

# **GESTÃO DE RISCO EM SISTEMAS CRÍTICOS: PROPOSTA DE MODELO PARA DECISÃO DE ESCOLHA DE AEROPORTO ALTERNATIVO PARA O SISTEMA DE TRÁFEGO AÉREO BRASILEIRO COM APLICAÇÃO DO MÉTODO BOW-TIE**

**Carlos Frederico Barros**

LABRISK Laboratório de Engenharia de Alta Complexidade - Universidade Federal Fluminense  
UFF

[carlosfredericobarros@gmail.com](mailto:carlosfredericobarros@gmail.com) (21) 98709-0827

**Vitor Rodrigues**

LABRISK Laboratório de Engenharia de Alta Complexidade - Universidade Federal Fluminense  
UFF

[contato.vitor.rodrigues@gmail.com](mailto:contato.vitor.rodrigues@gmail.com) (21) 98199-5518

**Danilo Colombo**

CENPES PETROBRAS

[colombo.danilo@petrobras.com.br](mailto:colombo.danilo@petrobras.com.br) (21) 98355-0437

## **RESUMO**

Este artigo foca no estudo da avaliação das características e do estado da arte do sistema aéreo brasileiro, propondo o desenvolvimento de uma metodologia de gestão de risco baseada no conceito Bow-tie para apoiar nos processos decisórios nas questões associadas ao tráfego aéreo e seus aeroportos, em especial a decisão para o uso de aeroporto alternativo.

## **ABSTRACT**

This article focuses on the study of the evaluation of the characteristics and state of the art of the Brazilian air system, pertinent to the control and management of air traffic (ATC/ATM), proposing the development of a risk management methodology based on the Bow-tie concept to support the decision-making processes in issues related to air traffic and its airports, in particular the decision to use an alternative airport.

**Palavras-chave:** Transporte aéreo, Redes aeroportuárias, Gestão de risco, Sistemas complexos e críticos, Método Bow-tie.

## 1. INTRODUÇÃO

A Gestão de Risco Tecnológico se manifesta hoje como um elemento de criação de valor, seja obstando as potenciais perdas humanas, ambientais e patrimoniais, seja ao reduzir perdas operacionais, impactando positivamente na produtividade e mitigando os custos associados aos eventos indesejáveis às atividades das instituições e empresas.

O método Bow-Tie é uma poderosa ferramenta para a análise e gestão de riscos complexos e dinâmicos. Este método foi adaptado pela Shell nos anos 90 e hoje é largamente utilizado por empresas da área de energia, aeronáutica e transporte dentre outras.

Sistemas e produtos complexos (COPS) podem ser definidos como qualquer produto, subsistema, sistema ou construção de alto custo e engenharia intensiva.

A crescente complexidade dos sistemas de operações aeronáuticas tem sido objeto de preocupação, por parte de especialistas, no que se refere à segurança. A complexidade implica não somente em novos tipos de perigos como também os tornam mais difíceis de serem identificados.

O Sistema de operação aeronáutico, em especial o subsistema aeroportuário, são classificados de complexos com componentes de risco intensivo.

Uma série de questões regulatórias faz a gestão da aviação civil estabelecer suporte para uma operação da aviação civil eficaz e segura.

Segurança é considerado como um dos aspectos mais importantes na aviação civil.

Todos os sistemas têm uma taxa de falhas inerentes às suas funcionalidades e ao ambiente de risco tecnológico e ambiental.

O grau e a capacidade do sistema aeronáutico, e em especial dos aspectos aeroportuários de resistir a perturbações do seu ambiente operacional, mantendo a sua capacidade operacional em níveis compatíveis com as demandas dos stakeholders e as questões regulatórias, e responder de forma satisfatória a elas, estabelece o nível de sua eficácia.

Nosso objetivo neste artigo é aumentar esta eficácia, desenvolvendo uma modelagem

de gestão de risco para a tomada de decisão de uma aeronave escolher um aeroporto alternativo, caso encontre inoperante por algum motivo o aeroporto de destino previsto.

## 2. GERENCIAMENTO DE RISCO

O gerenciamento de riscos é frequentemente visto sob a ótica empresarial como algo reativo, ou pior, não responsivo. Trata-se de uma visão ainda com amplas oportunidades de mudança. Em adjunção a responsabilidade social atualmente é uma maneira de empresas causarem interferências positivas no ambiente (comunidades, colaboradores, etc.) em que operam, gerando oportunidade para a menor perturbação possível através de suas operações, assim como estabelecer um vínculo positivo com todos os stakeholders. A redução de riscos associados às suas atividades se insere neste contexto.

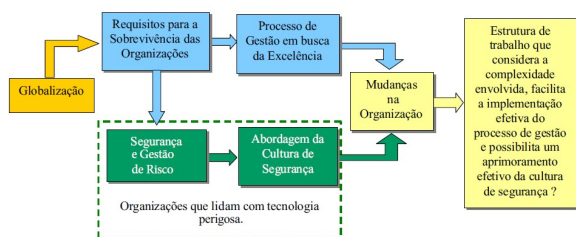
Desse modo a Gestão de Risco se manifesta hoje como um elemento de criação de valor, seja obstando as potenciais perdas patrimoniais, humanas e ambientais, seja ao reduzir perdas operacionais, impactando positivamente na produtividade empresarial e mitigando os custos associados a eventos indesejáveis às atividades das empresas.

Uma nova proposta de visão pode ter foco em facilitar a comunicação interna das empresas e organizações através do uso de uma linguagem comum e uma sistemática consistente de gestão, promovendo o alcance dos principais objetivos do Gerenciamento de Riscos, dentre os quais: tornar o gerenciamento de riscos parte integrante do negócio; apoiar a gestão das empresas e organizações na prestação de contas de sua atuação perante a sociedade e a comunidade local; fortalecer a base ética, a credibilidade e a imagem das organizações e, por fim, minimizar riscos, custos patrimoniais e operacionais, passivos trabalhistas e ambientais.

## 3. CULTURA DE SEGURANÇA

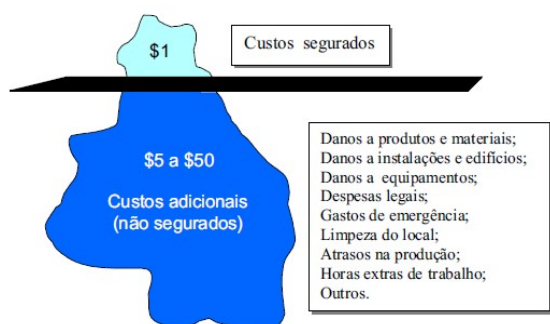
Historicamente a causa da segurança evolui em consequência de um desastre. Inapropriadamente significa que catástrofes

são necessárias para que os stakeholders compreendam que segurança é investimento e não custo, e que acidentes são necessários para aprimorar a efetividade das medidas de segurança (Figura 1).



**Figura 1: Risco e Mudanças nas Organizações**

Um estudo realizado em 1993 pela Health and Safety Executive (HSE) do Reino Unido estima que para cada \$1 de custos que podem ser recuperados por meio de seguro, outros \$5 a \$50 (Figura 2), são acrescidos à conta final em função de uma variedade de outras perdas financeiras, o que indica que as perdas financeiras efetivas com acidentes são, na verdade, muito superiores àquelas percebidas pela maioria dos gerentes.



**Figura 2: Iceberg dos custos com acidentes**

Acidentes industriais não custam apenas vidas, são também economicamente desastrosos para as organizações, sendo raras aquelas que conseguem suportar todos os tipos de prejuízos a elas causados, quando de grande monta. Temos um exemplo recente com a ruptura da barragem da Empresa Samarco em Minas Gerais e o megadesastre ecológico no golfo do México da Empresa British Petroleum (BP). A título de ilustração, a Tabela a seguir apresenta as perdas financeiras provocadas por alguns grandes acidentes na indústria petroquímica.

**Tabela 1: Perdas financeiras provocadas por alguns grandes acidentes na indústria petroquímica.**

<i>Acidente</i>	<i>País</i>	<i>Perda financeira (libras)</i>
Piper Alpha	Reino Unido	\$2,5 bilhões*
Exxon Valdez	EUA	\$3,5 bilhões
Sleipner A	Noruega	\$300 milhões
La Mede	França	\$260 milhões
Sodegaura	Japão	\$171 milhões
Croatzcoalcas	México	\$98 milhões

\*Sem considerar os custos incalculáveis de 167 mortes.

O avanço tecnológico, ao mesmo tempo em que proporciona muitas soluções para problemas associados às situações de trabalho reais vigentes até então, origina novos problemas em consequência do estabelecimento de novas situações de trabalho. A automatização pode ter diminuído a ocorrência de certos tipos de erros, mas introduziu novas categorias de erros associados às interfaces homem-máquina que ainda precisam ser completamente compreendidos. Mesmo uma automatização completa não elimina o envolvimento do fator humano com o sistema, servindo apenas para transferir as responsabilidades críticas do operador para o projetista. A automatização de modernos sistemas críticos com respeito à segurança tem ampliado os problemas relacionados ao operador humano, ao invés de reduzi-los.

Como forma de obter aprendizado sobre as diferentes causas envolvidas em acidentes industriais de grandes proporções, profissionais e organismos internacionais fizeram análises detalhadas dos acidentes das usinas nucleares de Three Mile Island, EUA, em 1979 e Chernobyl, na Ucrânia, em 1986, da indústria petroquímica Union Carbide, mais conhecido como o acidente de Bhopal, na Índia, em 1984, e da nave espacial Challenger, EUA, em 1986, dentre outros. Essas análises demonstraram que a operação segura e confiável de processos industriais que utilizam tecnologia perigosa em sistemas complexos depende não apenas dos fatores

técnicos relacionados aos processos, mas também dos aspectos relacionados a fatores humanos e organizacionais e de suas múltiplas e complexas interfaces.

Um olhar aproximado nos grandes acidentes recentes mostra que eles não são causados por uma coincidência aleatória de falhas e erros, mas por uma migração sistêmica do comportamento organizacional em direção às fronteiras da operação segura. Grandes acidentes são o efeito colateral de decisões tomadas por vários tomadores de decisão, em diferentes organizações e em distintos momentos no tempo, todos fazendo o seu melhor para serem localmente efetivos. A experiência atual mostra que a quantidade relativa de causas de incidentes se concentra, de maneira crescente, no comportamento humano, sendo esse, entretanto, influenciado de forma direta e indireta pelas deficiências da organização onde os indivíduos trabalham.

As propostas atuais poderiam, então, iniciar um novo momento das operações, uma quebra de paradigma, onde setores de Sistema de Gestão de Qualidade, Gestão das Operações, Gestão da Manutenção e setores de Segurança, Meio Ambiente e Saúde (SMS), por exemplo, iniciariam um processo contínuo, sistemático e evolutivo de Gestão do Risco, que deve e pode evitar lucros cessantes para empresas e organizações, preservando vidas e patrimônio. A metodologia Bow-Tie faz esta integração sistêmica e organizacional, como veremos a seguir neste artigo.

#### **4. GERENCIAMENTO DE RISCO EM SISTEMAS CRÍTICOS**

Atualmente, os serviços ou aplicações disponibilizados à comunidade têm como mola propulsora, a descoberta de novas tecnologias ou evolução nos sistemas existentes. O fato relevante nesse processo é a clara indicação de que estes avanços são realizados por meio do uso de tecnologias que, de alguma forma, utilizam-se de sistemas computacionais embarcados.

Porém, em alguns casos, os serviços ou aplicações a serem disponibilizados dependem de certos requisitos de operação do sistema, requisitos estes considerados críticos,

desde que um mau funcionamento no sistema pode resultar em sérias consequências a seus usuários. Genericamente, tais sistemas são denominados de sistemas críticos de segurança. Requisitos típicos no projeto desses sistemas incluem a proteção à vida humana, ao meio ambiente ou dos recursos materiais. Em sistemas críticos, a denominação segurança refere-se sempre à expressão “*safety*” em contraposição ao termo “*security*”.

Portanto, independente do tipo de sistema crítico considerado, o sucesso do empreendimento deve estar relacionado com o cumprimento dos critérios de segurança (*safety*) e da confiabilidade do sistema, sem os quais os benefícios dos mais sofisticados sistemas e tecnologias serão em vão.

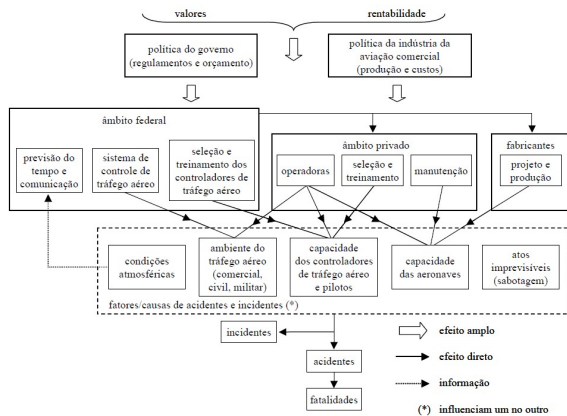
Em outras palavras, a segurança deve representar para a comunidade envolvida (órgão regulador, fabricantes e operadoras), a elementar prioridade em garantir níveis mínimos de risco aos usuários finais.

Segundo Johnson (1990), a segurança é uma característica de um sistema crítico definida como a probabilidade, em um determinado período de tempo, de que o sistema executará corretamente suas funções. Em caso de descontinuidade, o sistema deve buscar um estado final de forma a não interromper a operação de outros sistemas ou comprometer a segurança de quaisquer pessoas associadas ao sistema. Portanto, a segurança indica a capacidade do sistema em buscar um estado final seguro em caso de falha (*fail-safe*).

A confiabilidade atribuída a um sistema implica que o mesmo irá executar corretamente suas funções e de forma consistente ao longo de um determinado período de tempo. A confiabilidade de um sistema como uma função do tempo, indica a probabilidade condicional de que o sistema estará funcionando no intervalo de tempo  $[0, t]$ , dado que estava operacional no instante  $t = 0$ . O termo confiabilidade é também utilizado na qualificação de sistemas cujo reparo não possa ocorrer de imediato.

De modo geral, os sistemas críticos de segurança podem estar sujeitos à ocorrência de algum tipo de problema ou anormalidade durante a sua operação. As expressões

indicativas de problemas incluem *fault*, *error* e *failure*, termos estes imprescindíveis para o perfeito entendimento das idéias nesta área. De acordo com NETJASOV, F., JANIC M, 2008, a melhor terminologia corresponde às seguintes traduções: *fault* como falha, *error* como erro e *failure* como disfunção.



**Figura 3: Causa dos acidentes e incidentes aéreos.**

As características dos sistemas aeronáuticos é de que são críticos e complexos (Figura 3).

## 5. GERENCIAMENTO DE RISCO NA NAVEGAÇÃO AÉREA

### O Fator Humano e a Automação

Outro aspecto relacionado aos acidentes em geral refere-se à automação, dado os avanços nas técnicas e processos da engenharia. Estes avanços tecnológicos, principalmente pelo uso de computadores, têm permitido a automação de muitos processos e trabalhos antes manuais. A automação abrange vários aspectos e, como regra geral, relaciona-se com os seguintes objetivos: aumento da produtividade, redução de custos, redução de fadiga e de tempo em processos repetitivos, precisão no manuseio de informações e atendimento a certos critérios de segurança.

Nos sistemas críticos, a automação é fundamentada principalmente com relação ao controle de alguns sistemas mais complexos, cujos requisitos de segurança excedem a capacidade e as habilidades humanas (Leveson, 1995).

Porém, no setor aéreo, Scardigli (2002) assinala que, “a vulnerabilidade do sistema do setor aéreo frente a problemas, poderá

originar-se de algumas aplicações devido à complexidade das informações contidas nas centenas de computadores embarcados em um avião de carreira. Apesar da tecnicidade da aviação comercial estar particularmente avançada em termos de automação dos vôos e, portanto, proporcionando eficiência econômica, crescimento do desempenho e regularidade nos vôos, deve-se levar em conta que, os idealizadores do ‘totalmente digital’ também são seres humanos e podem cometer erros que conduzem a acidentes”.

No transporte aéreo, a pressão para aumentar o número de vôos de forma segura e eficiente, tem levado à comunidade do setor a desenvolverem novas propostas com respeito a equipamentos mais poderosos e confiáveis e, paralelamente, aumentando-se o nível de automação das facilidades pertinentes ao controle de tráfego aéreo.

Segundo Wickens *et al* (1998), tais propostas têm levantado algumas preocupações no sentido de que a automação possa comprometer a segurança do sistema pela marginalização das habilidades do controlador de tráfego aéreo em prover as ações necessárias quando da interrupção do sistema automatizado. Vários estudos têm mostrado que uma automação bem projetada pode ajudar o operador humano e, consequentemente, melhorar o desempenho do sistema. Como exemplo, pode-se citar no gerenciamento do tráfego aéreo, o processo de handoff (\*) automatic (passagem da aeronave de um setor aéreo para outro) e o uso de displays como ferramenta de auxílio no sequenciamento de aeronaves.

Com respeito ao fator humano, uma suposição bastante difundida na literatura refere-se à atribuição generalizada do elemento humano como o maior agente responsável pelos acidentes no setor aéreo (NASA, 1996). Nas plantas nucleares, o percentual atribuído a erros humanos está situado na faixa de 50% a 70% (LaSala, 1998).

Naturalmente, o resultado destas estatísticas não deve surpreender, desde que o elemento humano está de fato, direta ou indiretamente, envolvido na maioria dos acidentes que ocorrem nas plantas industriais de qualquer natureza. No transporte aéreo, o

fator humano é representado pela figura dos pilotos, controladores de tráfego aéreo, equipes de manutenção e operadores de terra.

Contudo, segundo Johnson (1980) *apud* Leveson (1995), por meio de uma investigação mais detalhada sobre um determinado acidente, invariavelmente foram encontrados como causas dos acidentes, condições não seguras dos equipamentos ou sistemas. Dessa forma, apesar dos percentuais de 60 a 80% dos acidentes, em várias indústrias pesquisadas, serem atribuídos indistintamente ao fator humano, determinou-se que em 75% destes casos, diversas funcionalidades do sistema de segurança não operavam corretamente e precediam da ação do operador.

Em sistemas críticos de segurança, o erro humano é definido como qualquer desvio no desempenho de uma sequência de ações especificadas ou prescritas. Contudo, instruções e procedimentos escritos quase nunca são seguidos. Estudos realizados com operadores em ambientes de sistemas críticos complexos de alto risco, como nas plantas nucleares, modificações nas instruções são repetidamente encontradas e a violação das regras parece ser bastante compreensível, em face da carga de trabalho que os operadores são submetidos (Leveson, 2002).

Nestas situações, existe um conflito básico entre o erro visto como um desvio dos procedimentos normativos e, o erro visto como um desvio dos procedimentos efetivamente utilizados racionalmente e usualmente. Como implicação, após a análise minuciosa de um acidente, será fácil encontrar alguma pessoa envolvida no fluxo dinâmico dos eventos e que tenha violado as regras formais, seguindo-se a prática estabelecida em vez da prática especificada. Portanto, devido aos desvios frequentes da prática estabelecida, a partir de instruções e regras normativas de trabalho, não deixa de ser surpresa que erros de operadores sejam encontrados como causa em 70 a 80% dos acidentes analisados (Leveson, 2002).

## **O Gerenciamento do Tráfego Aéreo**

O Gerenciamento do Tráfego Aéreo, *Air Traffic Management* (ATM), compreende

todo o processo de gestão, de organização, de utilização e de controle de recursos para viabilizar o melhor desempenho do tráfego aéreo do espaço controlado, sujeito às características das instalações aeroportuárias, dos auxílios à navegação, das aeronaves, das condições de vôos, da previsão dos movimentos, da evolução do tráfego, entre outras. Em linhas gerais, tem como objetivo permitir às operadoras cumprirem seus tempos de vôo, pousos e decolagens planejados e aderirem a perfis de vôos com um mínimo de constrangimento, sem o comprometimento dos níveis de segurança acordados (Machado, 2000).

Deve ser ressaltado que, em termos de responsabilidade, o piloto em comando tem a autoridade decisória em todos os aspectos relacionados à operação da aeronave, sendo de sua responsabilidade que as operações sejam realizadas de acordo com as regras predefinidas, podendo delas se desviar em situações absolutamente necessárias no atendimento às exigências de segurança (Sales, 2002).

O sistema de controle de tráfego aéreo é organizado de forma a disponibilizar diversos serviços e facilidades que incluem (Perry, 1997):

- Monitoração das aeronaves no solo e autorização de pousos/decolagens pela torre de controle;
- Controle de ascensão e aproximação das aeronaves de/para aeroportos pelos radares terminais de controle de aproximação;
- Controle das aeronaves em espaços setorizados e em altas altitudes entre aeroportos pelos diversos centros de controle ao longo das aerovias. Cada controlador de tráfego aéreo é responsável por um setor do espaço aéreo da ordem de vários milhares de pés de altitude e desde 20 a 200 milhas náuticas de extensão (1 milha náutica = 6.080 pés = 1.853 metros).

O espaço aéreo de um país é dividido em classes com requisitos específicos e regras de operação distintas para cada classe do espaço aéreo, sendo definidas pela Organização da Aviação Civil Internacional,

ou *International Civil Aviation Organization* (ICAO).

Segundo Weigang (1994) e Sales (2002), o espaço aéreo brasileiro é dividido em:

- Espaço aéreo não controlado: nestes espaços, os próprios pilotos são responsáveis pela separação entre as aeronaves. Portanto, o serviço de separação entre aeronaves não é de responsabilidade do *Air Traffic Control* (ATC), independente das condições meteorológicas.
- Espaço aéreo controlado: corresponde aos espaços aéreos onde se prestam os serviços de controle de tráfego aéreo ATC. São divididos em cinco regiões e administrados pela Diretoria de Eletrônica e Proteção ao Vôo (DEPV) por meio de centros denominados de Serviços Regionais de Proteção ao Vôo (SRPV) e pelo Centro Integrado de Defesa Aérea e Controle do Tráfego Aéreo (CINDACTA). O SRPV corresponde aos órgãos regionais da DEPV, cuja finalidade é facilitar as tramitações referentes à proteção ao vôo.
- Espaço aéreo condicionado: aquele restrito à circulação aérea geral e de dimensões definidas, constituindo-se de áreas proibidas (vôo não permitido em áreas próximas a refinarias, fábricas de explosivos, usinas hidroelétricas e áreas de segurança nacional), restritas (situações de exercício de tiro, lançamento de foguetes e pára-quedismo) e perigosas (áreas onde existam riscos em potencial como no treinamento de aeronaves civis). Os limites são indicados nas cartas aeronáuticas e manuais da DEPV, sendo estabelecido em caráter temporário ou permanente.

O serviço de tráfego aéreo, *Air Traffic Services* (ATS), é prestado em todo espaço aéreo brasileiro, sendo divididos em Serviço de Controle de Tráfego Aéreo (ATC), Serviço de Informação ao Vôo (FIS) e Serviço de Alerta (AS).

## Sistemas de Navegação Aérea e sua evolução

A partir do início da década de 80, nos principais países desenvolvidos, uma carga progressiva de trabalho foi imposta aos centros de controle de tráfego aéreo como consequência do aumento no volume do tráfego aéreo de passageiros. Nesse período, no Brasil, o aumento anual no fluxo de passageiros no Aeroporto Internacional de Guarulhos cresceu a uma taxa média de 7% a.a. (Weigang, 1994).

Vários fatores limitantes na atual plataforma podem acelerar a saturação do sistema. Esses fatores incluem a utilização ineficiente do espaço aéreo (rotas prédeterminadas), uso de equipamentos obsoletos em operação nos centros de controle de tráfego aéreo, comunicação restrita e congestionada (voz) entre aeronaves e o centro de controle (ATC) e pouca flexibilidade na navegação através do uso de estações transmissoras fixas, VOR (\*<sup>1</sup>), em terra (Tomlin; Pappas; Sastry, 1998).

Dessa forma, com a saturação da atual plataforma, é possível que os requisitos mínimos de segurança, em situações onde o tráfego aéreo seja demasiadamente alto, sejam comprometidos. Outrossim, o aumento de gastos extras com combustíveis nos circuitos de espera e de tempo para pousos e decolagens pode se tornar rotina, gerando como consequências, atrasos e insatisfação por parte dos usuários finais. Nesse contexto, objetivando o atendimento da demanda prevista no futuro próximo, torna-se imperativo o desenvolvimento e implementação de uma nova plataforma para o setor aéreo de transporte de passageiros.

Portanto, um modelo de gestão de risco baseado no método Bow-Tie, proposto no item 7, visa contribuir para superar as limitações do sistema atual e satisfazer a evolução da demanda do tráfego aéreo e dos requisitos dos usuários em termos de eficiência e economia, mantendo ou

---

<sup>1</sup> (\*) VOR (VHF Omni directional Range): sistema de navegação em terra para a transmissão de cursos de navegação. Cada VOR é designado com uma frequência entre 108,10 e 117,90 MHz.



melhorando os níveis de segurança existentes do sistema aéreo brasileiro.

## 6. AS METODOLOGIAS DE GESTÃO DE RISCO E O MÉTODO BOW-TIE

A metodologia proposta apontada se deu através de cotejamento entre métodos existentes para definir o mais aderente às características das operações analisadas. Foram estudados três métodos de mitigação de risco normalmente usados na indústria internacional, notadamente nas atividades de engenharia. Os métodos estudados foram: o método baseado nas técnicas de avaliação de risco; o método baseado na investigação de acidentes; e o método baseado na filosofia de barreiras de segurança.

Foi feita a opção mais adequada ao ambiente aeronáutico, que é a metodologia de barreiras, já difundida no setor (Conceito do queijo suíço), e em especial o modelo Bow-Tie

O método Bow-Tie é uma poderosa ferramenta para a análise e gestão de riscos complexos e dinâmicos. Este método foi adaptado pela Shell nos anos 90 e hoje é largamente utilizado por empresas da área de energia e transporte dentre outras. A análise de construção de cenários se concentra esquematicamente no Evento Indesejado, o qual representa a não conformidade do processo de gestão/operação de um sistema e é o ponto de partida para a metodologia proposta.

No nosso caso específico, o evento indesejado é a impossibilidade da aeronave aterrisar por perda de capacidade operacional do aeroporto destino.

O evento que não se quer que ocorra é colocado no centro do esquema. No lado esquerdo, estão listadas as causas potenciais que podem eventualmente provocar a geração do evento.

No lado direito, as potenciais consequências, caso o evento ocorra são listados (Figura 4).

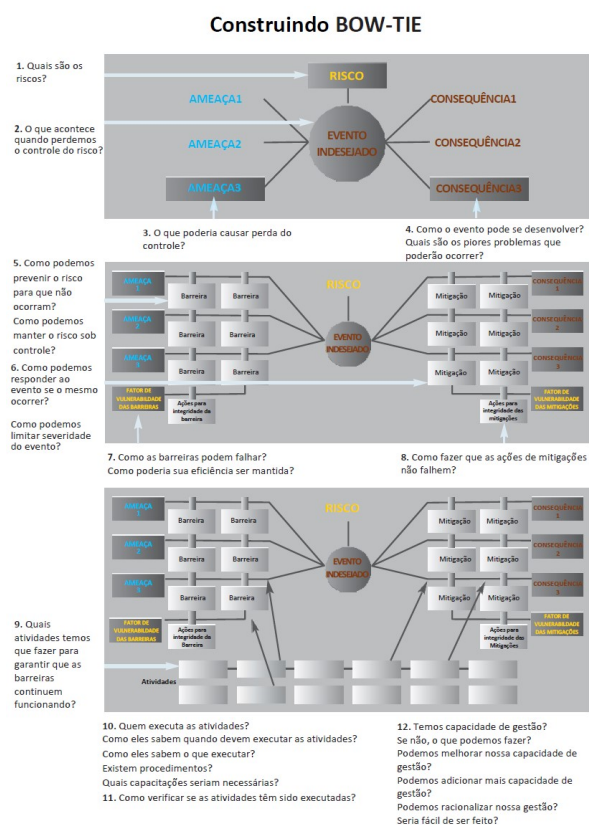


Figura 4: Modelo Bow -tie (Autores)

O artigo *Bow Tie, An Elegant Solution?* descreve o método como uma solução forte para o gerenciamento de riscos. O método do Bow-Tie fornece uma visualização prontamente compreensível das relações entre as causas de transtornos de negócios, a escalada de tais eventos, os controles que impedem o evento e as medidas de prontidão que limitam o impacto comercial. Mais importante ainda, as medidas preventivas e atenuantes estão ligadas a tarefas, procedimentos, indivíduos e competências responsáveis. Bow-Tie se originou como um método para avaliar perigos e riscos operacionais, embora as origens exatas da metodologia sejam um pouco nebulosas. A primeira menção parece estar em um curso de treinamento da *Imperial Chemical Industries* a partir de 1979. Indubitavelmente, o Royal Dutch/Shell Group foi a primeira grande empresa a integrar o método Bow-Tie em suas práticas comerciais e é creditada pelo desenvolvimento da técnica a qual é amplamente utilizada atualmente.

A Figura 5, a seguir, demonstra o esquemático do método simples na sua filosofia, porém poderoso nos seus resultados.





**Figura 5: Construindo Bow-tie (Adaptação Autores)**

## 7. PROPOSIÇÃO DE DESENVOLVIMENTO DE UM MODELO DE RISCO PARA DECISÃO DE ESCOLHA DE AEROPORTO ALTERNATIVO

O desenvolvimento do modelo proposto objetiva tratar o evento indesejado, o qual é a impossibilidade da aeronave aterrisar por perda de capacidade operacional do aeroporto destino.

O modelo possui as seguintes fases:

- 1- Identificação dos cenários geradores do evento indesejado;
- 2- Validação dos cenários com os experts aeronáuticos;
- 3- Geração das fichas de risco Bow-Tie conforme exemplo da Figura 6;
- 4- Estabelecimento das ameaças ao sistema aeronáutico quanto ao evento indesejado;
- 5- Desenvolvimento das barreiras às ameaças do evento;
- 6- Avaliação das consequências do evento;
- 7- Estabelecimento das mitigações;

8- Desenvolvimento dos planos de respostas a partir das mitigações estabelecidas;

9- Hierarquização da implementação dos investimentos nas barreiras e mitigações de consequências;

10- Avaliação da redução do risco residual.

Este modelo deverá atender as contingências necessárias para evitar o evento indesejado.

O processo decisório de onde sairão as opções para aeronave definir seu novo destino encetará os cenários estáticos e dinâmicos avaliados desde sua aterissagem, na origem do voo, até a aproximação do aeroporto destino.

Ele desenvolverá as alterantivas de pouso levando em conta fatores operacionais da aeronave e do tráfego aéreo, econômicos, e tecnológicos implícitos à decisão.

O recente episódio da “greve dos caminhoneiros” afetando a questão de disponibilidade de combustível em aeroportos brasileiros, e em especial uma característica de *hub airport*, como Brasília, mostra a importância deste modelo, e nos leva a estender este modelo futuramente para gestão de risco cruzado de colapso associado em toda malha aeroportuária.

FICHA ESTRUTURANTE DE RISCO							Nº/ID: 000
Grau da Matriz de Risco (Tipologia de Risco X Área de Risco)							00
Negócio	Terminais						
Unidade	Aeroporto						
Área	01 Administrativo Financeiro / 02 Abrigagem / 03 Armazenagem / 04 Comercial / 05 Controle - Tráfego / 06 DHO / 07 Engenharia / 08 Jurídico / 09 Manutenção / 10 Marketing / 11 Meio Ambiente / 12 Operações / 13 Qualidade / 14 Segurança do Trabalho / 15 Segurança Patrimonial / 16 Seguros / 17 Suprimentos / 18 Off Site						00 Indicação de área hegemônica do risco e áreas adjacentes
Área de Risco / Perigo	Transport		Load/Unload	Operation / Control	Plant Process		
	Pátio/Pista	Vôo/Aeronave	Movimentação Horizontal Vertical	Tripulação / operadores de terra	Operação Geral do Terminal	Off Site	Condições atmosféricas
	X	X	X	X	X	X	X
Tipologia do Risco	Operacional	Ambiental	Patrimonial	Saúde Ocupacional	Legal e Trabalhista	Externo / Offsite	Outro a especificar
	X	X	X	X	X	X	X
Risco Associado / Cenários Percebidos	Quais são os riscos?						
Evento Indesejado / Perturbador	O que acontece quando perdemos o controle do risco?						
Ameaças	Barreiras	EF-Fatores de Vulnerabilidade das Barreiras	EFC- Ações para Integridade da Barreira	Mecanismos associados às Barreiras	Observações Referentes a Políticas, Processos de Planejamento, Execução e Operação		
O que poderia causar perda do controle?	Como podemos prevenir o risco para que não ocorram? Como podemos manter o risco sob controle?	Como as barreiras podem falhar?	Como poderia sua eficiência ser mantida?	Quais atividades temos que fazer para garantir que as barreiras continuem funcionando?	Quem executa as atividades? Existem procedimentos? Quais capacidades seriam necessárias? Temos capacidade de gestão?		
Consequências	Mitigações	EF-Fatores de Vulnerabilidade das Mitigações	EFC- Ações para Integridade de Mitigações	Mecanismos associados às Mitigações	Cenários e Impactos Possíveis		
Como o evento pode se desenvolver? Quais são os piores problemas?	Como podemos responder ao evento se o mesmo ocorrer? Como podemos limitar severidade do evento?	Como as mitigações podem falhar?	Como fazer que as ações de mitigações não falhem?	Quais atividades temos que fazer para garantir que as mitigações continuem funcionando?	Conforme Conceito de Geração de Cenários e Priorização dos Módulos da Metodologia Proposta		

Figura 6: Ficha estruturante de risco (Autores)

## 8. REFERÊNCIAS

CHEN, Z. et al. A total environmental risk assessment model for international hub airports. *International Journal of Project Management*, Volume 29, Issue 7, October 2011, Pages 856-866.

GARDNER, L., SARKAR, S. A Global Airport-Based Risk Model for the Spread of Dengue Infection via the Air Transport Network. *PLOS ONE* 13(3): e0194955. Disponível em: <<https://doi.org/10.1371/journal.pone.0072129>>. Acesso em 29 Maio 2018.

JOHNSON Jr., N. System reliability and MTBF. *Reliability Review*, v. 10, p. 3-4, December, 1990.

LaSala, Kenneth P. Human Performance Reliability – A Historical Perspective, *IEEE Transactions on Reliability*, vol 47, no.3-SP. September 1998.

LEMES, M.J.R. Complexidade, acoplamento e criticidade (C2A) como indicadores de risco em projetos de sistemas. 2012. Ed. Rev.: São Paulo, 278 p. Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo.

LEVESON N., 1995, A new approach to system safety engineering, M.I.T.

LEWIS, S., HURST, S. Bow Tie, An Elegant Solution? *Strategic Risk Magazine*, 8 November, 2005.

NETJASOV, F., JANIC M. A review of research on risk and safety modelling in civil aviation. *Journal of Air Transport Management*, Volume 14, Issue 4, July 2008, Pages 213-220.

OGATA, P. H. Avaliação do Perigo de Colisão entre Aeronaves em Operação de Aproximação em Pistas de Aterrissagem Paralelas.

PERRY, T. S. In Search of the Future of Air Traffic Control - The Truth about Air Traffic Control. *IEEE Spectrum*, August 1997.

SCARDIGLI, V. Um Mundo Totalmente Digital? *Revista Eletrônica Le Monde Diplomatique*. Ano 3, no 33 – Tradução Fábio Castro, Outubro, 2002.

SILVA FILHO, R. I. AGUIAR, M.A. KOVÁCS, Z. L. Um Estudo de Caso Genérico de Diagnóstico Preditivo para Sistemas Complexos, Laboratório de Automação e Controle POLI/USP.

WICKENS, C. D., et al. The Future of Air Traffic Control - Human Operators and Automation. *National Academy Press*, 1998.

Weigang, L. Knowledge-Based System for Air Traffic Flow Management. 159p. Tese ITA. SP, 1994.