens com baixa demanda de operação e itens de operação contínua [6].

|  |
| --- |
| **Tab.2**– Relação entre SIL e RRF para itens com baixa demanda |

|  |  |
| --- | --- |
| **SIL** | **RRF** |
| 1 | 10 – 100 |
| 2 | 100 – 1.000 |
| 3 | 1.000 – 10.000 |
| 4 | 10.000 – 100.000 |

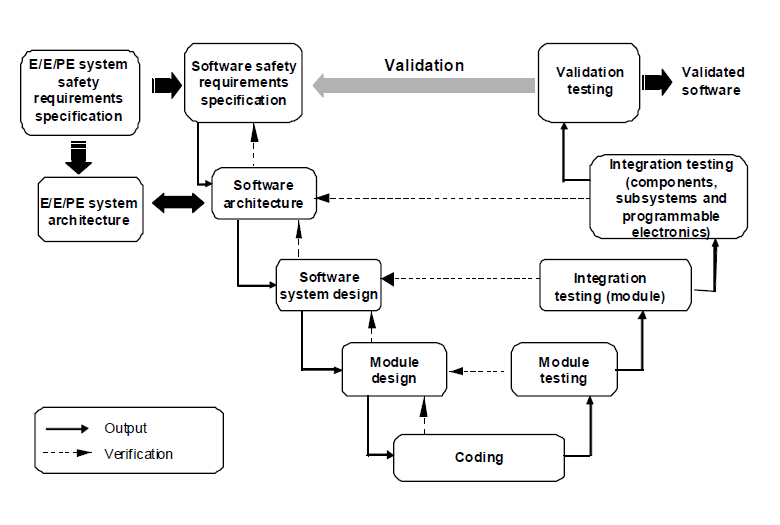
|  |
| --- |
| **Tab.3**– Relação entre SIL e RRF para itens de operação contínua |

|  |  |
| --- | --- |
| **SIL** | **RRF** |
| 1 | 100.000 – 1.000.000 |
| 2 | 1.000.000 – 10.000.000 |
| 3 | 10.000.000 – 100.000.000 |
| 4 | 100.000.000 – 1.000.000.000 |

O conjunto de processos recomendados pela norma IEC 61508 resumem-se às seguintes etapas [6]:

1. Software safety requirements specification
2. Validation plan for software aspects of system safety
3. Software design and development
   * software architecture
   * detailed design and development
   * code implementation
   * software module testing
   * software integration testing
4. Programmable electronics integration (hardware and software)
5. Software operation and modification procedures
6. Software aspects of system safety validation
7. Software modification
8. Software verification

A figura a seguir representa de modo esquemático o encadeamento de tais etapas, conforme recomendado pela IEC 61508 [6].



|  |
| --- |
|  |
| **Fig.4** – Processo de desenvolvimento de software de acordo com norma IEC 61508 |

* 1. **Saúde**

IEC 62304

Essa norma define um processo de desenvolvimento de software para equipamentos médicos críticos [8], o qual pode ser evidenciado via documentação técnica contendo todos os registros de verificação do processo de desenvolvimento. Tal norma está diretamente relacionada com requisitos da ANVISA conforme sumarizado a seguir.

Em 2001 a ANVISA emitiu resolução RDC Nº 185/2001 estabelecendo que:

* Equipamentos médicos são classificados nas categorias I, II, III e IV, de acordo com o risco à saúde do paciente, onde a classificação I é a mais severa;
* O software do equipamento médico segue a mesma classificação.

De acordo com a instrução normativa da ANVISAIN13/2009, para se registrar um equipamento médico classe I ou II, o requerente deve prover documentação técnica com todos os registros de verificação capazes de provar a adequação do projeto ao seu uso pretendido.

Desde o ano de 2015, a ANVISA vem reconhecendo a norma IEC 62304 como o principal guia para a geração de evidências de verificação capaz de comprovar adequação do projeto ao uso pretendido.

O processo de verificação da norma IEC 62304 segue um desenvolvimento em V, conforme ilustrado esquematicamente na figura a seguir. Cada elemento de software de aplicação médica denomina-se PEMS (*Programmable Electrical Medical Devices*) [8].



|  |
| --- |
|  |
| **Fig.5** – Processo de desenvolvimento de software médico de acordo com norma IEC 62304 |

* 1. **Nuclear**

CNEN NE 1.26

A Comissão Nacional de Energia Nuclear (CNEN) é uma autarquia federal vinculada ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), criada em 1956 e estruturada pela Lei 4.118, de 27 de agosto de 1962, para desenvolver a política nacional de energia nuclear. Órgão superior de planejamento, orientação, supervisão e fiscalização, a CNEN estabelece normas e regulamentos em radioproteção e é responsável por regular, licenciar e fiscalizar a produção e o uso da energia nuclear no Brasil.

A CNEN investe também em pesquisa e desenvolvimento, buscando um uso cada vez mais amplo e seguro das técnicas do setor nuclear, e seu foco é garantir os benefícios da energia nuclear a um número cada vez maior de brasileiros, sempre com segurança na operação dos materiais e equipamentos radioativos.

A CNEN disponibiliza um grande conjunto de normas voltadas à garantia da segurança tanto do projeto quanto da operação de instalações de geração de energia nuclear. Dentre tais normas merece um destaque a norma CNEN NE 1.26 que trata da segurança da operação de usinas nucleoelétricas.

A norma CNEN NE 1.26 estabelece os requisitos mínimos necessários para garantir que a condução da operação de usinas nucleoelétricasseja mantida sem risco indevido à saúde e à segurança da população como um todo e ao meio ambiente [9]. Nela se define que a organização operadora deve desenvolver, aplicar e permanentemente aperfeiçoar um modelo para gerenciamento do risco associado às diversas configurações operacionais, sem prescrever qual seria esse modelo.

Por outro lado, fica explícito na referida norma que o modelo para gerenciamento do risco deve incorporar a base de dados da organização operadora, contendo a experiência operacional específica acumulada durante um período em que esses dados sejam estatisticamente significativos [9].

Enquanto a norma CNEN NE 1.26 estabelece requisitos para a operação de usinas nucleoelétricas, os requisitos de projeto dessas instalações são definidos em conformidade com a norma internacional IEC 61513 [10].

* 1. **Espacial**

NBR ISO17666

Essa norma define os princípios e requisitos para o gerenciamento do risco integrado em um programa espacial e esclarece o que é necessário para implementar uma política de gerenciamento do risco integrada a um projeto, por qualquer participante do projeto e em qualquer nível (por exemplo: clientes e fornecedores nos diversos níveis) [11].

O texto do documento contém um resumo do processo geral de gerenciamento do risco, que é subdividido em quatro (4) passos básicos e nove (9) tarefas. A aplicação pode ser adaptada às condições específicas de cada projeto [11].

* 1. **Mineração**

NR 22

A ANM (Agência Nacional de Mineração) foi criada por meio da Medida Provisória n° 791, de 25 de julho de 2017. De acordo com o teor da referida Medida Provisória, a ANM tem como missão substituir o então Departamento Nacional de Produção Mineral (DNPM), ora extinto, nas suas funções de Estado que englobam o planejamento da exploração mineral e o aproveitamento dos recursos minerais, assegurando, controlando e fiscalizando o exercício das atividades de mineração, além de regular o uso dos recursos minerais de domínio da União.

A regulação do uso de recursos minerais da Uniãoatende a critérios de utilidade pública, racionalidade do aproveitamento dos bens minerais, reparabilidade financeira e estrutural à sociedade e a sustentabilidade do meio ambiente.

A ANM em conjunto com o Ministério do Trabalho fiscaliza a Segurança e Saúde Ocupacional na Mineração tendo por referência normativa, a norma NR 22, cujo objetivo consiste em disciplinar os preceitos a serem observados na organização e noambiente de trabalho, de forma a tornar compatível o planejamento e o desenvolvimento da atividade mineira com abusca permanente da segurança e saúde dos trabalhadores [12].

A NR 22 se aplica tanto a minerações subterrâneas, minerações a céu aberto, garimpos, atividades de beneficiamentos minerais e realização de pesquisa mineral. Sua primeira versão é de julho de 1978, tendo a sua última atualização em abril de 2019 [12].

Essa norma estabelece que cabe à empresa ou Permissionário de Lavra Garimpeira elaborar e implementar um Programa de Gerenciamentode Riscos - PGR, incluindo, no mínimo, aspectos relacionados a [12]:

a) riscos físicos, químicos e biológicos;

b) atmosferas explosivas;

c) deficiências de oxigênio;

d) ventilação;

e) proteção respiratória, de acordo com a Instrução Normativa n.º 1, de 11/04/94, da Secretaria de Segurança e Saúdeno Trabalho;

f) investigação e análise de acidentes do trabalho;

g) ergonomia e organização do trabalho;

h) riscos decorrentes do trabalho em altura, em profundidade e em espaços confinados;

i) riscos decorrentes da utilização de energia elétrica, máquinas, equipamentos, veículos e trabalhos manuais;

j) equipamentos de proteção individual de uso obrigatório;

l) estabilidade do maciço;

m) plano de emergência e

n) outros resultantes de modificações e introduções de novas tecnologias.

Conforme requerido pela norma, o Programa de Gerenciamento de Riscos - PGR deve incluir as seguintes etapas [12]:

a) antecipação e identificação de fatores de risco, levando-se em conta, inclusive, as informações do Mapa de Risco, quando houver;

b) avaliação dos fatores de risco e da exposição dos trabalhadores;

c) estabelecimento de prioridades, metas e cronograma;

d) acompanhamento das medidas de controle implementadas;

e) monitorizarão da exposição aos fatores de riscos;

f) registro e manutenção dos dados por, no mínimo, vinte anos e

g) análise crítica do programa, pelo menos, uma vez ao ano, contemplando a evolução do cronograma, com registrodas medidas de controle implantadas e programadas.

1. **CONCLUSÕES**

É possível perceber que o processo de avaliação qualitativa e quantitativa de riscos de diversos setores econômicos possui muitas semelhanças e geralmente permeia tanto a fase de projeto quanto a operação de sistemas. Existe inclusive uma taxonomia comum entre os diversos setores, havendo poucas carências de harmonização nesse sentido.

Por outro lado, percebe-se um desbalanceamento quanto ao uso de técnicas e ferramentas de análise, sendo o setor aeronáutico aquele que se encontra em estágio mais avançado quanto ao emprego das melhores práticas tanto qualitativas quanto quantitativas de gerenciamento de riscos.

O potencial de avanço no estudo de métodos e ferramentas para avaliação qualitativa e quantitativa de riscos é enorme e depende de diversos fatores, a saber: compartilhamento de experiências entre profissionais de diferentes setores, estímulo ao desenvolvimento de uma cultura de segurança e normatização, treinamento e capacitação de pessoas, fomento ao fortalecimento da comunidade que estuda e trabalha com sistemas críticos à segurança, bem como maior interação entre indústria e comunidade acadêmica.

1. **REFERÊNCIAS:**

[1] SAE, SAE-ARP-4761Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE, US (1996);

[2] RTCA, RTCA/DO-178C Software Considerations in Airborne Systems and Equipment Certification, RTCA, US (2011);

[3] ICAO, ANNEX 19 Safety Management,ICAO, US (2013);

[4] PETROBRAS, N-2595 REV C. Critérios de Projeto e Manutenção para SistemasInstrumentados de SegurançaemUnidadesIndustriais,PETROBRAS, BRASIL (2012);

[5] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 61511Functional safety - Safety instrumented systems for the process industry sector, IEC, SUÍÇA (2016);

[6] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES), IEC, SUÍÇA (2010);

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 26262 Road vehicles – Functional safety, ISO, SUÍÇA (2011);

[8] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 62304Medical device software – software life cycle processes, IEC, SUÍÇA (2015);

[9] COMISSÃO NACIONAL DE ENERGIA NUCLEAR, CNEN NE 1.26 Segurançanaoperação de usinasnucleoelétricas, CNEN, BRASIL (1997);

[10] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 61513Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, IEC, SUÍÇA (2011);

[11] ABNT, NBR ISO 17666SistemasEspaciais – Gerenciamento do risco, ABNT, BRASIL (2012);

[12] MINISTÉRIO DO TRABALHO E EMPREGO, NR 22Saúde e SegurançaOcupacionalnaMineração, MTE, BRASIL (2019).