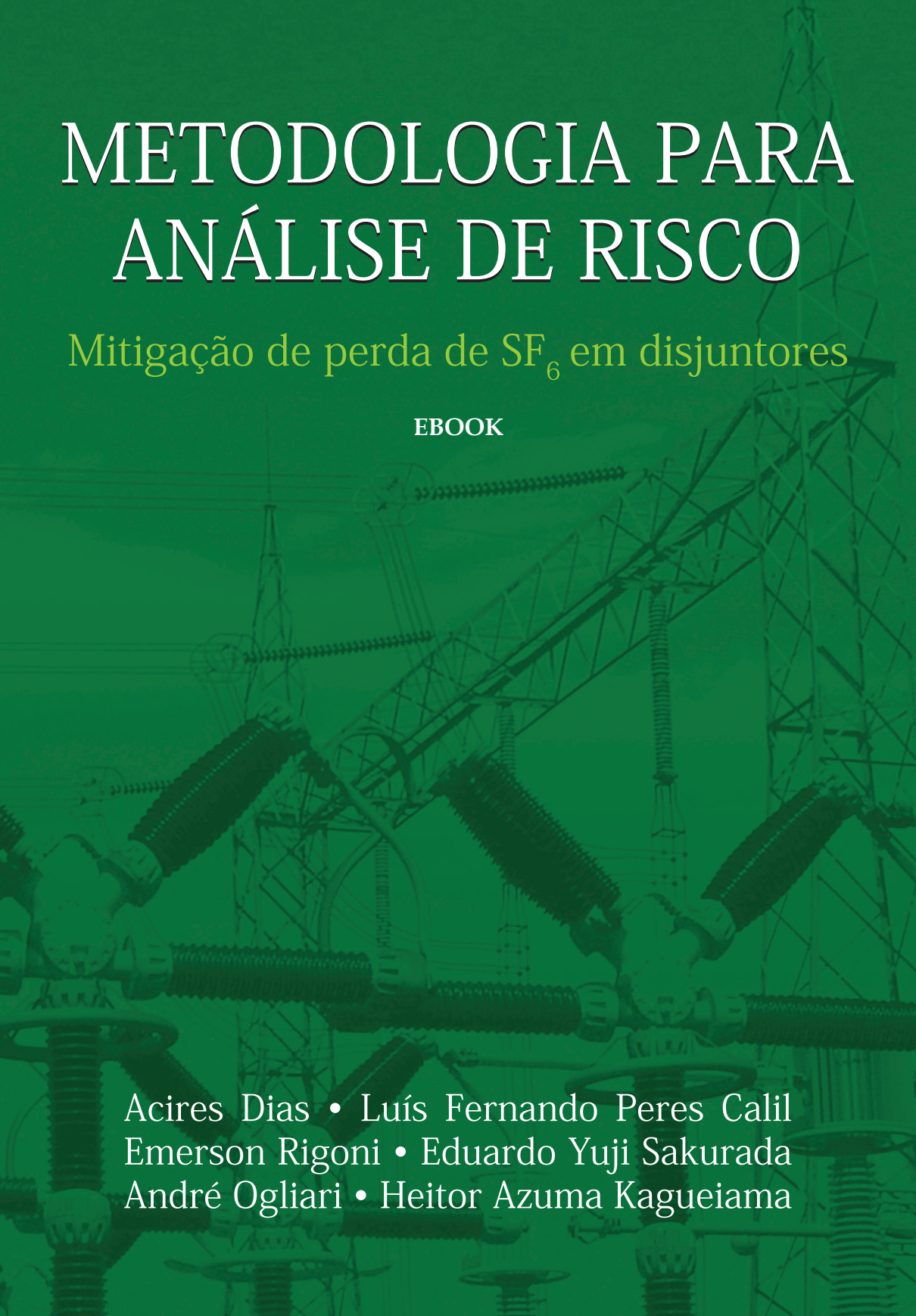
METODOLOGIA PARA ANÁLISE DE RISCO

Mitigação de perda de SF_6 em disjuntores

EBOOK



Acires Dias • Luís Fernando Peres Calil
Emerson Rigoni • Eduardo Yuji Sakurada
André Ogliari • Heitor Azuma Kagueiama

Acires Dias
Luís Fernando Peres Calil
Emerson Rigoni
André Ogliari
Eduardo Yuji Sakurada
Heitor Azuma Kagueiama

METODOLOGIA PARA ANÁLISE DE RISCO

Mitigação de perda de SF_6 em disjuntores

Equipe técnica da Eletrosul
Altair Coutinho Azevedo Jr.
Clóvis Nicoleit Carvalho
Alzete Martins Quadros
Jovani Afonso de Souza

Florianópolis
2013

EBOOK

Capa, Projeto Gráfico e Diagramação
STUDIO S Diagramação e Arte Visual
studios@studios.com.br (48) 3025-3070

Edição e preparação de originais
Fábio Brüggemann

M593 Metodologia para análise de risco : mitigação de perda de SF_6 em disjuntores / Acires Dias ...[et al.]. – Florianópolis : [S.n.], 2013.
303p.

ISBN: 978-85-98128-61-0 (ebook)
Inclui bibliografia

1. Análise de risco – Metodologia. 2. Disjuntores elétrico – Manutenção e reparos. 3. Confiabilidade (Engenharia). 4. Manutenção Produtiva total. 5. Redes bayesianas. I. Dias, Acires.

CDU: 621.31

Catalogação na publicação por: Onélia Silva Guimarães CRB-14/071

SUMÁRIO

AGRADECIMENTOS

Esta obra é resultado da crença e do entusiasmo de muitas pessoas e instituições que atuam no setor elétrico e de ensino, tendo por meta facilitar a inter-relação entre empresas e universidades cujas ações contribuíram para organizar e potencializar o conhecimento tácito e explicito em prol da sustentabilidade.

Desde a fase da formulação do projeto MitiSF_6 houve grande empatia entre os integrantes da ELETROSUL e da universidade, que facilitou a sistematização da proposta de metodologia e programação das ações para o desenvolvimento da pesquisa com o objetivo de mitigar a emissão de SF_6 em todos os setores da empresa. Esse espírito colaborativo e motivador, para se obter resultados positivos, aconteceu em toda a execução do projeto, em todos os setores que foram visitados dentro da empresa e em outras empresas do setor elétrico no Brasil e no exterior.

Somos muito gratos a todas as pessoas e organizações que contribuíram com o projeto de pesquisa que resultou na construção deste livro. Porém, há instituições e pessoas que atuaram diretamente no projeto, ao longo de todo o processo da pesquisa. A elas segue um agradecimento especial:

À ELETROSUL e a todos os seus colaboradores, pela qualificação técnica e gerencial do pessoal da empresa, pela clareza de objetivo e disposição em investir tempo, capital intelectual, equipamentos e dinheiro para investigar os procedimentos de manutenção, operação, armazenamento e tratamento do SF_6, cujos resultados foram importantes para tornar-se uma empresa de referência no setor, ao mesmo tempo em que contribui com todo o setor elétrico e educacional. Destacamos um agradecimento especial à equipe da ELETROSUL que atuou diretamente no projeto: aos engenheiros Clóvis Nicoleit Carvalho, gerente do projeto, Altair Coutinho de Azevedo Jr., gerente de manutenção, e aos químicos Alzete Martins Quadros e Jovani Afonso

de Souza. Este agradecimento é extensivo aos colegas da empresa que participaram das reuniões, visita aos laboratórios, oficinas, seminários de avaliação dos relatórios e na discussão de diretrizes.

À ANEEL, por contribuir com a pesquisa e extensão, e pelo desenvolvimento de políticas de financiamento que motivam as atividades compartilhadas entre empresa e instituições de pesquisa e ensino.

Às empresas ITAIPU-Binacional e Furnas Centrais Elétrica, por receberem a equipe de pesquisadores e demandarem esforços para apresentar alternativas de solução que contribuísse com a mitigação da emissão de SF_6 no âmbito do setor elétrico nacional. À CEPEL–Centro de Pesquisas de Energia Elétrica (Eletrobras) por receber os pesquisadores e participarem dos seminários de apresentação do projeto, responderem os questionários relativos à temática da pesquisa e socializarem o conhecimento conosco.

Em nível internacional, agradecemos à equipe da empresa ELIA, com sede em Bruxelas, Bélgica, ao órgão governamental de meio ambiente LNE – Departement Leefmilieu, Natuur en Energie e empresas ELTEC BVBA e representante da DILO, com sede em Louven, Bélgica. Agradecemos também o sr. Robert Jeanjean, da RJ Consulting, e aos gerentes e técnicos da empresa AREVA, com sede em Lyon, França. A equipe de gerência de manutenção e técnicos da empresa IBERDROLA, com sede em Madrid, Espanha. Todas estas empresas receberam a equipe do projeto (ELETROSUL e UFSC) para discussão e troca de experiências no uso e tratamento de SF_6 no setor elétrico.

Os autores e pesquisadores são gratos à Fundação do Ensino da Engenharia em Santa Catarina — FEESC, com sede no Centro Tecnológico da UFSC, pelo apoio durante todo o desenvolvimento do projeto.

À Universidade Federal de Santa Catarina, especialmente ao Departamento de Engenharia Mecânica e ao Centro de Engenharia da Mobilidade, por disponibilizar os pesquisadores professores e estudantes para participarem deste projeto de pesquisa e da edição do livro.

Queremos ainda agradecer a todas as pessoas que fazem parte das instituições citadas, aos estudantes que atuaram no projeto ao longo da pesquisa, aos professores Victor Juliano De Negri e Nelson Back, que ajudaram nas discussões das diretrizes e análise dos resultados.

Os autores

APRESENTAÇÃO

Durante séculos, mais principalmente no início do século XX, a sociedade se utilizou dos recursos naturais imaginando serem infinitos. As organizações focaram seus esforços na obtenção da maximização do lucro, descartando a preocupação com a questão social e ambiental impactada pelos seus negócios. Isso desencadeou um desequilíbrio na rede ecológica natural.

Com as mudanças climáticas e com a perda da qualidade de vida das pessoas nas últimas décadas, buscam-se soluções para grandes problemas contemporâneos por meio de ações dos movimentos sociais, governamentais, empresas públicas e privadas, pois reequilibrar as forças naturais e a espécie humana é fundamental para a sobrevivência das futuras gerações.

Então, buscou-se um novo conceito de desenvolvimento, que vem ganhando força no cenário mundial e se difunde como uma proposta de desenvolvimento diferenciada, proporcionando o surgimento de um novo paradigma global, amplamente baseado em avanços científicos e tecnológicos.

A sustentabilidade surgiu como um conceito sistêmico onde se conciliam os aspectos econômico/financeiros, sociais e ambientais, de forma a atender as necessidades humanas e ao mesmo tempo preservando a biodiversidade e os ecossistemas.

A construção de uma consciência ambiental global é indispensável, e o intuito de transformar uma empresa tradicional em uma organização sustentável é cada vez mais imperativo. É necessário agir de forma ética e transparente, sendo responsável no que afeta a todos os públicos com a qual se relaciona. Portanto, deve dialogar e incorporar compromissos no planejamento de suas atividades, buscando ser inserida e reconhecida pela sociedade como um organismo sustentável.

A visão de que é preciso "pensar globalmente e agir localmente" está diretamente vinculada ao fato que, no nível local, os problemas ambientais deixam de ser difusos e se tornam pontuais e pessoais. A situação planetária serve de alerta, mas, para tomar medidas concretas, cabe agir no plano local. As medidas concretas necessárias para remediar a situação são diferentes em cada localidade, exigindo participação direta das pessoas que conhecem a sua própria realidade.

Na busca pela sustentabilidade e com a multiplicação dos riscos socioambientais nas últimas décadas, cada vez mais é necessário buscar a conscientização da sociedade para noções de sustentabilidade que ultrapasse a questão ambiental.

A Eletrobras ELETROSUL, uma empresa sustentável, responsável social e ambientalmente, promove a efetiva inserção regional e do desenvolvimento sustentável, implantando ações e medidas que subsidiem as decisões estratégicas aos conceitos de sustentabilidade e equidade entre gerações, promovendo, no alinhamento estratégico, o apoio e incentivo ao desenvolvimento tecnológico, a inovação e o conhecimento, por meio de estudos e pesquisas.

A melhoria da qualidade de vida da população das áreas onde a empresa tem empreendimento é uma ação prioritária, de forma a implementar medidas como Políticas e Programas de Governo Federal que visam superar as questões que dificultam a eficiência alocativa dos recursos, valorizar as potencialidades locais, reduzir as desigualdades regionais e promover a inclusão social.

Importante destacar que a Eletrobras ELETROSUL, alinhada às políticas energéticas e socioambientais do Governo Federal, investe em fontes de energia renováveis, como a hidráulica, e em novas fontes renováveis e limpas, como a eólica, a solar e a biomassa, contribuindo para o desenvolvimento sustentável do país e, diretamente, com a população que vive nas áreas de influência dos seus empreendimentos, reforçando, assim, as iniciativas adotadas para levar energia a toda a população.

A Eletrobras ELETROSUL vem implementando um modelo de gestão que busca o desenvolvimento sustentável que vai além do foco no lucro financeiro produzido pelas suas atividades, olhando as demais circunstâncias do processo de desenvolvimento, como a preservação das fontes de recursos naturais, que são finitas. Assim, numa época de grandes investimentos e desenvolvimento do Brasil,

alavancadas pelo Programa de Aceleração do Crescimento – PAC, do Governo Federal, a Eletrobrás ELETROSUL desenvolve projetos e realiza investimentos com responsabilidade socioambiental, buscando a sustentabilidade desses projetos e da própria empresa.

Medidas sistemáticas para minimizar os impactos ambientais têm sido realizadas no sentido de combater as agressões impostas pela atividade econômica e pela ação do homem.

Desta forma, a Eletrobras ELETROSUL, visando se solidificar como uma empresa sustentável, incentiva e promove o desenvolvimento de estudos e pesquisas que venham a contribuir com a sustentabilidade para a empresa e para o planeta.

Neste contexto, e alinhado ao Protocolo de Kyoto, que determina a redução média global em 5,2% da emissão de gases poluentes de 2008 até 2012, aprovou e apoiou o desenvolvimento do projeto ANEEL "MitiF6", que tem por objetivo identificar os pontos de perda de hexafluoreto de enxofre - SF_6 e propor soluções.

Esta questão é importante para a empresa, pois na geração e transmissão de energia elétrica, na qual a utilização do SF_6 como dielétrico em equipamentos de transmissão e distribuição de energia elétrica vem provocando impactos ambientais decorrentes dos efeitos de um gás com maior potencial de dano no que se refere ao efeito estufa, é necessário praticar ações mitigadoras urgentes.

A presente obra apresenta uma pesquisa que mostra medidas para identificar os pontos de perda de SF_6 e propõe soluções para abrandá-las, bem como o gerenciamento de risco que objetiva maximizar resultados positivos e minimizar negativos. O projeto contempla também a Metodologia de Análise de Risco, que compõe o gerenciamento de risco.

Apesar de conter uma ampla base teórica sobre o SF_6 e sobre a Gestão de Risco, este livro, é, sobretudo, uma obra que visa contribuir para a construção de um projeto integrado no Sistema ELETROBRAS.

Por fim, gostaríamos de agradecer aos autores, pela dedicação ao escrever esta obra, que contribuirá para os profissionais e especialistas do Setor Elétrico Brasileiro, e, por consequência, na preservação do nosso Planeta.

Diretoria Executiva da Eletrobras ELETROSUL

Capítulo 1

INTRODUÇÃO

Este livro foi organizado para divulgar o conhecimento resultante das atividades de pesquisa efetuadas durante o desenvolvimento do projeto "análise e desenvolvimento de procedimentos para operação e manutenção de disjuntores visando mitigar a emissão de SF_6", chamado de MitiSF_6 (ELETROSUL, 2008). O objetivo final do projeto foi apresentar procedimentos para mitigar a emissão do Hexafluoreto de Enxofre (SF_6) utilizado em equipamentos elétricos isolados com este gás, normalmente utilizado em sistemas de geração, transmissão e distribuição de energia elétrica. O MitiSF_6 abordou apenas os sistemas de transmissão de energia elétrica, com enfoque maior para os Disjuntores, componentes da Rede Básica (≥ 230kV).

1.1 PARA QUEM SE DESTINA O LIVRO

Os estudos foram desenvolvidos com o objetivo de mitigar a emissão do gás SF_6. Para tanto, utilizaram-se algumas técnicas de análise de risco para estudar e melhor compreender os processos de operação e manutenção de disjuntores isolados a SF_6, bem como os procedimentos para aquisição, armazenamento, transporte e recuperação do gás na empresa.

Dado que a perda de SF_6 tem consequência direta para o ambiente e para a segurança humana, a abordagem centrou-se em análise de risco. Tal abordagem ganha muita importância quando a falha de um sistema implica no comprometimento da continuidade da função principal do sistema, que, nesse caso, está associada à transmissão de energia elétrica. Isso porque, a falha no disjuntor pode levar a interrupção de transmissão de energia elétrica.

Nesta perspectiva, mostra-se alguns resultados da pesquisa para socializar o conhecimento em análise de risco com todos que

atuam em manutenção e operação de sistemas técnicos, cuja falha tem implicação na segurança humana e ambiental ou na continuidade da função principal. É um livro que tem o foco na aplicação, e visa contribuir com os processos de capacitação em técnicas e metodologia de análise e gestão do risco. Evidentemente, tem foco também nos sistemas inerentes à distribuição de energia elétrica, principalmente no contexto da manutenção. Mas as técnicas estudadas são de ampla aplicação e de interesse para a formação de nível técnico, tecnólogo e de engenharia. Será também importante ferramenta para a capacitação corporativa das empresas ligadas ao setor.

Para melhor situar o leitor, faz-se, no capítulo 2, uma apresentação do projeto de pesquisa MitiSF_6. Nos capítulos 3 e 4 aborda-se respectivamente os conceitos de gerenciamento de risco em sistemas técnicos e a metodologia de gerenciamento de risco. Para o tratamento do risco em sistemas, várias técnicas são utilizadas. Apresenta-se as seguintes: IDEFØ (*integrated definition for function modeling*) utilizada para organizar a análise dos processos e ajudar na comunicação entre os vários agentes de um processo de análise, descrita no capítulo 5; análise funcional e síntese funcional, apresentada no capítulo 6; análise dos modos de falha e efeitos (FMEA - *failure mode and effects analysis*) no capítulo 7; análise de árvore de falhas (FTA - *fault tree analysis*) no capítulo 8; análise por árvore de evento (ETA - *event tree analysis*) no capítulo 9; redes bayesianas no capítulo 10 e; análise de eventos por rede causal (CNEA - *causal network event analysis*) no capítulo 11.

Como o projeto de pesquisa teve um foco específico em disjuntores isolados a SF_6, apresenta-se, no capítulo 12, a caracterização do gás Hexafluoreto de Enxofre (SF_6), e, no capítulo 13, os aspectos gerais e as partes constituintes dos disjuntores isolados a SF_6.

Nos capítulos finais desenvolve-se a metodologia de análise de risco e o uso das técnicas para mitigar a emissão de SF_6. Assim, tomando-se por base o projeto de pesquisa, apresenta-se no capítulo 14 a metodologia de análise de risco, com alguns exemplos desenvolvidos ao longo do projeto MitiSF_6; aborda-se também as contribuições resultantes do projeto de pesquisa, organizadas no contexto da metodologia e das técnicas utilizadas.

As técnicas apresentadas, de forma geral, estão presentes também nas abordagens sobre os atributos de qualidade, mais es-

pecificamente, confiabilidade, mantenabilidade e segurança. Estes três atributos, por estarem presentes no cotidiano de manutentores, são apresentados a seguir dado que as técnicas usadas na análise de risco são as mesmas utilizadas nesses atributos. Além disso, o conteúdo técnico é estruturante para organizar o conhecimento em gestão da manutenção, principalmente, na manutenção centrada em confiabilidade (MCC ou RCM – *reliability centered maintenance*) e manutenção produtiva total (TPM – *total productive maintainance*). Entende-se que o livro também interessa aos que atuam em qualquer um desses modelos de gestão, e por isso será feito uma breve apresentação dos mesmos. Observa-se, porém, que dependendo do atributo considerado, o resultado será específico ou próprio para cada uma das técnicas aqui apresentadas.

1.2 ATRIBUTOS DO PRODUTO

1.2.1 CONFIABILIDADE

Confiabilidade é um atributo muito importante para produtos e sistemas e permeia todo o ciclo de vida. É multidisciplinar e engloba especialidades e especialistas em engenharia, estatística, matemática, computação, física, química, entre outras. Há autores que denominam de Engenharia de Confiabilidade. Sua aplicação está estruturada em técnicas de análise e de síntese, entre as quais: análise da árvore de falha (FTA), análise do modo e do efeito da falha (FMEA), análise do modo de falha, do efeito e da criticidade (FMECA), análise da causa raiz (RCA - *Root Cause Analysis*), análise da causa de falha de modo comum e de técnicas associadas ao atributo da qualidade (DIAS, 2005).

De certa maneira, a utilização dessas diferentes técnicas ou modelos de análise necessita de informações básicas, registradas com um mínimo de conhecimento técnico, linguagem apropriada, obtidas ao longo do ciclo de vida dos itens, de preferência de forma constante.

A confiabilidade é um elemento chave para o sucesso dos ativos no setor comercial, industrial e para o meio ambiente como um todo. A confiabilidade se propõe a determinar a probabilidade do ativo cumprir sua função ao longo do ciclo de vida. A partir das técnicas

de análise é possível gerenciar o ciclo de vida do item, na medida em que estabelece estruturas e técnicas para definir a probabilidade de ocorrência da falha baseado no tempo, acompanhar o desenvolvimento da falha baseado na condição ou eliminar a falha para um tempo de vida considerado a partir de ações de projeto.

A confiabilidade, segundo a norma ABNT NBR 5462 (1994), é definida como a probabilidade de um ativo desempenhar uma determinada função, de forma adequada, durante um intervalo de tempo, sob condições especificadas. Há certamente outras definições, com mais ou com menos detalhamento. O importante é compreender que em qualquer que seja a definição de confiabilidade, quatro conceitos fundamentais ou categorias estão presentes: probabilidade, comportamento adequado, período de uso e condições de uso (DIAS, 1996). Detalhando cada uma dessas categorias tem-se:

- **Probabilidade**: expressa a possibilidade de ocorrência de um evento. É recomendável que se tenha um conhecimento prévio do comportamento do item a ser analisado, ou uma estimativa que sirva de referência para se fazer o cálculo da probabilidade. Normalmente, não existe uma única fórmula ou técnica para estimar a confiabilidade. São diversas as distribuições de probabilidade que podem ser utilizadas. Mas em qualquer das aplicações a qualidade da análise depende dos dados de entrada. Para produtos novos, a confiabilidade depende basicamente da qualidade do projeto do produto, da experiência da equipe de projeto, da organização do sistema de produção e do controle de qualidade utilizado no processo produtivo. Por isso, é normal fazer controle estatístico de processo, dado que, com o mesmo, pode-se estabelecer a probabilidade do produto ter confiabilidade igual a 100% antes de entrar em operação. Para produtos em operação a confiabilidade está estreitamente relacionada com a especificação de compra para a função que irá cumprir ao longo do ciclo de vida. A confiabilidade, por ser um atributo do produto, é definida no projeto. Em outras palavras, uma vez o produto pronto, está integrada ao mesmo, como se fosse um DNA do produto. Não há como mudar, a menos que se façam alterações no projeto. Assim, a manuten-

ção durante o ciclo de vida útil pode, no máximo, garantir a confiabilidade que foi especificada no projeto. Mesmo assim, é esperado que ao final do ciclo de vida haja a probabilidade crescente de falhas. Nessa perspectiva, a confiabilidade tende a zero quando a vida tende para o infinito, ou seja, a probabilidade de falha é de 100%.

- **Comportamento adequado**: para saber se o item tem ou não comportamento adequado é recomendável que tenha um padrão (*benchmarking*), um referencial a ser atingido ou já definido anteriormente. Nos casos em que se dispõe de informações estatisticamente consistentes, torna-se mais provável dispor de um padrão. No caso da não existência de dados, simplesmente estabelece-se uma meta a ser alcançada *a posteriori*. Em alguns casos há que considerar métodos que possibilitem transformar as informações qualitativas em quantitativas, de forma a criar uma referência que sirva de base em todo o ciclo de vida do produto. O padrão pode ser obtido por meio de estratégias de *marketing*, em normas técnicas, por exigências contratuais ou governamentais, requisitos de leis ou de histórico de falhas. Técnicas qualitativas e quantitativas existem para obter as informações necessárias para definir o comportamento adequado de um item, na perspectiva do atributo de confiabilidade.
- **Período de uso**: é expresso, normalmente, em função do tempo. Depende de informações que represente a expectativa de bom funcionamento do produto em relação ao ciclo de vida. Essa categoria chama a atenção do analista de confiabilidade para soluções de projeto relacionadas com métodos para evitar, prevenir ou acomodar as falhas. No primeiro caso é requerido produto robusto, com redundância de projeto, uso bem controlado e com gestão de manutenção apropriada, centrada em confiabilidade, ou centrada no risco. Projeto de produtos para prevenir falhas ao longo do período de uso vem com métodos de predição de falhas no item, com recomendação para uso de recursos de manutenção preventiva, preditiva, com prioridade para gestão de manutenção centrada em confiabilidade ou manutenção produtiva total. Métodos para acomodar falhas são os que admitem a ocorrência da falha. Contudo, para garantir

a função são adotados em conjunto com sistemas redundantes. Contudo, se a falha afetar a segurança humana ou ambiental deve ser evitado. Em qualquer situação, deve-se admitir que todo produto tem um ciclo de vida de uso definido, e que falhará ao longo do ciclo de vida. Por isso que a confiabilidade, embora seja um atributo definido no projeto, está sempre associada à mantenabilidade e à gestão de manutenção. Algumas medidas são recorrentes no período de uso, por exemplo: taxa de falha, tempo médio entre falhas (MTBF), tempo médio até a falha (MTTF), tempo médio até a primeira falha (MTTFF), tempo médio de reparo, tempo médio entre manutenção etc.

- **Condição de uso**: a condição de uso precisa ser bem definida, dado que o sucesso de um evento pode não se manter se as premissas de uso anteriormente estabelecidas forem modificadas. A condição de operação depende de aspectos técnicos e humanos. Essa está integrada a todo o ciclo de vida, desde a fase inicial ou de juventude, vida de uso e vida de desgaste. Os princípios utilizados na gestão para a produtividade total (TPM) são importantes para a integração entre confiabilidade, operação e manutenção.

1.2.2 MANTENABILIDADE

A função mantenabilidade é definida como a "capacidade de um item ser mantido ou recolocado em condições de executar suas funções requeridas, sob condições de uso especificadas, quando a manutenção é executada sob condições determinadas e mediante os procedimentos e meios prescritos" (ABNT, 1994). Por meios entendem-se inclusive os econômicos. Blanchard et al. (1995) diz que a mantenabilidade é um parâmetro de projeto, enquanto que a manutenção é uma consequência do projeto. O tempo médio de reparo ou tempo de manutenção, ou custo de manutenção dependem do projeto do item.

Deve-se entender também que é no projeto que se define toda a logística de suprimento, ferramentas, acesso aos itens, diagnóstico de falha e ciclo de vida na condição de tão bom quanto novo. Assim, a gestão da manutenção não pode modificar a habilidade do item ser mantido, a menos que: altere o projeto, substitua materiais, construa

ferramentas especiais, desenvolva programas de capacitação apropriados etc., para compensar o que deveria ter sido feito no projeto para a mantenabilidade.

Monchy (1989) utiliza o termo manutenabilidade para a mesma definição. Os que adotam essa terminologia querem enfatizar o ato de fazer manutenção, ou seja, expressar a habilidade do item sofrer manutenção. Manutenção, segundo Ferreira (1988), "é a ação de segurar com a mão, ato ou efeito de manter-se", o termo vem do latim *manutenere* (*manu* = mão + *tenere* = ter → ter na mão). Por vezes, é também utilizado o termo manutenibilidade, que indica a capacidade do item ser manutenível, ou seja, que "se pode manter ou manutenir" (FERREIRA, 1988). Em outras palavras, pode-se dizer que manutenabilidade indica a habilidade de manter, ou seja, está associado a quem faz; já manutenibilidade indica a possibilidade do item ser manutenível, quer dizer, a capacidade de sofrer manutenção.

A expressão mantenabilidade é etimologicamente apropriada e ganhou lugar na nomenclatura técnica em português após ser adotada pela norma NBR 5462 (ABNT, 1994). Também é mais aderente a nomenclatura técnica em inglês, que utiliza o termo *maintainability* para expressar a habilidade de ser mantido.

A mantenabilidade, embora seja um atributo definido no projeto, é efetivamente medida após falha do produto em operação, com a condição de recolocá-lo na condição de tão bom quanto novo, por uma gestão apropriada da manutenção. Para compor as medidas de mantenabilidade se utiliza técnicas iguais aos do atributo de confiabilidade para fazer diagnóstico de falhas, levantar requisitos de testabilidade, desenvolver análise da acessibilidade e testar a robustez em relação ao fator humano, tanto na contribuição para a falha quanto na percepção da falha. Influencia na medida de mantenabilidade características do produto como:

- Facilidade para detectar as falhas, precisão, segurança, economia em ser mantido, custo para recolocar na condição de tão bom quanto novo;
- Necessidades de recursos humanos especializados, equipamentos de testes, ferramental especial, de instalações adicionais, suporte logísticos etc.

1.2.3 SEGURANÇA

O atributo de segurança aqui expresso está relacionado com os modos de falha que geram desdobramentos na função do item de tal forma que podem afetar o homem, o ambiente ou o próprio sistema técnico. Assim, assume-se que segurança é a capacidade (ou habilidade) do item estar no estado de uso (função: estar em operação) e passar para o estado de falha (modo de falha: não estar em operação) e vice-versa, sem risco de dano para homem, ambiente e para o próprio sistema técnico.

Como será aprofundado no capítulo 3, o conceito de segurança relativa a danos (que em inglês é definido por *safety*) é distinto do conceito de segurança relativa a patrimônio e privacidade (em inglês, definido por *security*). Por exemplo, a segurança de patrimônio foca principalmente em ações maliciosas – tais como: invasões, atentados, sabotagem, vírus de computador. Este tema foge do escopo deste trabalho.

A definição de segurança, no contexto deste livro, fica mais apropriada se tomar o disjuntor isolado a SF_6 como exemplo. Como será mostrado nos capítulos seguintes, alguns modos de falha no disjuntor podem provocar o vazamento do gás, que se em ambiente fechado e em quantidades significativas tem chance de comprometer a saúde e até a vida dos que estiverem no ambiente. Nesse caso, o modo de falha tem consequência direta para a segurança humana. Também afeta o ambiente na medida em que o gás contribui para o efeito estufa. Além disso, em contato com o meio, pode gerar combinações tóxicas.

Em casos como esse é recomendável que o processo de análise da falha seja feito considerando as técnicas e meios de análise de risco. Por isso que análise de risco é o tema central do livro.

1.3 GESTÃO DA MANUTENÇÃO

1.3.1 MANUTENÇÃO CENTRADA EM CONFIABILIDADE

A Manutenção Centrada em Confiabilidade (MCC) teve suas origens na década de 50, como resultado de vários estudos de confiabilidade desenvolvidos pela indústria da aviação civil americana. Na década de 60 alguns conceitos da MCC ganharam importância na indústria aérea nos Estados Unidos da América.

Em 1967, representantes das linhas aéreas, fabricantes e o governo estadunidense apresentaram o MSG-1 (*Maintenance Steering Group* – Grupo Governamental "de Condução" da Manutenção), cujo objetivo foi estabelecer um procedimento em manutenção para melhorar a segurança de voo, aplicados no Boeing 747. A partir dos documentos MSG-1 e MSG-2, Nowlan e Heap (1978) desenvolveram estudos mais detalhados, encomendados pelo Departamento de Defesa dos Estados Unidos, para a determinação de normas e procedimentos de manutenção com base numa ampla análise estatística. Este documento, conhecido como MSG-3, tornou-se um marco para a manutenção da indústria aeronáutica, no qual os autores denominaram a metodologia de manutenção de *Reliability Centered Maintenance* (RCM). Os estudos de Nowlan e Heap (1978) consolidaram e proporcionaram a base teórica para o desenvolvimento da MCC. Desses estudos, duas conclusões se destacaram (RIGONI, 2009):

Revisões programadas baseada no tempo têm pouco efeito na confiabilidade total de um equipamento complexo, a menos que exista um modo de falha dominante;

Existem muitos equipamentos para os quais não há forma efetiva de manutenção programada.

A Manutenção Centrada em Confiabilidade (MCC) é uma concepção de manutenção que combina, basicamente, várias técnicas e ferramentas para a administração da manutenção tais como as árvores de decisão (FTA, ETA, IDEFØ) e a análise do modo de falha e efeito (FMEA/FMECA), de forma sistemática, para apoiar efetiva e eficientemente as decisões de manutenção.

O melhor desempenho dessa concepção ocorre quando é aplicada desde as primeiras etapas do projeto dos itens, ou seja, quando o atributo de confiabilidade e mantenabilidade já estão presentes no processo de projeto. No entanto, pode ser usada para avaliar programas de manutenção com a finalidade de introduzir melhoramentos. A MCC tem por princípio preservar a função, identificar os modos de falha que podem afetar a função, priorizar os requisitos da função (por meio dos modos da falha) e selecionar tarefas de manutenção que sejam efetivas. MCC pode, entre outros fatores, garantir a disponibilidade, confiabilidade e segurança do sistema definidos no projeto (FUENTES, 2006).

Em contraposição ao planejamento tradicional, o paradigma central da MCC é a "preservação da função do sistema", sendo que a análise da MCC basicamente fornece respostas às seguintes perguntas:

- Quais são as funções e os níveis normais de eficiência dos equipamentos em seu atual contexto operacional?
- Qual é o estágio da falha para haver perda da função?
- Qual é a causa de cada falha funcional?
- O que acontece quando cada falha ocorre?
- De que forma cada falha se manifesta?
- O que fazer para prevenir cada falha?
- O que fazer se uma tarefa preventiva adequada não pode ser executada?

Grande parte dos esforços na implementação da MCC está concentrada em responder a estas questões, em especial na definição das funções e de seus níveis de referência (FUENTES, 2006).

1.3.1.1 PROCEDIMENTOS PARA IMPLANTAÇÃO DA MCC

Os programas para a implantação da MCC são diversos. Autores como Fuentes (2006) e Rigoni (2009) apresentaram extensa revisão dessa sistemática. Neste livro optou-se por resumir a proposta de Rigoni (2009), que desenvolveu um conjunto de procedimentos para auxiliar a implantação da MCC. Para tanto, o autor chama atenção para a importância de ponderar as características e objetivos da empresa às necessidades do sistema ao qual a MCC será implantada e os fatores críticos para o sucesso de um programa de MCC. Ao final da análise, é possível propor ferramentas e normas de conduta que minimizem os aspectos que podem afetar negativamente o programa de MCC.

O procedimento de referência segue as etapas mostradas na Figura 1.1. Cada etapa pressupõe requisitos específicos de entrada e das saídas que serão utilizadas nas etapas seguintes ou que irão compor o manual de MCC da empresa. Além disso, cada etapa demanda determinadas tarefas, mecanismos e controles para sua execução, como indicado na Figura 1.2. O detalhamento de cada uma dessas características será explicitado no item referente aos aspectos de cada

etapa. O procedimento de referência foi desenvolvido para contemplar todas as etapas do ciclo de vida da MCC, desde a verificação de sua adequação para o sistema pretendido até a realimentação das decisões tomadas ao longo do processo de implantação, em função de critérios de desempenho do programa de MCC (RIGONI, 2009).

Cinco macro-etapas compõem o procedimento de referência proposto, as quais são: Pré-implantação; Análise; Tomada de decisão; Implementação; e Execução, como explicitado na Figura 1.1.

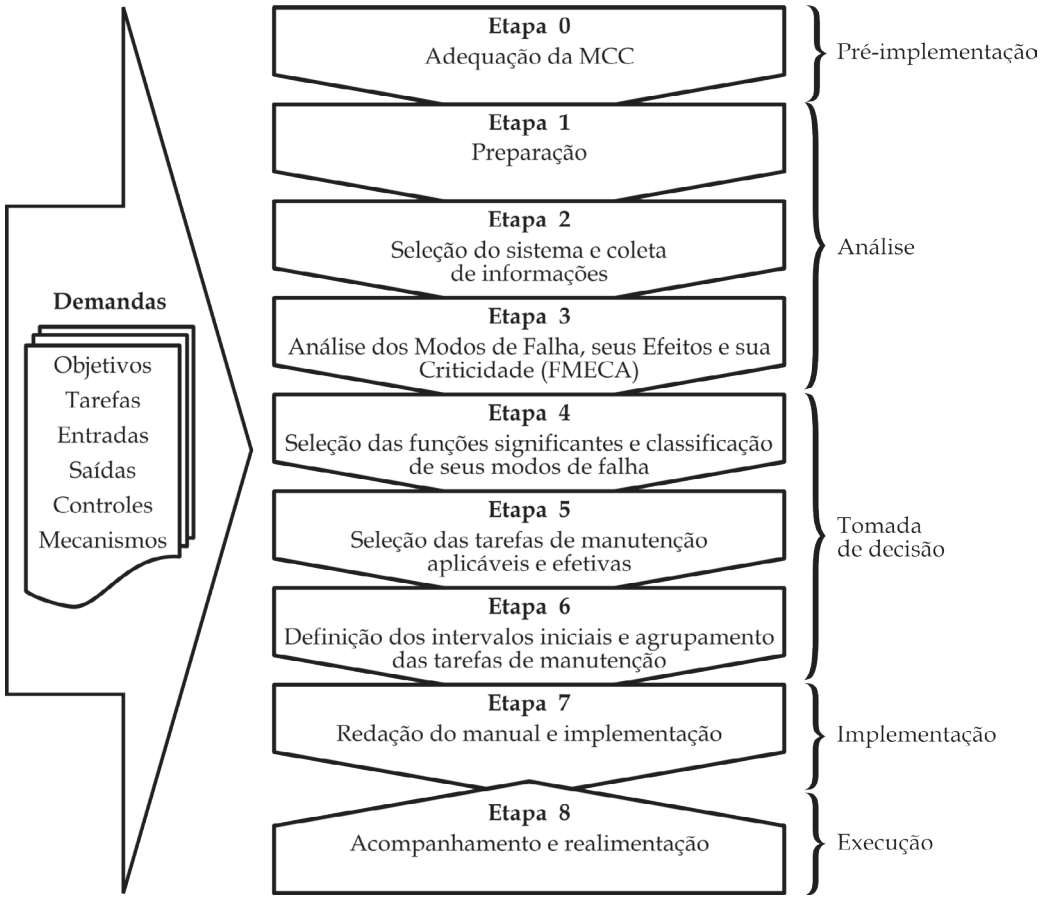


Figura 1.1 Procedimento de referência para implantação da MCC (RIGONI, 2009)

Para completar o procedimento de implantação, oito etapas devem ser desenvolvidas e, em cada uma delas, objetivos, tarefas, entradas, saídas, controles e mecanismos (Figura 1.2) devem ser planejados e implementados. A etapa de número oito, que é de acompanhamento e realimentação, e está dentro da macro-etapa de execução, tem a seta invertida para indicar que perpassa todo o processo de implantação e realimenta-o a partir das avaliações e lições apreendidas.

1.3.1.2 AÇÕES PARA IMPLEMENTAR CADA ETAPA DA MCC

A implementação da etapa, segundo Rigoni (2009), tem por referência uma abordagem adaptada da IDEFØ, como apresentado na Figura 1.2, definida em entradas, saídas, controles, mecanismos, objetivos e tarefas de cada etapa, como explicitado a seguir:

- Objetivos – São as razões de existência de cada etapa e estão relacionados com as funções que cada etapa desempenha dentro do programa de MCC, por exemplo: verificar aderência a determinado critério; definir um sistema para implementação da MCC; levantar os modos de falha seus efeitos e sua criticidade para o sistema sob análise;
- Tarefas – São atividades a serem desenvolvidas em cada etapa para atendimento de seus objetivos e das necessidades do programa de MCC, por exemplo: preencher a planilha de FMECA; conceber índices de desempenho; documentar a atividade desenvolvida na etapa;

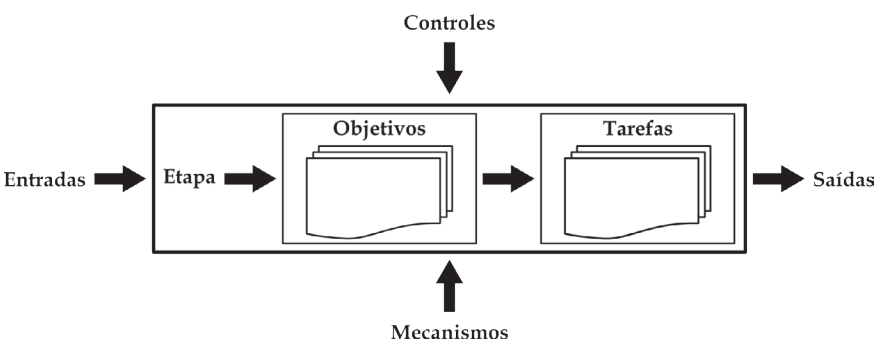


Figura 1.2 Procedimento de referência para implementar cada etapa do processo de implantação de MCC

- Entradas – São os requisitos exigidos pela etapa para obtenção das saídas, por exemplo: especialistas, documentação, dados, informações ou conhecimento sobre o sistema no qual será implantada a MCC; resultados de etapas anteriores;
- Saídas – São os resultados do processamento de cada etapa, para uma próxima etapa ou para o manual de MCC, por exemplo: decisões documentadas; planilha de FMECA preenchida; manual das ações de manutenção;
- Controles – São informações, critérios ou estratégias para monitoramento e/ou garantia da correta execução da tarefa, por exemplo: normas aplicáveis; conhecimento do especialista; necessidades da empresa; índices de desempenho;
- Mecanismos – São os recursos/ferramentas necessários ou que auxiliam a execução da etapa, por exemplo: planilha de FMECA; diagramas de decisão; equações para formulação de índices de desempenho.

Seguir as etapas recomendadas e o procedimento de referência para cada etapa vai ajudar nas atividades da equipe de manutenção durante a implantação e acompanhamento de MCC. Evidentemente, para o sucesso da implantação programas de capacitação devem ser desenvolvidos para todos que atuam no empreendimento industrial.

1.3.2 MANUTENÇÃO PRODUTIVA TOTAL

Com o final da Segunda Guerra mundial, as empresas japonesas, obrigadas pela necessidade urgente de reconstrução do país deixaram, a partir de 1950, de atuar prioritariamente com a política de manutenção corretiva de emergência para a implementação dos conceitos de manutenção preventiva baseada no tempo. Posteriormente, agregaram os conceitos de manutenção do sistema de produção, de manutenção corretiva de melhorias, de prevenção da manutenção e de manutenção produtiva (Figura 1.3) que buscasse a maximização da capacidade produtiva dos equipamentos (NAKAJIMA, 1989).

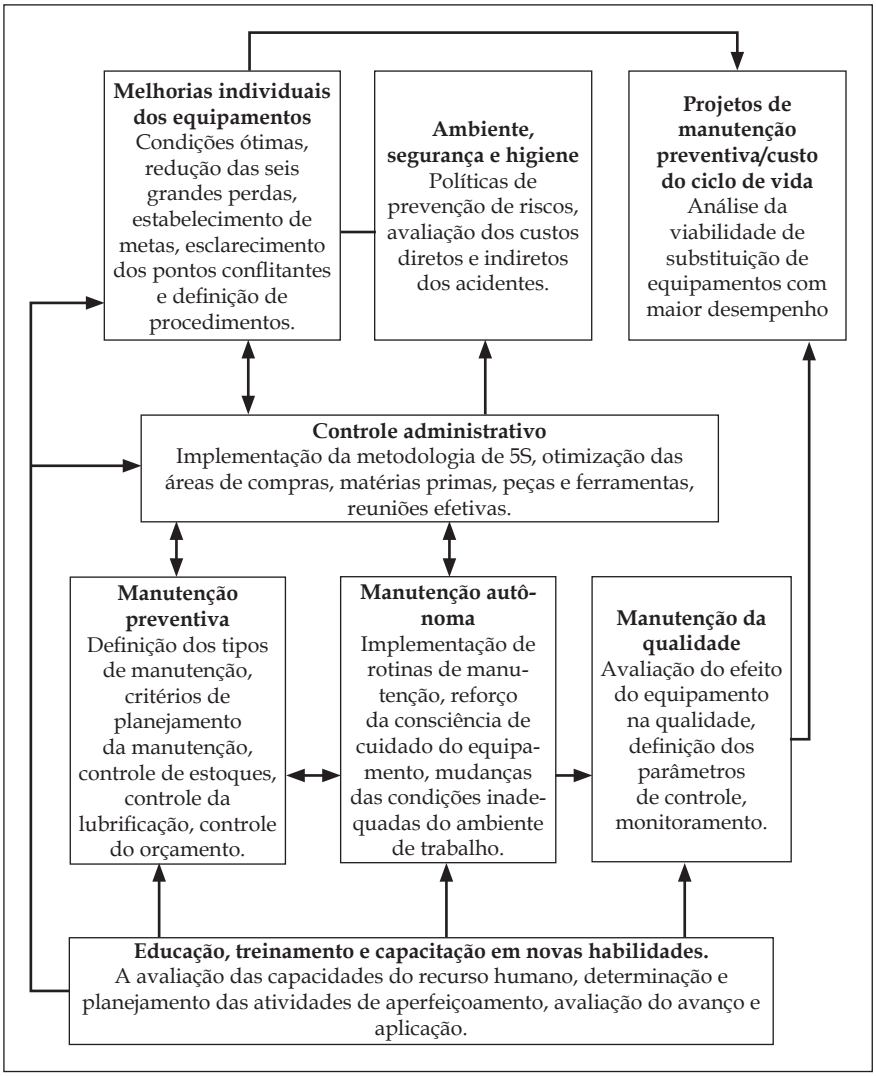


Figura 1.3 Oito pilares básicos para implementação da manutenção produtiva total – TPM (FUENTES, 2006)

Os resultados desse processo de associação de produção e manutenção chegaram ao ocidente em meados dos anos de 1980, denominada de manutenção produtiva total (TPM – *Total productive maintainance*). Essa concepção da manutenção tem como objetivo principal a realização da manutenção dos equipamentos com a participação do pessoal da produção, dentro de um processo de melhoria

contínua, na perspectiva da política de qualidade total. Considera que o operador é quem melhor conhece o funcionamento do equipamento que lhe é confiado.

Por certo, existem especificidades na implantação da TPM para cada ramo industrial e metas específicas para cada caso. Contudo, as características da gestão da TPM são, em grande parte, muito parecidas, e usualmente conhecidas como os oito pilares básicos da TPM (Figura 1.3). Os oito pilares são assim denominados: manutenção preventiva; melhorias individuais dos equipamentos; projetos de manutenção preventiva/custo do ciclo de vida; educação, capacitação e treinamento para novas habilidades; manutenção da qualidade; controle administrativo; ambiente, segurança, e higiene e finalmente manutenção autônoma.

Esses oito pilares básicos norteiam a política de TPM e definem ações concretas para alcançar a principal meta: quebra-zero. É sabido que, para perseguir essa meta, alguns objetivos específicos devem ser priorizados: eliminação das seis grandes perdas (paradas por quebra, preparação e ajustes, redução da taxa de produção, ociosidade e interrupções, defeitos e re-trabalho e perdas na partida), manutenção autônoma; manutenção planejada; educação e capacitação.

A implantação da TPM é uma tarefa organizacional. Assim, há que envolver a alta gestão da empresa, os setores de manutenção, de produção e da engenharia. Essa gestão de manutenção tem a característica de concitar todos os setores a traçarem o objetivo comum de quebra-zero. A opção por processo de educação e capacitação conduzido por meio de atividades em pequenos grupos, formados desde a alta gerência até o "chão de fábrica", é uma pré-condição para o sucesso da TPM.

Da mesma forma que para outras formas de gestão de manutenção, diversas são as técnicas e métodos utilizados para a implantação e controle de um programa de TPM na empresa. Uma das mais importantes é a Efetividade Global do Equipamento - OEE (*Overall equipment effectiveness*) - a qual é composta em três parâmetros que têm papel relevante na gestão da TPM: disponibilidade do equipamento, taxa de produção ou eficiência e a qualidade do produto. A multiplicação dos três é a OEE. Este índice ou medida mostra em quais das seis grandes perdas é necessário concentrar-se para aumentar o desempenho do sistema produtivo da empresa.

Segundo Biasotto (2006), frequentemente no ocidente a TPM é também entendida como manutenção autônoma. Mas a TPM hoje está cada vez mais integrada à infraestrutura da empresa e, por causa disso, algumas vezes é referenciada como *total productive manufacturing*, ou manufatura produtiva total ou até *total productive management* ou gestão produtiva total. Mesmo assim, em qualquer das situações, é permanente as metas a serem atingidas:

- Ter como objetivo a estruturação da organização que busque os limites do rendimento do sistema produtivo (sistema global);
- Criar um sistema fundamentado na prevenção de todos os tipos de perdas como "acidente zero" e "falha/quebra-zero", considerando-se todo o ciclo de vida do sistema produtivo;
- Envolver todos os departamentos além da produção, como desenvolvimento comercial, administrativo etc.;
- Ter a participação de todos, desde a alta direção até os funcionários da base;
- Alcançar a "perda zero", por meio das atividades de pequenos grupos sobrepostos.

1.4 CONSIDERAÇÕES FINAIS

O pensamento dos autores e de todos que participaram do projeto de pesquisa MitiSF_6 foi de socializar esse conhecimento que, em grande parte, fica restrito somente aos que têm acesso aos relatórios de pesquisa.

A ideia central foi dedicar a escritura do livro para os estudantes que atuam em sistemas técnicos em todos os níveis de formação. Posteriormente, verificou-se que o conteúdo deveria também auxiliar os cursos de formação continuada e os programas de capacitação que são desenvolvidos nas empresas. A identidade do livro está centrada na análise de risco com aplicação em disjuntores isolados a SF_6. O assunto tratado é abrangente, e por isso pode e é utilizado em várias aplicações. A análise foi feita para o setor de transmissão, mas pode ser aplicada para geração e distribuição, para análise dos itens que são portadores de risco para o homem e ambiente. Chama-se a atenção do leitor de que as abordagens feitas também podem ajudar na implementação de atributos do produto e sistemas como

os de confiabilidade, mantenabilidade e segurança, como também na implantação e acompanhamento de gestão de manutenção centrada em confiabilidade ou na manutenção produtiva total. É importante observar ainda que o livro aborda os seguintes aspectos:

1. Contextualização inicial orientado o leitor para os tópicos abordados e os aspectos principais do projeto MitiSF_6;
2. Abordagem sobre gerenciamento de risco;
3. As principais técnicas sobre gerenciamento de risco;
4. As características importantes do gás SF_6 e do disjuntor; e
5. A metodologia de análise de risco, com exemplo de aplicação.

Estas abordagens estão contextualizadas nos quatorze capítulos constituintes do livro.

Capítulo 2

FUNDAMENTOS DO PROJETO DE PESQUISA MITISF_6

O objetivo deste capítulo é apresentar as diretrizes que potencializaram o projeto de pesquisa em análise de risco para mitigar a emissão de Hexafluoreto de Enxofre (SF_6) utilizado em disjuntores, durante a operação, manutenção, transporte, recuperação e descarte.

2.1 CARACTERIZAÇÃO DO TEMA DE PESQUISA

O tema deste livro teve origem numa necessidade percebida pela Centrais Elétricas do Sul do Brasil – ELETROSUL, no contexto da transmissão de energia elétrica. A ELETROSUL é uma transmissora de energia que tem por visão "atuar no mercado de energia, contribuindo para o desenvolvimento sustentável da sociedade", cuja missão, projetada para 2020, é ser "uma empresa sustentável e competitiva, padrão de excelência em energia limpa" (ELETROSUL, 2010).

Centrada em sua visão e missão, a empresa destinou recursos a partir de projetos de pesquisa junto a ANEEL para subsidiar o planejamento de ações que propiciasse concretude ao pretendido e reforçasse a cultura que a empresa já tinha desenvolvido ao longo de sua história. Para tanto, a ELETROSUL estabeleceu parceria de trabalho de pesquisa com a Universidade Federal de Santa Catarina (USFC) por meio do Núcleo de Desenvolvimento Integrado de Produtos (NEDIP) do Departamento de Engenharia Mecânica, para "análise e desenvolvimento de procedimentos para operação e manutenção de disjuntores visando mitigar a emissão de SF_6", chamado de MitiSF_6 (ELETROSUL, 2008).

O projeto MitiSF_6 teve como objeto de estudo identificar os pontos de perda do gás SF_6, em disjuntores utilizados nas subestações de transmissão de energia elétrica e propor soluções para mitigá-lo. Como será detalhado no capítulo 12, o gás SF_6 não é tóxico, mas pode provocar a asfixia em ambientes fechados, em face de ser mais pesado

do que o ar. O gás também traz efeitos danosos para o disjuntor, na forma de substâncias corrosivas, a partir da formação de subprodutos advindos da decomposição, principalmente na presença do ar e da água. Observa-se ainda, que alguns desses subprodutos são tóxicos. Além disso, a corrosão danifica partes do disjuntor e pode provocar vazamento do gás. Com o vazamento, há diminuição da pressão interna no disjuntor, que pode provocar o desligamento do mesmo, ou até sua explosão quando operado. No entanto, a principal preocupação está relacionada com o ambiente, em face de potencializar o efeito estufa.

Há que se ter cuidados especiais na utilização do gás, dado que as falhas podem ter desdobramentos à integridade física das instalações que pode comprometer a continuidade de fornecimento de energia, para a segurança humana e para o meio ambiente. Assim, o tratamento desse problema não deve estar só relacionado com o planejamento de operação e de manutenção. Deve contemplar todos os aspectos relacionados à segurança.

Pode-se perguntar: qual o resultado esperado quando se faz uma abordagem de análise de risco? Significa que o tratamento dado para as ações resultantes da análise devem propiciar o desenvolvimento de procedimentos e legislação específica, cuja aplicação tem reflexo no conteúdo e na forma da capacitação dos operadores e dos manutentores, na catalogação do gás estocado, na codificação das garrafas, na sinalização relacionadas ao gás, nos equipamentos de manipulação, no uso de equipamentos de proteção individual, na construção de procedimentos para especificação de compra e garantias associadas, no estabelecimento de cláusulas de seguro, no tipo e na disposição de equipamentos de primeiros socorros, na simulação de acidentes, entre outros.

2.2 IMPORTÂNCIA DO GÁS SF_6 PARA O SETOR ELÉTRICO

Várias ações da atividade humana geram desequilíbrios na natureza, principalmente quando geram efluentes ou liberam produtos em quantidade e em velocidade que o meio não pode absorver ou processar. A geração, o transporte e o consumo de energia elétrica, como não poderiam deixar de ser, também produzem efluentes a partir de seus processos de trabalho. Influenciam o ambiente, podendo afetar a qualidade do ar, qualidade e disponibilidade de água, o *habitat* da fauna e flora aquática e terrestre, entre outras. Na geração,

há transformação de energia, e, dependendo da fonte primária de energia, a quantidade de rejeitos e efluentes para o meio ambiente pode ser mais ou menos significativa.

Já na transmissão e distribuição não há transformação de energia. A quantidade de efluentes para o ambiente depende dos materiais que estão presentes nos diferentes equipamentos utilizados para realizar suas funções. Muitos desses equipamentos requerem cuidados e procedimentos especiais e padronizados, em face de conterem pressão elevada e produtos que, durante o processo de trabalho, podem liberar o próprio produto ou efluentes que, por vezes, afetam o meio ambiente, seja pela toxidade, seja pela possibilidade de contribuir com o efeito estufa. Dependendo da quantidade desses produtos e do modo de falha do equipamento, maiores cuidados demandam em face da periculosidade e dos riscos para o ambiente e para as pessoas que operam ou fazem manutenção nesses itens.

Em face das características do gás SF_6, seu uso no setor elétrico tornou-se intenso e permitiu grande evolução no desenvolvimento de equipamentos. Contudo, cuidados especiais devem ser levados em consideração para os equipamentos que o utilizam. O SF_6 é utilizado em vários equipamentos do setor de transmissão como: disjuntores, secionadores, transformadores para instrumentos, barramentos, linhas de transmissão e subestações blindadas (*Gas Insulated Substation* - GIS). O SF_6 também serve para outras aplicações, por exemplo, na fabricação de semicondutores. Foi utilizado em pneumáticos, isolante térmico e de ruído. Hoje, porém, há restrições legais para essas aplicações.

O projeto MitiSF_6 focou mitigar a perda do gás nos disjuntores isolado a SF_6 em função da quantidade desse equipamento na empresa e de sua importância para a segurança de funcionamento e garantia da continuidade na transmissão de energia elétrica. Quando da realização da pesquisa constatou-se que a empresa tem um parque de mais de 450 disjuntores isolados a SF_6, acumulando aproximadamente 19.000 kg de gás. Embora estes valores sejam significantes, há empresas do setor elétrico no Brasil que tem quantidade de gás muito superior ao aqui apresentado. Em termos mundiais, a quantidade de gás é muito significativa. Por isso, é que há várias entidades estão atuando na regulação do uso, manipulação e descarte do gás, de forma concatenada em todo o mundo, com destaque para: EPA - US *Environmental Protection Agency*, CIGRÉ - *Comité International*

des Grands Réseaux Electriques, CAPIEL - *Coordinating Committee for the Associations of Manufacturers of Industrial Electrical Switchgear and Controlgear in the European Union*, IEC - *International Electrotechnical Commission* e, recentemente, também a ABNT - Associação Brasileira de Normas Técnicas que revisou a Norma NBR 11902 (Hexafluoreto de Enxofre para Equipamentos Elétricos – Especificação) que desde 1992 estava em descompasso com a normatização internacional.

Em função das características do gás, do total da produção mundial, em torno de 80% é utilizada no setor elétrico. Pode-se perguntar: por que este gás é tão utilizado no setor elétrico? É porque o mesmo oferece características funcionais excelentes, tais como: estrutura molecular extremamente estável, gás inerte, alta resistência dielétrica, habilidade extintora única, excelente estabilidade térmica e capacidade isolante (EPA, 2004; ENERVAC, 2004). Na verdade, o gás, em função das características apresentadas, proporcionou ao setor elétrico mais confiabilidade aos sistemas técnicos, especialmente aos disjuntores, tantos os presentes nas subestações abertas quanto nas blindadas. Contribuiu assim para a segurança funcional dos sistemas envolvidos e para a disponibilidade de energia elétrica para uso doméstico, público e industrial.

Em função das características adequadas para serem aplicadas no setor elétrico, seu uso está em crescimento. Contudo, suas desvantagens também são significativas. Pesquisas existem para encontrar meios adequados de gerar, transmitir e distribuir energia elétrica sem utilizar equipamentos que contenham o gás. É um esforço que ainda vai demandar tempo, dinheiro e determinação da sociedade para tal.

2.3 RESTRIÇÕES NO USO DO GÁS SF_6

Apesar da grande utilidade do gás para o setor elétrico em todo o mundo, desde meados do século XX, várias são as restrições que foram e estão sendo apresentadas para seu uso. O gás apresenta certas desvantagens que afetam a segurança humana e ambiental. Em relação aos seres vivos, no caso de vazamento em um ambiente fechado pode levar a asfixia, pois é mais pesado que o ar. Em relação ao ambiente, o SF_6 é um potente gás estufa, 23.900 vezes mais que o CO_2 (EPA, 2007), para um período de referência de 100 anos. O Quadro 2.1 apresenta uma lista de gás que contribui para o efeito

estufa, tomando por base o CO_2, com um destaque para o SF_6. O gás possui vida atmosférica elevada, aproximadamente 3.200 anos, ou seja, muito maior do que o CO_2, que leva em torno de 50 a 200 anos para se integrar a atmosfera (USA, 2004). Ainda em comparação com o CO_2, EPA (2007), ressalta que aproximadamente um quilograma de gás (duas libras de SF_6) tem um impacto no aquecimento global equivalente a 22 toneladas de CO_2. Observa-se ainda que durante a permanência na atmosfera o gás sofrerá reações químicas, produzindo subprodutos corrosivos, tóxicos etc.

Quadro 2.1 Potencial efeito estufa (GWP - Global Warming Potential) de alguns gases para 100 anos de horizonte de tempo (UNO, 2007)

Designação industrial ou nome comum	**Fórmula química**	**GWP (100 anos)**
Dióxido de carbono	**CO_2**	**1**
Metano	CH_4	21
Óxido nitroso	N_2O	310
CFC-11	$CC_{l3}F$	3.800
CFC-12	$CC_{l2}F_2$	8.100
CFC-113	$CC_{l2}FCC_1F_2$	4.800
HFC-23	CHF_3	11.700
HFC-32	CH_2F_2	650
HFC-125	CHF_2CF_3	2.800
HFC-134[a]	CH_2FCF_3	1.300
HFC-143[a]	CH_3CF_3	3.800
HFC-152[a]	CH_3CHF_2	140
HFC-227ea	CF_3CHFCF_3	2.900
HFC-236fa	$CF_3CH_2CF_3$	6.300
Hexafluoreto de enxofre	**SF_6**	**23.900**
PFC-14	CF_4	6.500
PFC-116	C_2F_6	9.200
PFC-218	C_3F_8	7.000
PFC-318	c-C_4F_8	8.700
PFC-3-1-10	C_4F_{10}	7.000
PFC-5-1-14	C_6F_{14}	7.400

Faz-se a ressalva que a contribuição para o efeito estufa proveniente da emissão do gás pelo setor elétrico é baixa, quando comparado com outros gases. Mesmo assim, estima-se que o setor elétrico participa com 11% do total da emissão de gases de alto potencial efeito-estufa (GWP – *global warming potential*) (EPA, 2004), tendo por referência o ano de 2003. Esse fato, e o grande potencial de dano no que se refere ao efeito estufa, levou sua inclusão no Protocolo de Kyoto firmado em 1997, ressaltando os cuidados que se deve ter em seu uso (EPA, 2004). O Brasil é signatário, e para ratificar tal determinação assinou o Decreto n° 5.445, em 12/05/2005, o qual estipula que o protocolo "[...] será executado e cumprido tão inteiramente como nele se contém" (BRASIL, 2005).

Destaca-se que alguns países já possuem regulamentação própria para a produção, transporte, uso e descarte de SF_6. A União Europeia, por exemplo, publicou os regulamentos (*commission regulation*) CE n° 842/2006, em 17 de maio de 2006, que regulamenta o uso de gases fluorados com efeito-estufa; e CE n° 305/2008, em 2 de abril de 2008, que estabelece, nos termos do CE n° 842/2006, "[...] os requisitos mínimos e as condições para o reconhecimento mútuo da certificação do pessoal que procede à recuperação de determinados gases fluorados com efeito estufa em comutadores de alta tensão" (UNIÃO EUROPEIA, 2008), i.e., o gás SF_6. Em alguns países, as empresas usuárias têm que declarar a quantidade de gás existente, o gás que vão adquirir e a quantidade e forma de recuperação ou de descarte que fazem. No Brasil, ainda não existe nenhuma publicação neste sentido.

Em face das especificidades em relação ao processo produtivo (como pode ser visto no capítulo 12) todo o gás SF_6 utilizado no Brasil é importado. Poucas são as empresas que detém a autorização para a importação e distribuição. A especialidade requerida para a fabricação e transporte o caracteriza como um produto que tem importante valor agregado. Além disso, a política mundial de uso e controle do gás, a partir do tratado de Kyoto, propiciou significativo aumento de preço, chegando aproximadamente a 600% em dois anos, tendo por base o ano de 2004 (ENERVAC, 2006).

Informações em catálogos de fabricantes de disjuntores indicam que a perda de gás em equipamentos novos é muito pequena e não supera a marca de 0,5% da massa de gás por ano. Tal fato não deve

afetar o desempenho do disjuntor. Contudo, como o ciclo de vida de um disjuntor é de 20 anos, pode, em alguns casos, desenvolver processos de degradação do equipamento em posições que potencializam maiores vazamentos, que leve a redução significativa da pressão mínima necessária para seu funcionamento.

Para evitar que o disjuntor fique disponível para operação com baixa pressão de SF_6, normalmente os disjuntores são fabricados com dois níveis de alarme: um de advertência e outro que abre o disjuntor em *trip*, ou seja, interrompe sua função. Por exemplo, o disjuntor trabalha com 6,0 bar de pressão nominal (na temperatura de referência de 20°C) e tem alarme de advertência com 5,2 bar e de *trip* com 5,0 bar. Nesses casos, houve um vazamento maior do que o especificado no processo de fabricação.

Além da perda de SF_6, também existe o problema da entrada de contaminantes. Ou seja, se existe saída de gás também ocorre entrada de ar e de umidade. A contaminação do SF_6 por baixos percentuais de ar não chega a afetar o desempenho do equipamento, no entanto, quando associado à umidade – mesmo em baixos percentuais –, na presença de arco voltaico, são gerados subprodutos que comprometem a capacidade dielétrica. Outra questão é a produção de ácido que ataca as vedações, o que gera um ciclo vicioso.

É interessante observar que a entrada de contaminantes pode ocorrer, também, quando o equipamento sofre manutenção, tanto pela introdução de ar e umidade durante o enchimento de SF_6 quanto pela exposição dos componentes do equipamento à atmosfera (por adsorção, por exemplo). No entanto, o SF_6 é um gás atóxico, mas, durante a operação do disjuntor, podem ser gerados subprodutos tóxicos a partir das reações químicas. No interior do disjuntor, parte dessas reações se acumula na forma de pó. Por isso, é muito importante demandar ações para reduzir a contaminação do gás, que, por sua vez, reduzirá a produção dos subprodutos e, por consequência, diminuirá a chance de dano à saúde dos colaboradores, principalmente os que vão atuar nas ações de manutenção, dado que terão de estabelecer contato direto com o equipamento. Além disso, proporcionará menor efeito sobre o ambiente.

Estudos desenvolvidos pela EPA no que se refere à manipulação do gás revelam que este é o ponto com maior potencial de redução

de perdas. O programa estadunidense de redução de perdas de SF_6, por exemplo, obteve uma redução na taxa de emissão próxima de 50% em 8 anos – vide Figura 2.1 –, majoritariamente pela redução de perdas na manipulação (EPA, 2007).

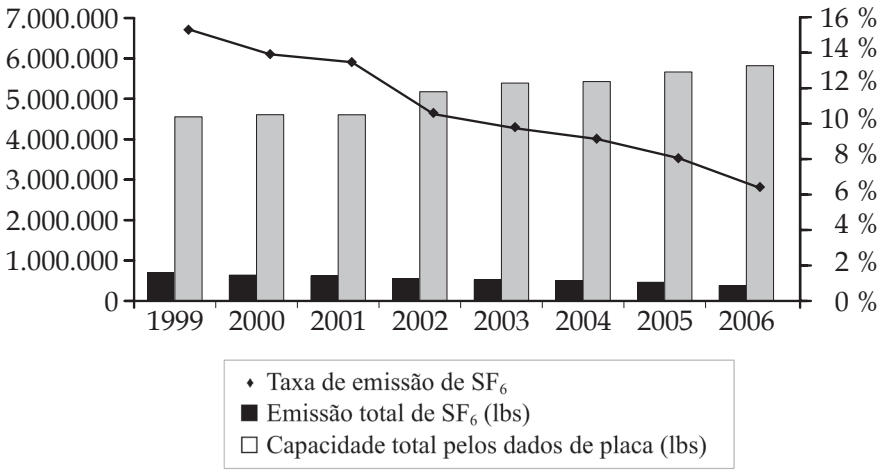


Figura 2.1 Emissão de SF_6 pelos parceiros do programa de redução de emissão de SF_6 no setor elétrico da agência de proteção ambiental estadunidense

A EPA/USA constatou, em uma pesquisa com 84% dos membros do programa de redução de emissão de SF_6, que os mesmos foram responsáveis pela emissão de 201.586 kg (444.424 libras) (1 libra = 0,45359 kg) de um total de 1.935.989 kg (4.268.148 libras) de SF_6 instalados em seus equipamentos (dados de placa) (EPA, 2004). Esse valor representa em torno de 10% do que foi pesquisado (EPA, 2004). A pesquisa foi significativa, dado que os membros do programa totalizaram aproximadamente 45% da indústria de energia elétrica no país. Comparando com outras fontes emissoras de gás causadoras do efeito estufa, este volume de SF_6 equivale a cerca de 800.000 carros em circulação durante um ano nos USA (EPA, 2007).

Não foi identificada informação em relação à emissão do gás durante os processos de manutenção corretiva, quando da falha do disjuntor, ou nas manutenções preventivas programadas. Mas há informações que merecem atenção, segundo EPA (2007):

- Ações consistentes na detecção de vazamentos poderão reduzir em até 20% do vazamento total;
- A reciclagem de equipamento poderá colaborar com 10% do total de emissão;
- O emprego da educação e capacitação dos colaboradores, com foco nas questões ambientais, poderá também contribuir com grande impacto para a redução da emissão.

2.4 METODOLOGIA PARA O DESENVOLVIMENTO DO PROJETO MITISF$_6$

O gerenciamento deste projeto, por estar inserido no programa P&D da ANEEL, seguiu as exigências da agência. Adicionalmente, fez-se o detalhamento seguindo as práticas usuais de gestão de projeto, tais como: desdobramento da estrutura de trabalho (WBS – *work breakdown structure*) detalhada com o respectivo cronograma, matriz de responsabilidade, alocação de recursos humanos, planejamento de aquisições etc.

Também foi definido um padrão de numeração dos documentos vinculados ao projeto, para facilitar a gestão. Para evidenciar os produtos das tarefas da WBS, foi associado o(s) número(s) do(s) documento(s) resultante(s) daquela ação – quando aplicável.

No intuito de avaliar o tempo que os recursos humanos foram dedicados ao projeto foi implementada uma folha de acompanhamento de homem/hora (*time sheet*). Esses dados possibilitaram um melhor controle do uso dos recursos empregados no projeto e visaram gerar estimativa de tempo para os projetos futuros. É sempre muito difícil fazer estimativas de projeto de pesquisa. Afinal, nesses, por serem de pesquisa, trabalha-se com o desconhecido. Assim, apesar do estabelecimento de cronogramas, há sempre imponderáveis que por vezes suprimem etapas, adiantando o tempo. Outras vezes depara-se com barreiras difíceis de serem ultrapassadas no tempo estimado podendo, às vezes, levar um tempo superior ao previsto para a etapa ou, para o próprio prazo do projeto.

A metodologia utilizada neste trabalho seguiu as sistemáticas adotadas no desenvolvimento de produtos (BACK et al., 2008). Para cumprir com os objetivos do projeto centrou-se no estudo do sistema

técnico a partir dos atributos de confiabilidade, mantenabilidade, segurança, risco, custo e ambiente. Em relação à análise do ciclo de vida dos equipamentos, tomou-se por referência a curva da taxa de falha (curva da banheira) para melhor caracterizar os equipamentos, em relação às fases de juventude, vida útil e de envelhecimento. Assim, dependendo da idade do equipamento, procedimentos específicos devem ser recomendados.

O planejamento do projeto é uma fase muito importante, cujo desenvolvimento já ocorreu no processo anterior à sua submissão para ANEEL/ELETROSUL. Após a aprovação, o planejamento foi retomado e utilizou-se técnicas e ferramentas específicas para a atividade. Evidentemente, ajustes foram requeridos para adequar os ritmos de trabalho e o fluxo de informações entre as equipes da UFSC e ELETROSUL. Com a reestruturação do planejamento, organizou-se um conjunto de técnicas e ferramentas para sistematizar a entrada de informações e outras para controle dos dados de saída, que formaram a base para a gestão do projeto, como exemplificado na Figura 2.2.

O processo de pesquisa foi organizado em quatro fases, como apresentado em Back, et al, (2008): fase informacional, conceitual, preliminar e detalhado. Em cada uma delas também foram utilizadas técnicas para sistematizar as informações, orientar as ações e fazer registros das decisões a serem implementadas. Algumas das técnicas utilizadas estão detalhadas na forma de capítulos ao longo do livro. Observa-se, porém, que adaptações foram feitas ao longo do processo de pesquisa, dado que Back, et al apresentam a metodologia para o processo de desenvolvimento de produtos. Aqui, o produto é uma atividade de pesquisa. Em face disso, outras técnicas foram utilizadas e algumas delas foram antecipadas ou utilizadas em mais de uma fase.

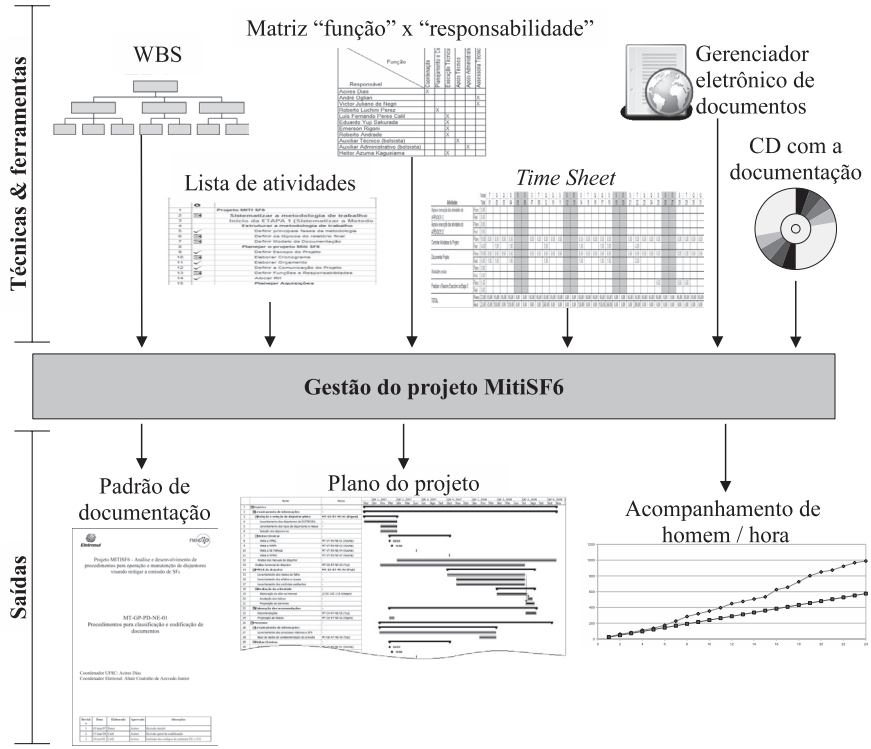


Figura 2.2 Principais técnicas de análise utilizadas na gestão do projeto MitiSF$_6$.

2.4.1 FASE INFORMACIONAL

Nesta fase foram obtidas as informações para a análise e caracterização do problema a ser estudado, a definição das necessidades e os requisitos para a fase de uso, do plano de atividades e das responsabilidades, estabelecimento apropriado das fronteiras do problema e a alocação de recursos para sua execução. Exemplos de técnicas utilizadas nesta fase são: questionário estruturado utilizado para obter informações de fabricantes de disjuntores, distribuidores de SF_6, empresas do setor de energia elétrica nacional e internacional; IDEFØ (*integrated definition for function modeling*) utilizada para organizar a análise dos processos e ajudar na comunicação entre os vários agentes desses processos. Visitou-se as bases de dados, utilizou-se de técnicas de criatividade para ajustar as informações às

necessidades do projeto, entre outras, como está mostrado na Figura 2.3. Na parte superior da Figura 2.3 explicitam-se as técnicas utilizadas para sistematizar as informações, e, na parte inferior, têm-se as saídas sistematizadas para tomada de decisão, na forma de tabela chamada de objetivos de risco e de caminhos que são apresentados na função global. Esses objetivos são os requisitos e necessidades que serão utilizados como entradas na fase conceitual. Por exemplo, Azevedo & Dias (2007) apresentaram, como saídas, 16 requisitos, baseados nas 27 necessidades da concessionária levantadas nas áreas relacionadas ao projeto de pesquisa, dentro da ELETROSUL. Com isso, foi possível direcionar as atividades das etapas seguintes, garantindo que a metodologia contemplasse os atributos desejados pelo cliente, no caso a ELETROSUL/ANEEL. Essas saídas foram utilizadas na fase conceitual do processo de pesquisa.

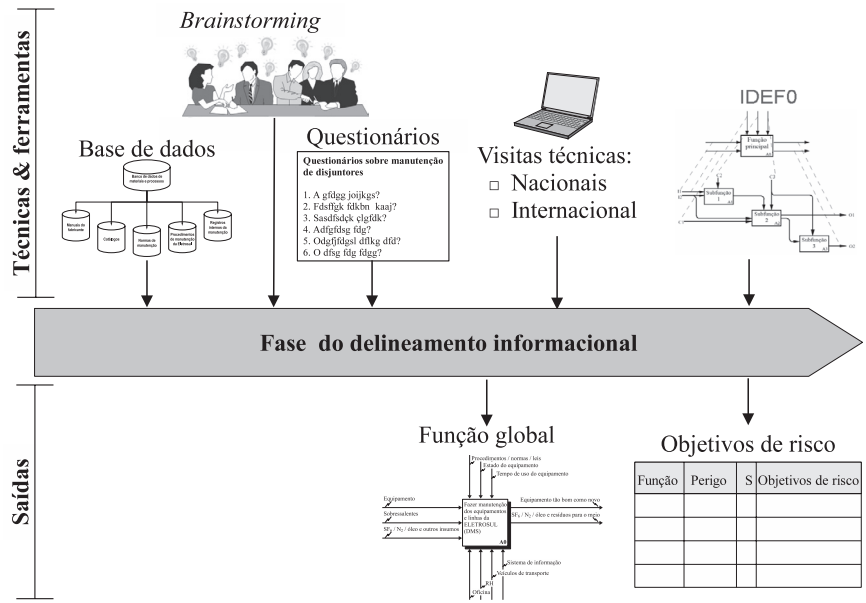


Figura 2.3 Principais técnicas de análise utilizadas na fase informacional do projeto MitiSF_6.

2.4.2 FASE CONCEITUAL

Como o sistema técnico já existe, os conceitos obtidos referem-se aos procedimentos relativos à mitigação de riscos de vazamento de gás SF_6. Uma vez estruturada as informações, aprofundou-se a

pesquisa em nível do estado da arte, para o desenvolvimento de soluções alternativas para mitigar vazamentos de gás nos disjuntores em uso, nos disjuntores que foram retirados para manutenção e nos diferentes processos de manipulação do gás. Nesta fase, é desejável ter-se como saída os conceitos para desenvolver as atividades em termos de operação e de manutenção dos disjuntores, e conceitos para melhorar a estrutura do setor de tratamento e armazenagem do gás, na perspectiva da perda-zero de SF_6 para atmosfera (Figura 2.4). Para isso, continuou-se a fazer as visitas técnicas ao setor de manutenção da empresa com o objetivo de acompanhar os procedimentos de recuperação de gás, retirada de disjuntores para manutenção e recuperação nas oficinas e a recolocação do disjuntor para operação, na condição de tão bom quanto novo. Utilizou-se o IDEFØ para o mapeamento de processo e caracterização da gestão de manutenção. Algumas das técnicas da fase anterior foram empregadas para ajustar as informações com o sentido de estruturar alguns conceitos e definir as ações para as fases seguintes. Alguns conceitos foram estruturados a partir dos seguintes referenciais: padronização de procedimentos; redução de consumo; conscientização das equipes de manutenção; tornar a ELETROSUL um *benchmarking*. (AZEVEDO & DIAS 2007). Já as ações foram definidas com o uso das seguintes técnicas: o modelo da corrente causal permitiu identificar o caminho mais provável para as falhas com maior probabilidade de ocorrer vazamentos; a técnica FMEA permitiu organizar a linguagem relacionando os itens do disjuntor com a função, e, por sua vez, com os modos de falhas potencialmente mais relacionados com o vazamento do gás; a técnica CNEA permitiu desenvolver a primeira análise do modo de falha, no sentido de relacionar do lado esquerdo as causas mais prováveis e as barreiras para inibir a atuação das causas para deflagrar o modo de falha e do lado direito, os efeitos produzidos pelo modo de falha e também as barreiras para impedir ou mitigar os efeitos do modo de falha.

Na parte inferior da fase do delineamento conceitual (Figura 2.4) tem-se as saídas na forma de conhecimento estruturado por meio das técnicas FMEA, IDEFØ, *software* e listas. Faz-se a síntese e também os registros das análises desenvolvidas. É a partir dessas saídas que se toma as decisões de implementação de atividades, experiências, testes, ensaios etc., a serem desenvolvidas na fase preliminar.

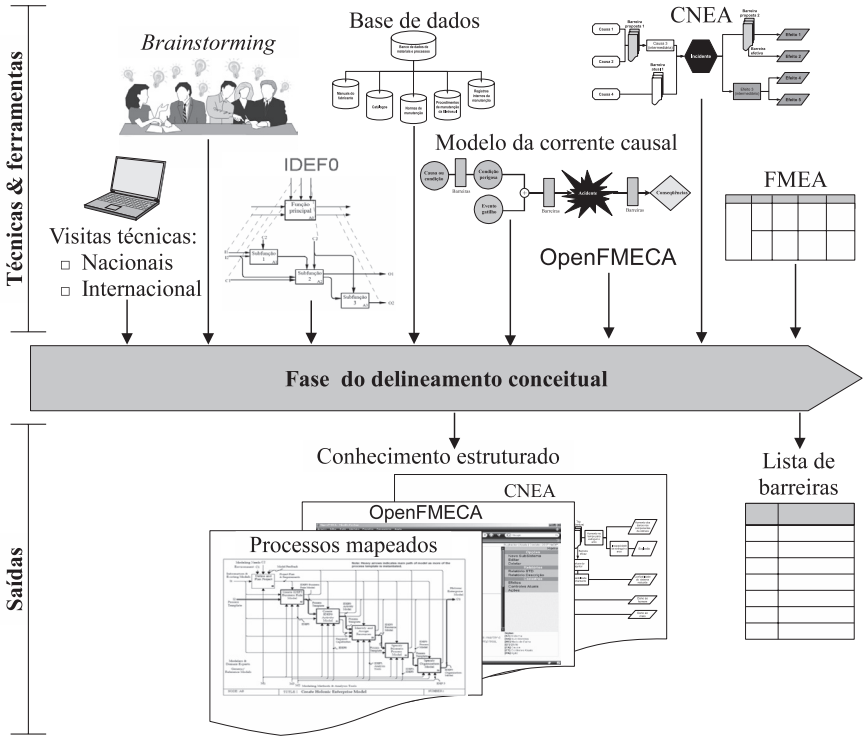


Figura 2.4 Principais técnicas de análise utilizadas na fase conceitual do projeto MitiSF_6.

Ao final da fase conceitual tem-se as informações para decidir sobre as ações que devem ser desenvolvidas para mitigar a emissão do gás SF_6 tanto do disjuntor quanto dos procedimentos de movimentação do gás dentro dos diferentes setores da empresa.

2.4.3 FASE PRELIMINAR

A fase preliminar conduziu ao desdobramento das ações no contexto da análise de risco, pelo uso de técnicas para a estruturação das decisões e planejamentos das ações a serem tomadas sobre os itens que fazem parte do cenário de trabalho em nível dos equipamentos portadores de SF_6 e das atividades relacionadas com o próprio gás, como mostra a Figura 2.5. Os atributos de confiabilidade, mantenabilidade, segurança humana e ambiental ganharam evidência. Esta é uma fase de se fazer sínteses, que, no âmbito do projeto, ocorreram

tanto sobre o disjuntor quanto sobre o processo de tratamento do SF_6. Nesta fase pode-se lançar mão de técnicas como: análise dos modos de falha e efeitos (FMEA -*failure mode and effects analysis*) descrita no capítulo 7; análise por árvore de falhas (FTA - *Fault Tree Analysis*) no capítulo 8; análise por árvore de evento (*ETA - Event Tree Analysis*) mostrada no capítulo 9; redes bayesianas no capítulo 10; e análise de eventos por rede causal (CNEA (*causal network event analysis*) no capítulo 11. Tais estudos propiciaram, a partir dos conceitos firmados na fase anterior, níveis de especificação que foram utilizados nas ações de operação e manutenção do sistema, com vistas a mitigação do gás para atmosfera. Diante disso, foi possível propor um processo para implementação das ações estudadas no âmbito do disjuntor e dos procedimentos de movimentação do gás.

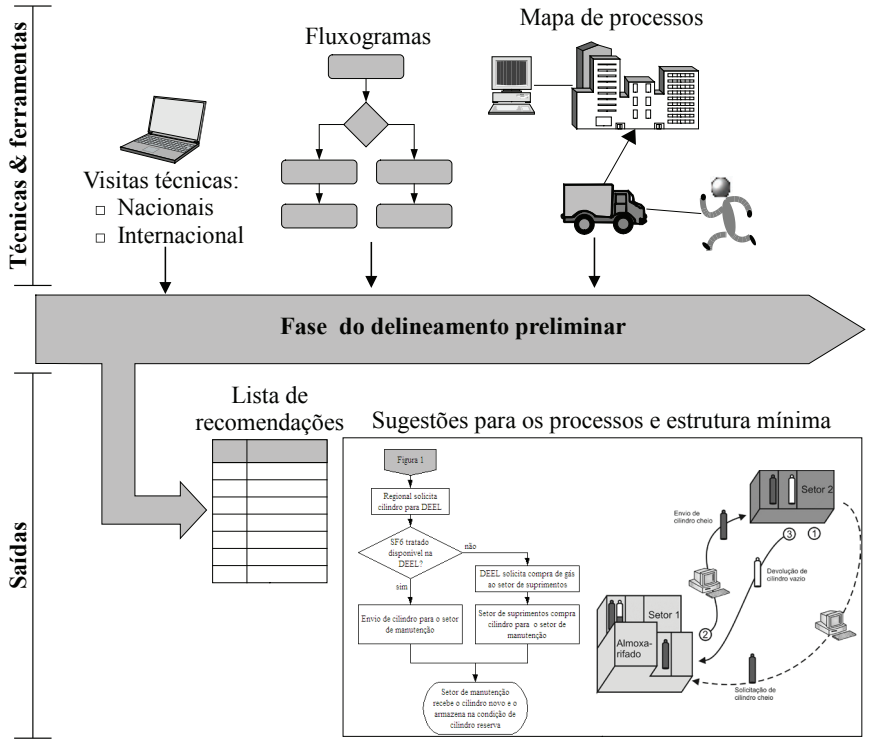


Figura 2.5 Principais técnicas de análise utilizadas na fase preliminar do projeto MitiSF_6.

2.4.4 FASE DETALHADA

A fase detalhada se configurou na apresentação do seminário de encerramento do projeto no qual foram apresentadas as recomendações, tanto para a empresa quanto para a ANEEL, segundo os seguintes aspectos: no âmbito da ELETROSUL foi recomendado efetuar redefinições em termos de política de atualização tecnológica; de política de atualização dos procedimentos e de política de capacitação. No âmbito da ANEEL recomendou-se definição de política regulatória em relação ao controle operacional de equipamentos que contenham SF_6 e controle de compra, consumo e descarte deste produto (ELETROSUL, 2008). Em face do acesso restrito aos relatórios do projeto MitiSF_6 (ELETROSUL, 2008), foi proposto estruturar, na forma de livro, as técnicas e o procedimento utilizado no projeto.

Nesta fase também aparecem técnicas que podem ser utilizadas além das que foram apresentadas nas fases anteriores. Esta é uma fase que ficou limitada, em nível de projeto de pesquisa, devido os prazos e porque as ações de detalhamento são desenvolvidas pelo corpo técnico da empresa, onde o projeto foi desenvolvido. Nesta fase, faz-se o detalhamento do sistema de manutenção e dos sistemas de suporte para cumprir as ações recomendadas, desenvolve-se os planos de capacitação, escreve-se leis, normas e regulamentos, padrões, redefine-se funções, estrutura-se sistemas para receber, organizar e analisar resultados, decide-se sobre investimentos, entre outros.

2.5 CONSIDERAÇÕES FINAIS

A compreensão das equipes que atuaram nesta pesquisa é de que o conhecimento abordado durante o projeto potencializa as ações para mitigar perdas de gás SF_6 para a atmosfera. Entende-se que o conhecimento e a conscientização de todos que operam com o gás só é possível por meio de estudo e processos intensos de capacitação. Para tanto, é necessário que se tome decisão em nível organizacional para aumentar a qualidade no trabalho, que passa necessariamente por capacitação de pessoal, estabelecimento de normas e resoluções, por procedimentos detalhados por uniformização de equipamentos para facilitar manutenção e operação, por atualização tecnológica,

e por sinergia entre as empresas que operam os sistemas de energia elétrica e a agência regulamentadora.

A percepção que se teve durante a pesquisa, no contato com profissionais das empresas do setor de energia elétrica no Brasil e no exterior, com pessoal de empresas fornecedoras de equipamentos e com pesquisadores, é de que existe um alto nível de maturidade e de comprometimento em contribuir, de forma definitiva, com as causas ambientais e de segurança. Por isso, houve sempre grande disposição em se envolver com este projeto, por todos os que foram contatados em fornecer informações ou foram submetidos a questionamentos.

Assim, detalhar o processo de projeto para socializar com todos que atuam nesse setor é, para as equipes do projeto, uma retribuição a todos que participaram na construção desse conhecimento.

Capítulo 3

GESTÃO DE RISCO: CONCEITOS E NOMENCLATURA

Neste capítulo aborda-se alguns conceitos e nomenclaturas referentes à gestão de risco aplicados para sistemas técnicos. Apresentam-se definições de termos como risco, incidente e, também, modelos para entender e classificar os riscos. Note-se que estes conceitos, juntamente com a contextualização sobre gestão de risco que se apresentará no próximo capítulo, são a base para o entendimento da metodologia para análise de riscos apresentada. Outro ponto a ser destacado é que, apesar de ter sido publicada uma norma ABNT/ISO (2000) para definição de termos utilizados na gestão de risco, ainda não existe um consenso. Assim, faz-se também uma análise da nomenclatura adotada, que facilitará o entendimento do leitor sobre o conteúdo do livro. Não existe diferença significativa quando se refere à gestão de risco ou ao gerenciamento. De certa forma as expressões estão imbricadas e refere-se no primeiro caso ao "ato de gerir" e no segundo ao "ato ou efeito de gerenciar" (FERREIRA, 1988). Assim, pode-se usar indistintamente um ou outro termo.

3.1 DEFINIÇÃO DE RISCO

Quando se discute sobre gestão de risco é necessário, primeiramente, entender o que é risco.

Em seu dicionário etimológico, Francisco Bueno (BUENO, 1988) esclarece que o termo risco origina-se da navegação, e seu primeiro significado é o de borda, orla, fio de rochedo, recife e, portanto, indica uma situação de eminência de dano às embarcações. Somente mais tarde é que o termo risco passou a significar – também – traço, linha.

Note-se que a dificuldade dos navegantes estava em identificar a posição exata desta linha de rochedos e a condição ambiental para que se evitasse uma colisão e, eventualmente, um naufrágio. Assim, o conceito de risco sempre esteve associado à incerteza dos resultados.

Com o tempo, o termo risco passou a ser utilizado para todo tipo de situação que apresenta incerteza de resultado, tanto positivo quanto negativo. Pode-se, por exemplo, avaliar o risco de ser contemplado com o prêmio de uma loteria.

É exatamente essa incerteza que motiva as ações das pessoas, o que faz do risco – de certa forma – desejável, além de inevitável. O gerenciamento de risco, então, objetiva maximizar resultados positivos e minimizar negativos.

No caso da embarcação, para entender o risco da mesma colidir com a linha de rochedo, por exemplo, é necessário caracterizar a posição da embarcação, sua velocidade e trajetória, a condição do mar e do vento, a estimativa da posição da linha de rochedo, qual seja, fazer o delineamento do estado inicial. Também é necessário levantar os possíveis estados futuros, que, nesse caso, poderiam compor resultados como não colidir com a linha de rochedo, evitar a colisão com danos menores a embarcação e a colisão com naufrágio e perda de tripulantes. Por fim, deve-se avaliar como cada estado futuro poderia ser alcançado a partir do estado inicial, que são os cenários. Todas estas informações compõem o perfil do risco.

Nesse contexto, pode-se definir risco como a chance de ocorrer um estado futuro "x", dada a ocorrência de um estado inicial – que pode ser expressa pela probabilidade condicional *P* (*Estado futuro "x"* | *Estado inicial*) –, sendo necessário, para sua completa caracterização, o delineamento dos dois estados, além dos cenários que possibilitem as transições.

Destaca-se, ainda, que para caracterizar os estados futuros é importante que se avalie quais as partes afetadas (*stakeholder*), além da relevância dos estados futuros, também chamada de significância, para cada uma delas.

Para entender o conceito de significância, suponha que você pretende caminhar sobre um cabo de aço esticado em um vão de dois metros de comprimento, entre dois pilares. Analise, então, duas situações: na primeira, o cabo de aço está a cinquenta centímetros de altura, e, na segunda, está a cinquenta metros. Considere que não existem outras variações entre os dois casos, como velocidade do vento, por exemplo. A probabilidade de êxito na travessia é a mesma, independentemente da altura em que o cabo está fixado. No entanto, os resultados decorrentes de uma queda são significativamente diferentes.

Outra questão, neste exemplo, é o motivo pelo qual se deseja fazer a travessia. Eventualmente, um prêmio de dez reais pode ser suficiente para motivar uma pessoa a enfrentar o desafio a 50 centímetros de altura, mas dificilmente fará a travessia a 50 metros do chão por este valor. No entanto, se o prêmio fosse aumentado para dez milhões de reais, o desafiante certamente ficaria tentado.

Note-se que estas condições definem os possíveis resultados da análise, por exemplo:

- atravessar com êxito o vão a cinquenta centímetros e ter um prêmio de dez reais;
- não conseguir atravessar e ter um entorse no pé pela queda de cinquenta centímetros; ou
- ter uma fatalidade em decorrência da queda de cinquenta metros.

Assim, o modelo utilizado para representar este risco deve possibilitar a caracterização dos estados inicial e futuros, bem como os cenários que possibilitam esta transição, para que o analista tenha condições de avaliar quais riscos podem ser considerados aceitáveis e quais não.

3.2 MODELOS PARA REPRESENTAÇÃO DO RISCO

Existem diversos modelos que foram desenvolvidos para aplicações específicas e que, posteriormente, ganharam generalidade que auxiliam o entendimento de riscos de forma global. No contexto deste livro, o interesse é modelar o risco de um perigo (estado inicial) evoluir para um determinado incidente e produzir consequências (estados futuros) não desejáveis para a função do sistema técnico, para o homem ou ambiente.

Pode-se definir incidente como todo evento que tem consequências negativas – o que inclui dano à saúde de pessoas, à propriedade ou ao ambiente; interrupção da função de um sistema ou do negócio de uma organização[1]e prejuízo financeiro. Na Literatura técnica, o

[1] No livro, será utilizado o termo "organizações" para designar companhias, firmas, instituições, órgãos de governo, fundações e outras entidades – independentes da natureza do empreendimento (com ou sem fins lucrativos).

uso do termo "acidente", por vezes, se refere aos eventos que resultam em dano ao homem ou ao ambiente. Note-se que a definição de incidente engloba o conceito de acidente[2], que é restrito a eventos que acarretem dano, como está destacado na Figura 3.1. Os autores entendem que incidente é qualquer manifestação técnica ou humana indesejável para o desempenho de uma função, ou que venha potencializar um perigo ou um risco. Já acidente é um subconjunto de incidente, que leva a um comprometimento da segurança.

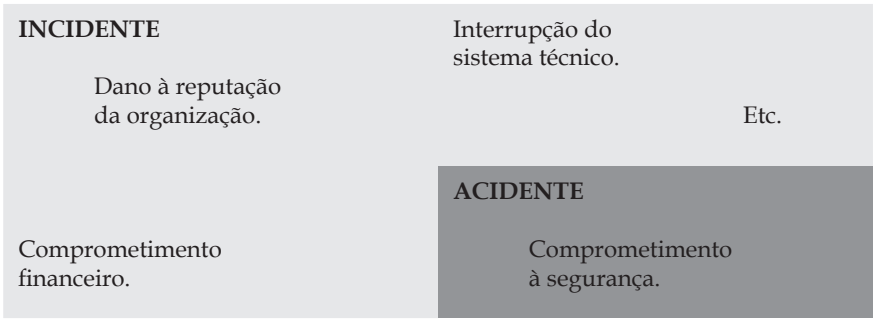


Figura 3.1 Relação entre incidente/acidente no contexto da teoria multicausal (CALIL, 2009)

Perigo, por sua vez, pode ser definido como qualquer ato (omissão ou ação), condição ou estado do sistema – ou uma combinação desses – com o potencial de resultar em um acidente, ou, de maneira mais abrangente, em um incidente (MOSLEH; DIAS, 2003). É sábio admitir que todo sistema técnico é portador de perigo.

Nesse contexto, se fosse possível elaborar relações determinísticas de quando a situação perigosa (estado inicial) se tornaria um incidente (estado futuro), não existiria o risco – pois se assim for feito, elimina-se a incerteza da mudança de estado. Em outras palavras, elimina-se a causa que leva a alteração de estado.

Pierre Simon Laplace (LAPLACE, 1995) ilustra essa situação incitando o leitor a imaginar uma inteligência capaz de computar, em uma única fórmula, o movimento de todos os elementos do universo – desde maiores objetos até as menores partículas. Assim "Para esta inteligência nada seria incerto, e o futuro, assim como o

[2] Note-se que – diferentemente do adotado no livro – alguns autores definem incidente como sendo um quase-acidente.

passado, estaria presente diante dos seus olhos". Essa inteligência foi posteriormente denominada de "Demônio de Laplace", já que Laplace postulava que ela jamais seria alcançada: "Todos os esforços na busca pela verdade tendem a levar a mente humana cada vez mais próxima da inteligência que acabamos de mencionar, entretanto sempre restará uma distância infinita dela". Assim, na perspectiva do Demônio de Laplace, não existiria risco, pois o futuro não seria incerto.

Na vida real, no entanto, muitas são as limitações de se controlar as variáveis do ambiente, homem e sistema técnico. Assim, diante da incapacidade de retratar fielmente a realidade, o homem faz uso de modelos para representá-la da melhor maneira possível.

É importante destacar que, por melhor que seja o modelo, o analista é obrigado a conviver com um certo nível de imprecisão (chamada de incerteza epistemológica ou de meta-incerteza). Devido a isso, existem inúmeros modelos que procuram representar a ocorrência de um incidente. Fundamentalmente, o que se deseja entender é: Por que ocorrem os incidentes? Como eles ocorrem? e Quais suas consequências?

3.2.1 POR QUE OCORREM OS INCIDENTES?

A visão de que todo incidente tem um culpado ainda é bastante comum, possivelmente por influência do sistema legal, no qual o acusador procura punir o suposto culpado. No entanto, quando se trata de uma organização, a adoção desta visão possivelmente irá resultar na punição de alguém que estava trabalhando diretamente no local ou mesmo de um colaborador com falta de sorte – sem se preocupar com fatores organizacionais ou pela interação entre as pessoas, por exemplo. Essa abordagem, a qual procura explicar a ocorrência de um incidente por uma única causa, é chamada de teoria monocausal no âmbito da segurança no trabalho. Salienta-se que as teorias monocausais se tornaram insuficientes para construir um modelo que explique o incidente no contexto atual. Em contrapartida, as teorias que consideram mais de uma causa (tais como: erro na operação, no projeto ou na manufatura; problemas de comunicação; falta de clareza na definição de responsabilidades; entre outros) são denominadas multicausais.

Assim, se o objetivo do sistema de gerenciamento de risco é identificar ações para evitar ou reduzir a chance de um incidente

ocorrer novamente – ou, ainda, mitigar suas consequências –, as teorias multicausais devem ser utilizadas.

Observe-se que a base de dados MARS (Major Accident Reporting System database), em maio de 1998, indicou que 64% dos incidentes de grande proporção – ocorridos na União Europeia – aconteceram por falha humana, sendo 53% por disfunção organizacional e 11% por erro do operador (LÉRGER et al., 2006). É importante destacar que os erros dos operadores podem, ainda, ter como causa raiz[3] um problema organizacional, por exemplo, no caso dele não ter sido adequadamente capacitado.

As causas para a ocorrência do incidente podem ser sistematizadas em fatores relativos ao homem, ao ambiente e à máquina (ou ao sistema técnico, em uma visão mais abrangente) – além da interação entre esses fatores, conforme ilustrado na Figura 3.2, na qual o sistema técnico pode ser entendido como um conjunto de equipamentos e instalações que tem uma (ou mais) função para ser desempenhada.

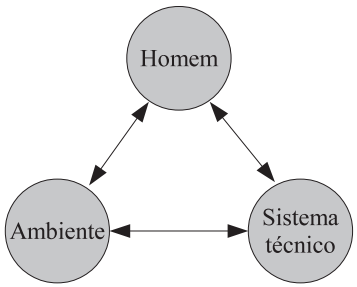


Figura 3.2 Relação entre os envolvidos no sistema da teoria multicausal da ocorrência de incidentes (Adaptada de Alonço (2004))

A Figura 3.2 é uma síntese de um problema bem mais amplo. Como é sabido, todo sistema técnico é desenvolvido a partir de uma ideação humana, motivado por uma necessidade previamente justificada. Uma vez que a idéia foi transformada em produto, seja uma usina nuclear ou um secador de cabelos, criou-se também o inter-relacionamento do sistema técnico (qualquer produto) com o homem e o ambiente, por sua vez, um risco proporcional a dimensão do produto. Um incidente numa usina nuclear pode comprometer o

[3] No capítulo que trata de FTA, aborda-se com mais detalhe o conceito de "causa raiz".

ambiente por muitos anos e a saúde de várias gerações, como ocorreu na usina de Chernobil. Já o secador, no caso de uma fuga de corrente, por exemplo, pode produzir um incidente para uma ou mais pessoas que estiverem em contato com o mesmo. É claro que, quando do descarte, o ambiente também será afetado, na proporção de cada um dos produtos. Para abordar cada um dos casos, na perspectiva da Figura 3.2, existem ferramentas de análise específicas, algumas das quais serão apresentadas ao longo do livro.

É interessante observar que a expressão sistemas técnicos também consideram *software*, além de itens físicos, que na literatura inglesa são chamados de *hardware*. Assim, a segurança nesses itens está intimamente ligada ao estudo de falhas de *software*, de componentes físicos, do homem e das perturbações do ambiente.

3.2.2 COMO OS INCIDENTES OCORREM?

Como já comentado, há uma série de modelos que procuram representar a ocorrência de um incidente. O que melhor se adere à metodologia apresentada no livro é o de Mosleh & Dias (2003) e Mosleh et al. (2004), representado na Figura 3.3, no qual o incidente é resultado de uma condição perigosa aliada a um evento deflagrador (ou evento gatilho), atravessando as barreiras. Este modelo é normalmente chamado de corrente causal.

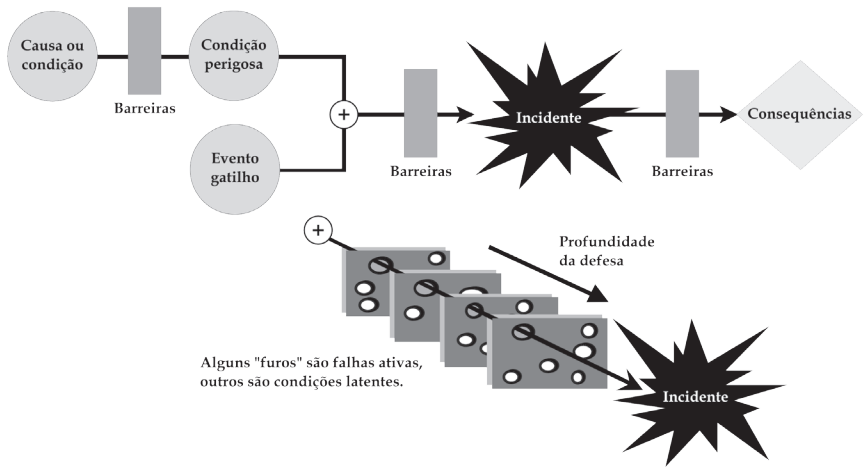


Figura 3.3 Desencadeamento de um incidente e sua trajetória através de barreiras (Adaptada de Mosleh & Dias (2003); Mosleh et al. (2004) e Reason (1997)).

A fim de diminuir a probabilidade de ocorrência do incidente ou, ainda, mitigar suas consequências, implementa-se barreiras ao longo da corrente causal. As barreiras podem ser físicas, de procedimentos, manuais, educação, capacitação, motivação ou qualquer medida que vise atuar na corrente causal evitando o incidente ou minimizando suas consequências.

Um procedimento de manutenção pode atuar para que um sistema não se degrade, ou não evolua para uma condição perigosa. Uma parede corta-fogo é, por exemplo, uma barreira para mitigar o incidente, e não permite que o incêndio se propague, o que minimiza as consequências desse incidente.

No entanto, as barreiras não são perfeitas, e seus "furos" – quer seja por uma falha ativa, quer por uma condição latente – podem permitir que o incidente ocorra, como está representado na parte inferior da Figura 3.3. A fim de reduzir o risco de ocorrer o incidente ou mitigar suas consequências, pode-se adotar mais de uma barreira, o que é denominado "defesa em profundidade". Este modelo é essencialmente importante para orientar a análise de risco. Serve para levantar e orientar a pesquisa sobre metodologias, técnicas de análise, exemplos já aplicados, lições apreendidas. Resumindo a leitura sobre a Figura 3.3, apresenta-se a causa ou condição da Figura 3.3 que orienta para o levantamento de todos os perigos do sistema técnico em análise. Admite-se que todo sistema técnico é portador de perigo. A barreira que se situa após a causa ou condição é para não deixar o perigo transformar-se na condição perigosa. Nem toda condição perigosa transforma-se em incidente. Contudo, a condição perigosa quando combinada com o evento gatilho pode gerar um risco e proporcionar um incidente se não houver barreiras para impedir ou mitigar o risco que se evidenciou, devido a combinação da condição perigosa mais evento gatilho. O evento gatilho é o que deflagra, ou pode deflagrar, a condição perigosa potencializando-a para o risco do incidente. Eventos gatilhos são, por exemplo, de natureza atmosférica, falta de capacitação, falta de procedimento, falta de qualidade em operação e manutenção, disjunção organizacional, entre outros.

3.2.3 QUAIS AS CONSEQUÊNCIAS DE UM INCIDENTE?

Outro ponto a se destacar é o tipo de consequência que o incidente provoca (que é a terceira questão levantada). Propõe-se que um incidente seja classificado como evidentes A, B, C e ocultos D/A, D/B ou D/C (Figura 3.4). Diz-se que são evidentes, porque estão diretamente relacionados com as funções principais do sistema e podem ser identificados durante os processos de análise, enquanto que os ocultos normalmente estão relacionados com funções redundantes ou que atuam eventualmente, ou surgem da combinação de diferentes probabilidades de ocorrência, difíceis de serem identificados durante um processo de análise. Para orientar o estudo de identificação das consequências em relação às categorias de incidente, um conjunto de outras perguntas deve ser formulado durante o processo de análise de um sistema técnico. A Figura 3.4, orienta o estudo de classificação da probabilidade da ocorrência do incidente, e a seguir destaca-se o significado de cada incidente:

- **A** incidente com comprometimento à segurança;
- **B** incidente com comprometimento à continuidade;
- **C** incidente com comprometimento à situação econômica e financeira;
- **D/A** incidente desconhecido oculto com comprometimento à segurança;
- **D/B** incidente oculto com comprometimento à continuidade;
- **D/C** incidente oculto com comprometimento à situação econômica e financeira.

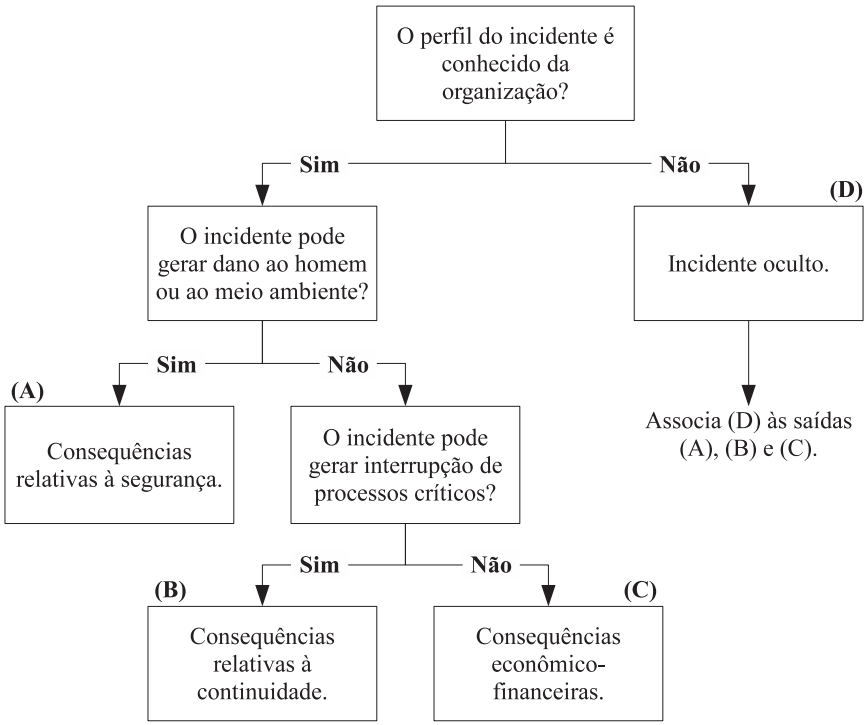


Figura 3.4 Classificação de incidentes em uma unidade organizacional (CALIL, 2009)

Observe-se que as classificações (A), (B) e (C) não são excludentes. Um incidente pode ter comprometimento à segurança, à continuidade e à situação econômica e financeira da organização. Os incidentes classificados somente como (C) devem ser gerenciados pelos processos cotidianos da organização, enquanto os (A) e (B) devem ser tratados e, quando aceitos, gerenciados de acordo com os respectivos planos de gerenciamento de incidente.

Quanto aos incidentes ocultos (D) e, portanto, involuntariamente retidos, recomenda-se que sejam gerenciados de acordo com o plano de gerenciamento de crises[4]. É importante destacar que uma apólice de seguro pode abranger também os riscos retidos. Assim, deve-se levar em consideração, no gerenciamento de risco, a contratação de seguro.

[4] O plano de gerenciamento de crises faz parte do planejamento de continuidade do negócio, sendo desenvolvido no âmbito da organização – conforme descrito, brevemente, no final da Seção 3.3.

Note-se que esta classificação não contempla os incidentes com comprometimento à imagem da empresa, pois a imagem pode estar associada a qualquer uma destas classificações, além de depender também de outros fatores, como, por exemplo, a forma que se gerencia o incidente.

3.3 CONSIDERAÇÕES SOBRE SEGURANÇA, CONFIABILIDADE E CONTINUIDADE

Os conceitos de segurança e confiabilidade foram apresentados no capítulo 1. Contudo, é interessante distinguir o conceito de segurança relativa a danos (que em inglês é definido por *safety*) do conceito de segurança relativa a patrimônio e privacidade (em inglês, definido por *security*). Normalmente, as ações para análise de risco, segundo cada conceito, são tratadas separadamente. Por exemplo, a segurança de patrimônio foca principalmente em ações maliciosas – tais como: invasões, atentados, sabotagem, vírus de computador. Este tema foge do escopo do trabalho. Assim, no livro, o termo segurança será utilizado para se referir à segurança relativa a danos, enquanto a segurança relativa a patrimônio e privacidade será abordada pela continuidade do negócio.

Assume-se que "segurança" é a capacidade (ou habilidade) de não ocorrer dano ao homem ou ao ambiente – o que pode ser expresso como a chance de ocorrer um estado futuro, caracterizado por não existir danos relevantes (que é um resultado positivo), dada a ocorrência do estado presente.

O conceito de confiabilidade, como foi visto, se estrutura em quatro pontos fundamentais: (1) probabilidade; (2) comportamento adequado; (3) período de uso (ou de vida); e (4) condições de uso. Assim, confiabilidade é a probabilidade de um sistema técnico cumprir a função até um determinado estado futuro (ou do sistema técnico operar de maneira adequada num determinado período de uso), dado a ocorrência de um estado inicial. A Figura 3.5 apresenta os possíveis cenários para que o estado inicial resulte em um dos "n" estados futuros. Note-se que, no contexto da confiabilidade, os estados futuros podem estar associados ao cumprimento da função ou, eventualmente, à falha do sistema técnico.

De forma análoga, se expressa "continuidade" como a chance de ocorrer um estado futuro caracterizado por não existir interrupção dos processos críticos da organização, acima do considerado suportável no estado presente.

Dessa forma, a segurança, a continuidade e a confiabilidade podem ser entendidas como atributos estruturantes do gerenciamento de risco.

Em muitos casos, uma ação pode afetar mais de um atributo. O Departamento de Defesa Civil, por exemplo, indica que a análise de segurança tem por finalidade aumentar a confiabilidade e o nível de segurança de um sistema (BRASIL, 1998).

De fato, os estudos de falha estão presentes tanto no gerenciamento de segurança quanto no de confiabilidade. Entretanto, esta relação nem sempre tem uma interação positiva. Por exemplo, a confiabilidade do sistema de refrigeração de uma usina nuclear é determinante para a segurança. Por outro lado, quando um relé térmico desliga um motor por uma questão de segurança, para a função e vai ao sentido contrário da confiabilidade, que é garantir a função do equipamento.

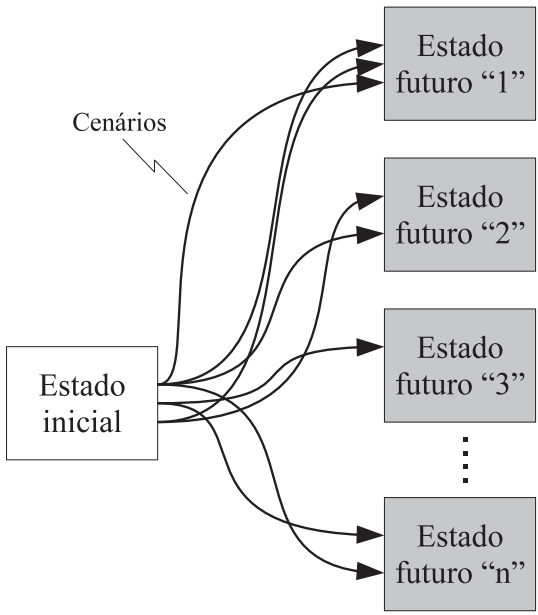


Figura 3.5 Representação da alteração do estado inicial para "n" estados futuros (CALIL, 2009)

Assim, independente da relação entre confiabilidade e segurança, um sistema de gerenciamento de segurança deve abordar as falhas resultantes da tríade homem, ambiente e sistema técnico (componentes físicos e *software*), a fim de evitar a ocorrência de danos materiais ao ambiente e/ou ao homem, ou que ocorram em menores proporções, dentro do que se considera aceitável. Nesses casos, a segurança é sempre prioritária.

Quanto à gestão da continuidade, esta objetiva manter os processos críticos ativos. Entende-se por processos críticos aqueles que são fundamentais – e mínimos – para garantir que o negócio permaneça ativo. Note-se que, no contexto da continuidade, o termo "negócio" é utilizado para designar a atividade fim da organização. Por exemplo, na área de energia, geração, transmissão e distribuição, a análise deve ser feita sempre levando em conta a continuidade desse sistema em face da dependência que a sociedade moderna tem dessas *commodities*.

O gerenciamento da continuidade do negócio é um conceito ampliado do planejamento para recuperação de desastres, que ainda é bastante utilizado por órgãos administrativos de governos, a fim de se preparar para determinadas catástrofes.

O termo "continuidade" passou a ser adotado no contexto de negócios, pois, na abordagem de "recuperação", admite-se que houve uma interrupção dos processos, enquanto a continuidade trabalha para não permitir que haja interrupções e, caso ocorram, garanta que as mesmas não atinjam um nível que se considera inaceitável.

Deve-se considerar, para efeito da continuidade do negócio, além dos possíveis incidentes que resultem em dano aos recursos críticos, os incidentes que possam causar a interrupção do negócio, tais como, invasão das instalações por grupos de interesse, greve, terrorismo, sabotagem e problemas com fornecedores. Nesse sentido, má gestão da cadeia de suprimentos, falta de política ambiental, não clareza em planos de salários e gratificações ou incentivos podem aumentar o risco de interrupção.

Destaca-se que a segurança deve ser levada em consideração no gerenciamento de continuidade e não deve ser gerenciada sem considerar a disponibilidade do sistema técnico.

A Figura 3.6 ilustra a relação entre continuidade, segurança e disponibilidade nos respectivos níveis da organização:

1. Nível da organização (empresa) onde se estabelece a missão e a visão que vai orientar o gerenciamento para a segurança e continuidade do negócio;
2. Nível das unidades organizacionais (por exemplo, a U.O.4 poderia ser o departamento de manutenção do sistema) cujos princípios organizacionais definem a política de gerenciamento da segurança e continuidade operacional dentro da unidade da organização; e
3. Nível dos sistemas técnicos, cujo gerenciamento tem foco na segurança e na confiabilidade, para garantir a disponibilidade dos sistemas, como por exemplo, disjuntores (S.T.1).

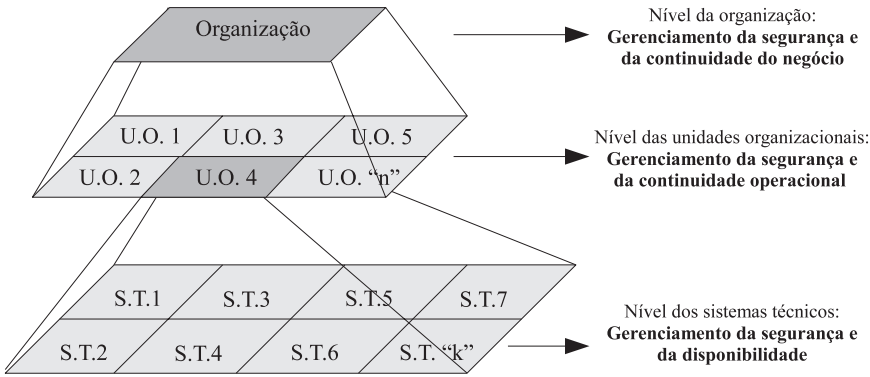


Figura 3.6 Níveis para o gerenciamento de risco em uma organização (CALIL, 2009)

Note-se que, no patamar do sistema técnico, o gerenciamento de risco visa manter a disponibilidade com níveis aceitáveis de segurança. A disponibilidade, por sua vez, depende da confiabilidade e da mantenabilidade do sistema técnico.

Lembre-se que a segurança nem sempre tem uma interação positiva com a confiabilidade. Assim, o gestor de risco, muitas vezes, terá que partir para uma solução de compromisso e favorecer uma em detrimento da outra.

É importante salientar que a disponibilidade dos sistemas técnicos não garante a continuidade da unidade organizacional. Por exemplo, em uma situação de greve ou na falta de fornecimento de matéria-prima, os sistemas técnicos podem estar disponíveis, mas a unidade organizacional pode não ter condição de operar.

De forma análoga, a continuidade das unidades organizacionais não garante que a continuidade do negócio da organização seja alcançada. A continuidade do negócio, por sua vez, contribui para a organização alcançar sua missão, mas ainda assim, depende de outros fatores, como política econômica, tendências de mercado, boatos etc. Assim, a continuidade é mais ampla e tem relação com o negócio envolvendo sistemas técnicos (mais próximo da disponibilidade), sistemas humanos (internos e externos a organização) e ambientais (em nível da organização e dos eventos diversos da natureza), ou das próprias consequências das tecnologias envolvidas.

Destaca-se que a segurança permeia os níveis de gerenciamento de risco e, portanto, deve ser considerada nos três patamares da Figura 3.6.

3.3.1 PROCESSOS RELACIONADOS À GESTÃO DE RISCO

Independentemente do atributo que se está focando, o gerenciamento de risco engloba a análise/avaliação[5], o tratamento, a aceitação e a comunicação de riscos – sendo que esta última é a troca ou compartilhamento das informações sobre o risco com as partes envolvidas.

A análise envolve a identificação dos riscos a que se está exposto e a avaliação dos mesmos, baseada em critérios pré-definidos. Dessa forma, podem-se assumir, para cada risco, três estratégias de tratamento – não excludentes:

- evitar o risco;
- transferir o risco; e
- reduzir o risco.

A ideia de se evitar o risco, apesar de bastante atraente, implica eliminar o perigo, pois somente assim não se correria risco – uma vez que não é possível eliminar totalmente a incerteza do perigo

[5] A norma NBR/ISO/IEC Guia 73 utiliza como a tradução do termo do inglês de risk assessment, que engloba a "análise" (risk analysis) e a "avaliação" dos riscos (risk evaluation). No entanto, neste livro, será adotada "análise de risco" em substituição à "análise/avaliação" (ABNT, 2005).

tornar-se um incidente. Ademais, todo sistema técnico é portador de perigo, o que implica que a organização, de alguma forma, está sujeita a algum nível de risco.

A transferência do risco está associada à contratação de seguro ou à "terceirização" do sistema técnico que está exposto ao risco, ou seja, transferir para outros a responsabilidade pelo incidente – o que, por si só, não exclui o risco do ciclo de vida do sistema técnico.

A opção de reduzir o risco, por sua vez, propõe que ele seja trabalhado a fim de diminuir a probabilidade de ocorrência do incidente e/ou seus efeitos. Pode-se reduzir a probabilidade do risco até um patamar que se considere insignificante, aceitando conviver com este nível de risco.

Aceitar um risco, mesmo quando está acima dos limites estabelecidos – chamados de riscos retidos ou relutantemente aceitos –, pode não parecer prudente, mas, em alguns casos, pode ser a melhor opção. A decisão passa, então, por uma avaliação de custo-risco-benefício. É interessante salientar que o processo de retenção do risco também inclui os riscos ocultos, que a organização não sabe que existem – chamados de involuntariamente retidos.

Dessa forma, a escolha não está entre "risco" e "ausência de risco", mas entre "risco aceitável" e "risco inaceitável" – o que dependerá da disposição do analista de ousar, já que o futuro é incerto.

3.3.2 PLANEJAMENTO PARA A OCORRÊNCIA DO INCIDENTE

Para o caso de um risco ser aceito (o que inclui os retidos) o mesmo deve ser acompanhado de um planejamento para a ocorrência do incidente, a fim de mitigar suas consequências – o que é designado aceitação ativa, ilustrada na Figura 3.7. Isso, por exemplo, estão presentes nos sistemas de aviação, viagens espaciais, usinas nucleares, petroquímicas etc. Em todos esses exemplos são requeridos estudos de cenários de acidentes com plano de resposta emergencial, e, em alguns casos, plano de operação alternativa e de retorno. Por certo, também é válido para setor elétrico.

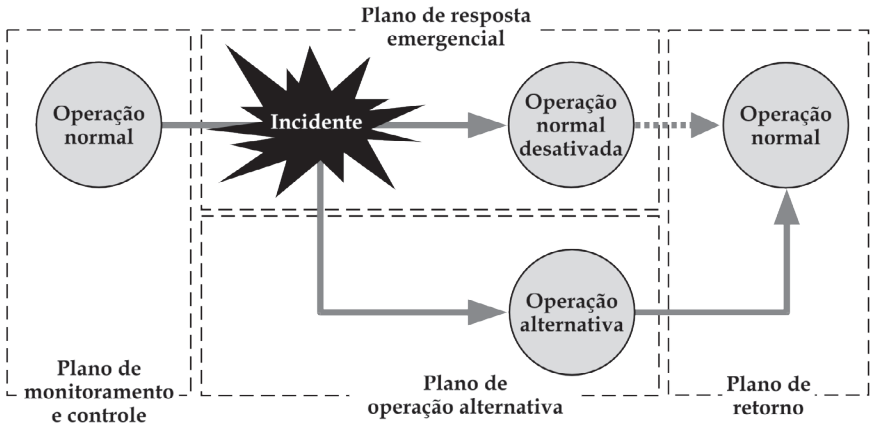


Figura 3.7 Estados de operação de um sistema e os respectivos planos, para o caso de ativação do plano de operação alternativa (CALIL, 2009)

Estudos são desenvolvidos para monitorar indicadores que permitem antever a ocorrência do incidente, e, então, acionar os planos para mitigar as consequências deste incidente. Na possibilidade de se poder antever o incidente, pode-se pensar, adicionalmente, em controlar as causas para sua ocorrência, atuando na sua prevenção – o que é chamado de "plano de monitoramento e controle".

Uma vez identificada a ocorrência do incidente, pode-se adotar duas estratégias, não excludentes: minimizar o impacto e a abrangência do incidente (plano de resposta emergencial) e/ou procurar fornecer alternativas para se executar os processos críticos a fim de mantê-los ativos, mesmo durante o incidente (plano de operação alternativa, ou operação interina).

Por fim, quando for possível retornar à condição normal de operação, aciona-se o "plano de retorno", recuperando os processos da organização e transferindo os processos alternativos para os processos usuais, quando aplicável.

Observa-se que as medidas de tratamento dos riscos atuam, na corrente causal, antes da ocorrência do incidente – objetivando evitá-lo ou fazer com que o mesmo ocorra em menores proporções. As medidas de aceitação ativa, por sua vez, objetivam mitigar as consequências, atuando principalmente após o incidente. No entanto, independentemente do tipo de medidas, atuam como barreiras na corrente causal.

É interessante observar ainda que, no nível do sistema técnico, tanto o monitoramento e controle quanto o planejamento para a ocorrência do incidente se dão, fundamentalmente, por ações de manutenção e garantia de confiabilidade.

Já no nível da unidade organizacional pode-se adotar estratégias como a redundância de sistemas técnicos – de um sistema de comunicação, por exemplo – ou um procedimento para operar em condições críticas.

No nível da organização, por sua vez, pode-se implementar redundância ativa de instalações de uma unidade organizacional (chamadas de *hot site*), como a de um *call center*, por exemplo.

Quanto à possibilidade de ocorrência de incidentes desconhecidos (riscos involuntariamente retidos), pode-se elaborar um plano de gerenciamento de crises, que vise fornecer aos gestores da organização um conjunto de componentes e recursos que podem ser úteis no momento da crise e um planejamento de como tratar a mídia e a comunicação com as partes afetadas. Esse plano contempla todo tipo de incidente, incluindo os que não foram previstos, tais como crises que não resultem na interrupção do negócio ou que tenham proporções além do escopo do sistema de gerenciamento de aviônicos risco (SGR).

3.4 CONSIDERAÇÕES FINAIS

Neste capítulo apresentou-se algumas definições e considerações sobre gestão de risco. Muitas das definições adotadas são coerentes com a ABNT NBR/ISO/IEC Guia 73 (2005), que traz recomendações quanto ao vocabulário relativo ao gerenciamento de risco utilizado nas normas técnicas. No entanto, alguns conceitos apresentados no livro divergem da norma, por exemplo:

- a ABNT NBR/ISO/IEC Guia 73 (2005) apresenta a retenção do risco como uma estratégia de tratamento de risco e, no livro, a retenção foi incluída no processo de aceitação; e
- a norma não considera a terceirização uma estratégia de transferência de risco.

Outros conceitos apresentados também podem divergir do praticado por alguns autores, como o de incidente, que eventualmente é tratado como quase-acidente.

Isto demonstra que não existe um consenso quanto à nomenclatura e os conceitos utilizados na gestão de risco. Contudo, observa-se que ao optar por um sistema de gestão, deve-se também optar por uma nomenclatura consensual na organização. Recomenda-se, ainda, que a confiabilidade, a disponibilidade, a continuidade e a segurança sejam tratadas como atributos do sistema de gerenciamento de risco (SGR).

Outro ponto salientado foi referente aos modelos utilizados para explicar a ocorrência dos riscos. Foi destacado que existem vários modelos para isto. Neste capítulo, porém, foi adotada a teoria multicausal para analisar por que os incidentes ocorrem; o modelo de Mosleh & Dias (2003) para delinear como os incidentes ocorrem; e foi apresentada uma classificação das consequências dos incidentes para orientar a tomada de decisão.

Por fim, foi apresentada uma hierarquização do gerenciamento de risco na organização, na qual, no nível dos sistemas técnicos, a gestão de risco visa garantir a disponibilidade com níveis aceitáveis de segurança. No nível das unidades organizacionais, o foco é manter a continuidade operacional com níveis aceitáveis de segurança; e, no nível da organização, concentra-se na continuidade do negócio e na segurança.

Assim, o capítulo foi escrito para orientar o leitor ao entendimento da terminologia, das abordagens e dos modelos de análise que servem de base para o desenvolvimento dos próximos capítulos. Também objetivou despertar a curiosidade e motivação dos profissionais que atuam em sistemas técnicos complexos a pensarem e planejarem ações apropriadas para garantia da segurança e continuidade, nos diferentes níveis do gerenciamento da organização que atuam.

Capítulo 4

METODOLOGIA PARA GESTÃO DE RISCO

A metodologia de gestão de risco constitui-se de um conjunto de procedimentos e técnicas organizadas, que tem como objetivo gerir sistemas técnicos, humanos e ambientes, com vistas a desenvolver processo de análise, tratamento, aceitação e comunicação do risco. A gestão de risco para alguns, ou gerenciamento de risco para outros, é o processo de administrar exclusivamente o risco. O que é gerir ou administrar o risco? É ter consciência organizacional. Em outras palavras, é pensar na gestão para a continuidade de uma função em um ambiente coletivo, contextualizado por uma indústria, empresa, setor de serviços ou setor público do ponto de vista de um incidente.

Ao chamar atenção para consciência organizacional ou coletiva em relação ao risco, pretende-se chamar atenção para o fato de que todo sistema é portador de perigo e que, segundo a teoria da corrente causal (Figura 3.3), dependendo da causa ou condição, qualquer sistema pode protagonizar um incidente. Aí está a importância de se dispor de uma metodologia de gestão de risco.

A partir da metodologia e das técnicas apropriadas para cada situação ou sistema técnico, a gestão do risco delineia cenários de consequências e ações para monitorar, eliminar, mitigar ou aceitar as consequências.

A Figura 4.1 ilustra as etapas da metodologia de gestão de risco que está dividida em cinco etapas: delineamento, implementação, utilização, revisão e desativação.

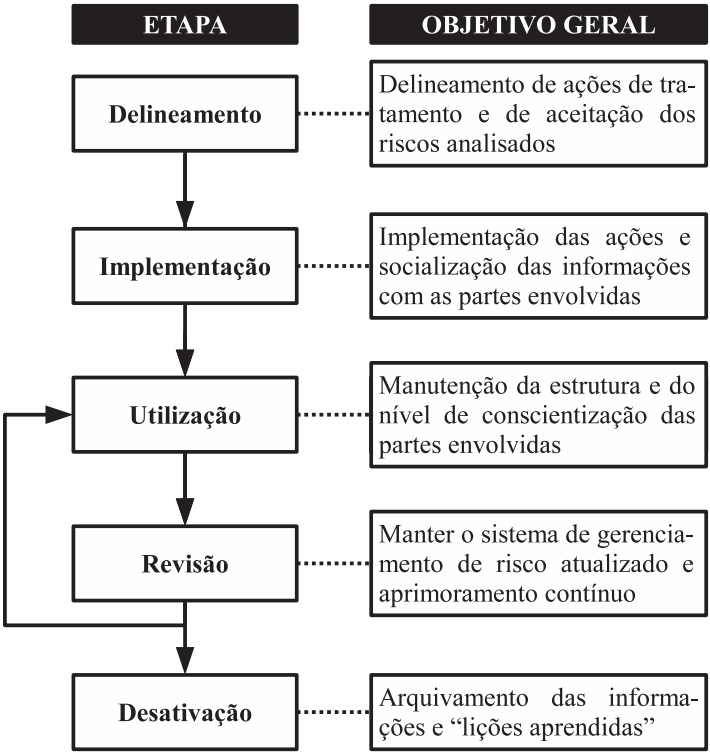


Figura 4.1 Etapas da metodologia de gestão de risco (Adaptada de Calil (2009))

Para se obter uma leitura mais elaborada da Figura 4.1, faz-se a seguir breve apresentação de cada uma das etapas da metodologia de gestão do risco, detalhando ações e apontando as técnicas mais apropriadas para bem definir um plano de gestão de risco para toda organização ou parte dela.

A metodologia de gestão de risco aplicada a sistemas técnicos parte do pressuposto de que no planejamento do produto e no processo de projeto já foram considerados todos os atributos do produto. Por exemplo, foram considerados os atributos de confiabilidade, mantenabilidade, segurança, montagem, operacionalidade, disponibilidade entre outros.

A etapa de delineamento da metodologia de gestão de risco pode ser iniciada pela análise, tratamento e aceitação do risco, dado que os riscos já foram descritos nas etapas de planejamento do produto e no processo de projeto.

4.1 ETAPA DE DELINEAMENTO

A primeira etapa, chamada de delineamento, significa esboçar, projetar ou elaborar um plano para poder gerenciá-lo posteriormente. A etapa de delineamento, foco principal deste capítulo, está dividida em análise, aceitação e tratamento do risco, destacada na Figura 4.1. Esta primeira etapa da figura é muito importante devido ser a mesma uma referência para todas as outras etapas, ou seja, só será implementado, utilizado, revisado o plano de risco que efetivamente estiver delineado. Sem essa etapa bem desenvolvida muito retrabalho ocorrerá e por certo, na presença de um incidente, a etapa de utilização será muito prejudicada, com grande probabilidade de potencializar as consequências.

Para facilitar o entendimento e aplicação desta etapa, propõe-se dividí-la em quatro fases – conforme ilustra a Figura 4.2: informacional, conceitual, preliminar e detalhada. As fases foram adaptadas de Back et al. (2008) que tratam especificamente de projeto de produto. Tal adaptação foi possível porque, como já registrado, delinear equivale a projetar, esboçar, fazer um plano.

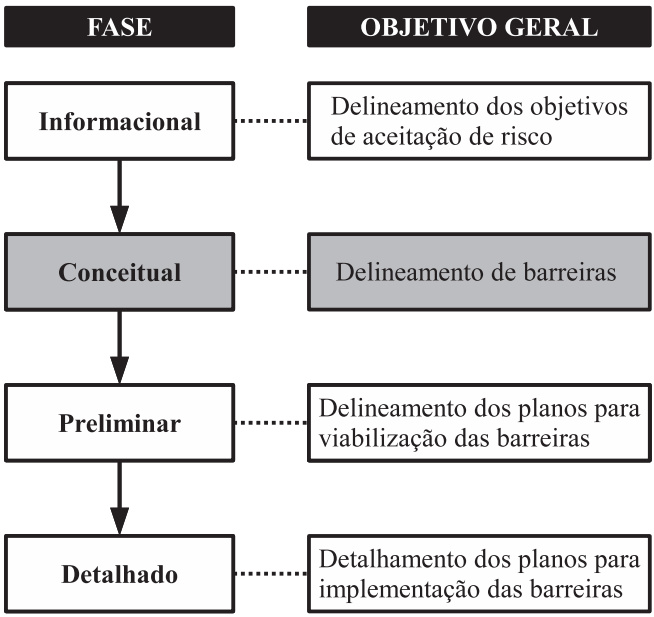


Figura 4.2 Fases da etapa de delineamento da gestão de risco

4.1.1 FASE INFORMACIONAL

A fase informacional da etapa de delineamento procura organizar todas as informações de modos de falhas, causas, efeitos decorrentes das causas e dos modos de falha, condições perigosas de caráter técnico, humano e ambiental, lições aprendidas, cenários de falhas e estudos de falhas efetuados. Atenção especial é dada para o sistema técnico em análise, evidenciando todas as tomadas de decisão que foram feitas no processo de projeto, fabricação, montagem, comissionamento, testes, uso e manutenção.

Além disso, é necessário coletar informações a fim de caracterizar a situação atual, definir as necessidades do sistema, levantar recursos críticos e restrições – como normas, regulamentações e leis. Também é interessante, nesta fase, que se faça uma análise das partes envolvidas (*stakeholders analysis*), para que se possa captar as necessidades e limitações das mesmas.

Identificar e relacionar o risco, como entrada para análise da informação, devem servir de referência para o processo de avaliação dos riscos. Para dar mais racionalidade à análise, recomenda-se que se utilize métricas como "frequência máxima de ocorrência de um evento" ou outros indicadores, por exemplo:

- Tempo máximo de interrupção tolerável (*maximum tolerable outage* – MTO), que é o tempo máximo que se tem para fazer a recuperação da função sem comprometer os objetivos do sistema.
- Objetivo para o ponto de recuperação (*recovery point objective* – RPO), que é o estado em que o sistema deve ser restaurado para garantir que seus objetivos possam ser alcançados, considerando o tempo máximo de interrupção tolerável.
- Custo líquido médio para prevenir uma fatalidade (*net cost of averting a fatality* – NCAF), que pode ser calculado pela Equação 4.1, onde: $\underline{\Delta Custo}$ é o custo adicional ocasionado pela implementação da barreira; $\underline{\Delta Benefícios}$ são os benefícios econômicos decorrentes da implementação da barreira; e $\underline{\Delta Risco}$ é a redução do risco em termos de fatalidades evitadas.

$$NCAF = [\Delta Custo - \Delta Benefícios] / \Delta Risco \qquad (4.1)$$

Cada vez que novo sistema técnico (S.T.), como está apresentado na Figura 3.6, for incluído no estudo de risco da organização, e um novo objetivo for definido, há que considerar os indicadores definidos na equação 4.1.

A definição dos objetivos de aceitação deve levar em consideração os valores da organização, a visão e o planejamento estratégico de médio e longo prazo, para que o sistema possa se adaptar às condições futuras.

Na saída da fase informacional têm-se os objetivos de aceitação de risco delineados, ou seja, identificados, organizados e priorizados para serem tratados como entradas na fase seguinte da etapa de delineamento.

4.1.2 FASE CONCEITUAL

A partir dos objetivos de aceitação dos riscos desenvolve-se um processo de análise dos riscos identificados. Análise de risco é o tema central do livro e é equivalente à *risk assessment* na literatura técnica inglesa. O objetivo da fase conceitual da etapa de delineamento é desenvolver a análise de risco e delinear as barreiras, como apresentado na Figura 4.2.

O primeiro passo no processo de análise é caracterizar o estado inicial do sistema de probabilidade do incidente estar próximo de zero, para o estado futuro, com a probabilidade do incidente tender à unidade, ou seja, falha iminente e incidente deflagrado.

A descrição entre o estado inicial e o estado futuro pode ser feita pela teoria da corrente causal, que permite visualizar as causas e condições no estado inicial, o incidente e a conseqüência no estado final. Entre esses dois estados têm-se os eventos intermediários das condições perigosas, de evento gatilho, de barreiras, falhas das barreiras, como explicitado na Figura 3.3.

Quando um incidente ocorre tem-se um novo estado inicial. Então, deve-se analisar quais suas consequências para o estado futuro e as possíveis correntes causais deflagradas pelo estado inicial. Procedendo-se dessa maneira, é possível caracterizar os cenários envolvidos e optar por aceitá-los ou não. Por decorrência, define-se o que deve ser feito à luz dos objetivos de risco determinados na fase do delineamento informacional.

O processo de avaliação também deve permitir que se identifiquem quais cenários são mais críticos, o que possibilitará fazer uma priorização dos riscos, e, dessa forma, direcionar os recursos da organização.

Os riscos considerados inaceitáveis devem ser tratados ou ser relutantemente aceitos. Nesse último caso, ainda é possível delinear medidas de aceitação ativa para mitigar as consequências do incidente, como, por exemplo, um plano de evacuação do prédio, diante a ocorrência de um incêndio.

Por fim, é recomendável fazer estimativas dos esforços necessários para a implementação das barreiras e avaliar a relação custo–risco–benefício das medidas.

Kumamoto & Henley (1996) apresentam uma estrutura (Figura 4.3) que pode ser utilizada para estabelecer critérios de aceitação de riscos, como os apresentados a seguir:

- Riscos sem benefício devem ter a frequência reduzida abaixo (inclusive) do limite "L" (limite inferior de frequência).
- Riscos com benefício extremo devem ser relutantemente aceitos (i.e., retidos).
- Riscos com benefício moderado e nível acima de "U" são inaceitáveis e devem ter suas frequências diminuídas para abaixo de "U".
- Riscos com benefício moderado e nível abaixo de "L" são aceitáveis.
- Riscos com benefício moderado e nível entre "U" e "L" devem ser estudados, para verificar se o benefício justifica o risco, ou não. Se justificar, o risco pode ser retido e, caso não justifique, a frequência deve ser reduzida até se justificar ou cair para nível inferior a "L". A justificativa deve ser feita com base no que é razoavelmente praticável em termos de redução do risco (ALARP – *as low as reasonably practicable*).

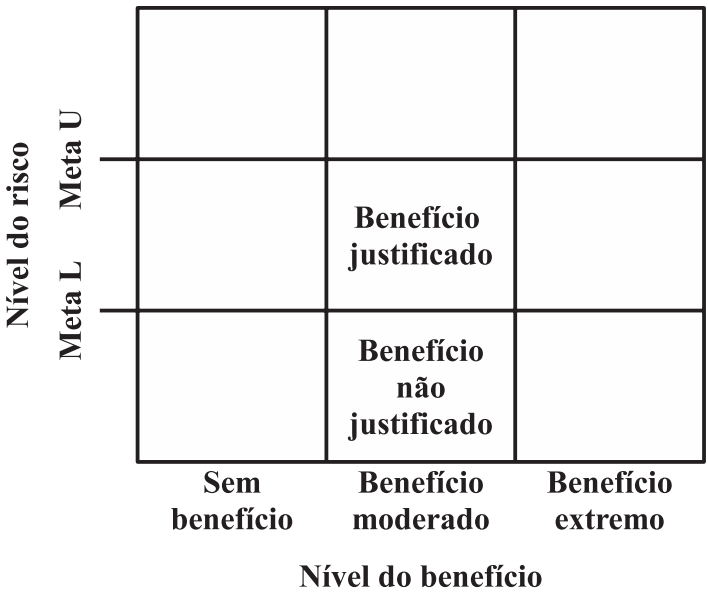


Figura 4.3 Critérios de aceitação de risco (KUMAMOTO & HENLEY, 1996)

A definição de metas de segurança (limites "L" e "U") simplifica o processo de análise do risco, já que não se devem estudar todos os riscos de uma planta. Os valores dos limites da taxa de ocorrência variam de autor para autor e de área de aplicação. Como exemplo, pode-se indicar $L = 10^{-6}$/[ano; indivíduo] e $U = 10^{-3}$/[ano; indivíduo]. Lê-se, para o caso do limite inferior (L), a ocorrência de um evento ao ano para cada 1.000.000 de indivíduos, e, para o caso superior (U), a ocorrência para cada 1.000 indivíduos (KUMAMOTO & HENLEY, 1996).

Quanto ao conceito de "benefício", conforme apresentado no capítulo anterior, está relacionado à utilidade do risco. Uma forma de se avaliar a utilidade do risco e considerar a hipótese de não se expor ao mesmo. Quais os prejuízos que se terá, ou que benefícios deixa-se de ter? Fazendo esse raciocínio inverso, pode-se ponderar quão importante é o risco para a organização. Caso seja de benefício extremo, pode-se relutantemente aceitá-lo. No entanto, isto não significa que não se deve tratá-lo ou aceitá-lo de forma ativa. As medidas que se justificarem – coerentemente com estratégia de ALARP – devem ser implementadas.

Um dos resultados da fase do delineamento conceitual é definir barreiras a serem implementadas para:

Garantir que a condição inicial de probabilidade de incidente zero não mude;

Isolar a condição perigosa do evento gatilho;

Evitar, mitigar a ocorrência de um incidente;

Estabelecer condições para retornar a condição inicial, caso o incidente ocorra.

4.1.3 FASE PRELIMINAR

O objetivo desta fase é viabilizar os conceitos relativos às soluções para eliminar, mitigar ou aceitar os riscos, aqui denominados de barreiras, desenvolvidos na fase conceitual. A partir dos conceitos, estrutura-se ações para construir e implementar as barreiras que devem evitar ou diminuir a probabilidade de ocorrência de incidentes.

Por vezes, mudanças mais significativas tornam-se prementes em decorrência de ações e das barreiras. Nesse caso é recomendável que se faça também mudanças nas instalações e na estrutura organizacional. Por decorrência, há que se delinearem novos planos de aceitação de risco, e deve-se também atuar sobre os planos de monitoramento e controle; resposta emergencial; operação alternativa; e retorno. Por fim, ações relativas à capacitação dos colaboradores e à divulgação para as partes envolvidas devem estar apresentadas no plano de comunicação. É, então, recomendável que se desenvolva os planos em condições de colocá-los em operação, pelo menos em nível de um "protótipo", ou seja, que possa ser testado numa simulação.

No plano de monitoramento e controle (Figura 3.7), incluem-se os procedimentos para monitorar a situação a fim de prever a ocorrência do incidente e os procedimentos para manter a condição perigosa dentro de limites aceitáveis. Note-se que esses últimos procedimentos são, na verdade, medidas de tratamento de risco, e não de aceitação, pois atuam na prevenção do incidente. No entanto, para fins de aplicação, é conveniente agrupar os procedimentos de controle ao de monitoramento.

Assim, o plano de monitoramento e controle é um conjunto de procedimentos – se possível vinculados a procedimentos operacionais – que visa avaliar a condição atual para, caso exista algum desvio, tomar medidas para retornar à condição de normalidade.

Fazem parte de um plano de monitoramento e controle ações como: acompanhamento das condições meteorológicas, avaliação da pressão de um tanque (e sua correção, caso esteja fora da faixa de segurança), controle de acesso (físico ou por *software*) etc.

O plano de resposta emergencial procura impor barreiras para que o incidente aconteça em menor proporção – também chamado de plano de mitigação. Este plano é um conjunto de ações que tem como objetivo minimizar o impacto nas pessoas, no ambiente, no patrimônio e nas funções vitais da organização submetida ao incidente em questão.

Exemplos típicos de planos de resposta emergencial são: planos de evacuação do prédio; combate a princípio de incêndio (brigada de incêndio); primeiros socorros; desligamento emergencial; etc.

O plano de operação alternativa (ou operação interina) deve ser elaborado para cada incidente estudado, visando estabelecer formas alternativas de se executar os processos críticos, mesmo que com alguma degradação de desempenho.

Fazem parte do plano de operação alternativa tarefas como: definição da equipe e responsabilidades; aquisições necessárias; transporte e logística; estimativa de custos; procedimentos etc.

Observe-se que, por se tratar de uma alternativa para os processos críticos, o plano deve ser executado por uma equipe especialmente definida para operação nesta condição.

Quanto ao plano de retorno, esse traz as atividades relativas ao restabelecimento das condições normais de operação. Assim como o plano de operação alternativa, o plano de retorno deve ser elaborado para cada incidente e, de maneira análoga, há que definir as condições para o retorno à operação normal; à definição da equipe e responsabilidades; o transporte e à logística, entre outras.

Adicionalmente, pode-se elaborar um plano de gerenciamento de crises que traz orientações úteis aos gestores da organização, para o caso de ocorrer um incidente – mesmo que não tenha sido previsto no SGR – tais como um planejamento de como tratar a mídia e a comunicação com as partes afetadas.

No que se refere ao plano de ação, é importante que se especifiquem os produtos e serviços a serem adquiridos – isso inclui consultorias e apólice de seguros – facilitando, assim, o levantamento dos custos envolvidos em cada ação. Também se deve atualizar as atribuições dos colaboradores e fazer a revisão da estrutura organizacional.

O plano de comunicação deve contemplar o planejamento da capacitação dos colaboradores e a divulgação para as partes envolvidas.

Quanto à capacitação, destaca-se a necessidade de se construir uma cultura de gestão dos riscos, que deve abranger toda a organização, pois ela é crucial para o sucesso do sistema de gerenciamento de risco.

O pessoal sem responsabilidade específica na gestão dos riscos pode ater-se somente à conscientização ou a um nível de proficiência pré-estabelecido de como proceder nas tarefas gerais da organização. Já os participantes dos planos de aceitação devem receber capacitação estruturada que garanta as habilidades, a competência (colocando em prática os planos) e o conhecimento necessário.

Assim, os planos de comunicação abrangem tanto a capacitação teórica quanto prática – objetivando alcançar a condição de se executar os planos de maneira automática, "sem ter que pensar".

Também faz parte dos planos de comunicação o relacionamento com as partes envolvidas. É recomendável existir um relacionamento das ações dos planos de aceitação com outras instituições, como Defesa Civil, Corpo de Bombeiros, assistências técnicas etc. Logo, é necessário elaborar planos de comunicação para definir como será esta interação e manter as partes envolvidas atentas.

A comunicação com outras instituições também contempla a companhia seguradora. É interessante que se faça um plano para acionamento da apólice, descrevendo como fazer, quem contatar, as informações e documentos necessários etc.

Fazem parte dos planos de comunicação, informações como: periodicidade de execução da capacitação; tipo de capacitação (teste de mesa, simulação do uso dos planos etc.); conjunto de instruções para execução do plano; responsável pelo plano de capacitação; e quem deve ser submetido à capacitação.

Na fase do delineamento preliminar, é importante orçar, na forma mais pormenorizada possível, os esforços necessários para a implementação dos planos, pois será com base nos valores que será planejada a implementação. Para tanto, leva-se em consideração não apenas o custo relativo a cada item dos planos, mas também o tempo necessário para a implementação; a disponibilidade de recursos internos da organização, e disponibilidade dos recursos

a serem adquiridos. É necessário avaliar os esforços referentes à manutenção da estrutura e à capacitação ao longo do tempo após a implementação. Por fim, é recomendável fazer uma avaliação de custo–risco–benefício, priorizar as medidas de tratamento a serem implementadas, e, eventualmente, descartar as não justificadas.

Essa avaliação baseia-se nos critérios de aceitação definidos na fase informacional. A ideia é confrontar os benefícios e a redução do risco com os custos das medidas, para verificar se as mesmas são justificáveis e, posteriormente, priorizá-las. Por exemplo, uma possível medida para alcançar o MTO (*maximum tolerable outage*) relativo ao fornecimento de energia elétrica é a aquisição de grupos geradores diesel. Adicionalmente, pode-se operá-los no "horário de pico", quando a energia elétrica é mais cara, e, assim, obter um benefício – que é a redução das despesas. No entanto, essa medida também pode introduzir novos riscos, que também devem ser avaliados.

Por fim, elabora-se o planejamento de implementação. Uma vez que as ações estão priorizadas, faz-se o planejamento para implementá-las. Infelizmente, na maioria das vezes, a organização não dispõe de recursos para implementar todos os planos de imediato. Assim, no plano de ação, planeja-se quando e como cada ação será implementada.

4.1.4 FASE DETALHADA

Nesta fase, é feito o detalhamento da etapa de delineamento e a implementação de testes e simulações dos planos preliminares obtidos na fase anterior.

No detalhamento dos planos, é importante contemplar o responsável pela ação, o planejamento dos recursos (incluindo recursos humanos), o custo, o cronograma de execução, o cronograma de desembolso e os riscos relacionados à implementação.

No que se refere ao plano de ação, destaca-se, ainda, a elaboração das especificações técnicas de compra (de produto ou serviço). No caso de envolver recursos internos, também é interessante elaborar uma especificação técnica, para evitar retrabalho.

Quanto aos planos de aceitação, seu conteúdo e estrutura variam de caso para caso, podendo ser desde uma lista de telefones dos contatos que devem ser feitos em determinadas situações até procedimentos detalhados – uma norma interna, por exemplo. Nesse

último caso, recomenda-se que o documento seja dividido em duas partes: uma estruturada cronologicamente (especificando o que deve ser feito e quem deve fazer), e outra estruturada por responsabilidade – para que cada um saiba de suas respectivas incumbências. Nesse sentido, também é interessante a geração de fichas de atribuições listando os procedimentos que cada um deve realizar.

Para facilitar a gestão da documentação digital, recomenda-se o uso de *software* específicos, chamados de DMS (*document management system*).

O detalhamento do plano de comunicação é de importância destacada para o sucesso do programa. Sem a devida capacitação, o corpo técnico não irá proceder como deveria, comprometendo a eficácia do programa.

Também é importante que os planos sejam testados por meio de lista de verificação (*check-list*) e de simulações virtuais do plano (teste em mesa). Esses dois tipos de teste são muito importantes para identificar possíveis problemas e melhorias nos planos, antes mesmo de serem executados.

4.2 ETAPA DE IMPLEMENTAÇÃO

A segunda etapa é de implementação, que significa, resumidamente, integrar os planos de tratamento do risco na operação normal, na emergência, incluindo nesse caso desativar a operação, operar em carater alternativo ou retornar às condições normais, como mostra a Figura 3.7. Na implementação socializam-se as informações na forma de capacitação, treinamento, comunicação, sinalização, rotinas e procedimentos. Organizam-se processos para ampla aceitação do risco, desenvolvem-se instrumentos de controle, faz-se adequação de organograma e desenvolvem-se estruturas alternativas de gestão para casos extremos.

Nesta etapa implementam-se em toda a estrutura organizacional ou em parte dela os planos elaborados, e as informações são socializadas com todas as partes envolvidas, de acordo com o planejamento de implementação desenvolvido no plano de ações.

A implementação dos planos de ação instala a estrutura necessária para os planos de aceitação, tais como: instrumentos para fazer o controle; alterações no organograma; estruturas alternativas que

serão utilizadas em uma contingência e assim por diante. Para uma efetiva implementação desses planos faz-se a devida capacitação dos colaboradores e a divulgação para as partes interessadas, conforme determinado no plano de comunicação.

Destaca-se que deve-se evitar o "efeito serrote", no qual os colaboradores são motivados, mas não se implementa o programa adequadamente – resultando em desmotivação. Então, faz-se uma nova investida na capacitação, e assim por diante. Isso pode gerar desmotivação, desconfiança e descrença na ação.

É importante que seja construído um contexto para se desenvolver a cultura do gerenciamento de risco – a ser integrada ao *modus operandi* da organização. Fazer visita a outras instituições e receber visitantes é uma forma boa de criar a cultura para o gerenciamento do risco.

Uma vez instalada a estrutura necessária para execução dos planos, é importante fazer simulações do uso dos planos de aceitação. A execução do plano possibilita que as pessoas envolvidas estejam mais preparadas, e aumenta a conscientização de todos os colaboradores, além de evidenciar deficiências e possíveis melhorias. Novos testes e simulações, além dos executados na fase detalhada do delinemanento, podem ser feitos em módulos ou na totalidade do plano, como se realmente estivesse passando pelas contingências. Após a realização dos testes, elaboram-se relatórios apresentando os procedimentos executados e as "lições aprendidas". Destaca-se que a implementação dos planos não garante que eles serão cumpridos. Há que manter o programa de treinamento até o ponto de os procedimentos serem executados de maneira automática e intuitiva. Mesmo assim, não se pode perder a comunicação.

É importante observar que é possível chegar à conclusão, após a execução dos testes e simulações, de que a condição que se esperava alcançar com a implementação das barreiras não condiz com a realidade. Isto significa que o processo de avaliação de risco executado na fase do delineamento conceitual não está coerente com a realidade. Nesse caso, deve-se deflagar uma revisão do sistema de gerenciamento de risco para verificar se a situação real, após a implementação das barreiras, é aceitável ou se serão necessárias novas barreiras.

4.3 ETAPA DE UTILIZAÇÃO

A etapa de utilização da gestão do risco acontece efetivamente somente se ocorrer o incidente. O ideal é que nunca seja necessário vivenciar todos os planos da etapa de utilização. Ou seja, que fique no máximo em nível do plano de monitoramento e controle (Figura 3.7). Contudo, se o incidente ocorrer, há que utilizar os planos de resposta emergencial, que podem se refletir na desativação da operação, ou na implementação de uma operação alternativa, até que o plano de retorno do incidente esteja viável.

Na etapa de utilização, os planos de aceitação (monitoramento e controle, resposta emergencial, operação interina e retorno à operação normal) também demandam por requisitos e suporte da estrutura necessária para executá-los, e por recomendações advindas das lições aprendidas dos testes e simulações anteriormente feitas para uso nestes planos de aceitação.

No que se refere à utilização dos planos de aceitação, prevê-se a execução do plano de monitoramento e controle durante a operação normal. Idealmente, estas ações situam-se nas atribuições cotidianas dos colaboradores –, conforme ilustrado na Figura 4.4.

No caso do incidente ser desencadeado, executam-se os planos de resposta emergencial ou operação interina (alternativa) e, ao final, retorna-se à condição normal de operação.

Os teste, e simulações e a manutenção da estrutura visam manter a capacidade de resposta da organização, mantendo o nível de conscientização adequado e as equipes devidamente capacitadas, além de verificar a integridade das instalações, equipamentos e insumos destinados à resposta de um incidente.

Adicionalmente, é importante que o programa seja regularmente auditado pelo sistema de qualidade, a fim de assegurar que os procedimentos estão sendo rigorosamente cumpridos e que a organização está apta a tomar as medidas estipuladas nos planos – tanto as relativas aos procedimentos quanto às instalações.

Os planos de resposta emergencial, de operação interina e de retorno devem ser exercitados conforme definido nos planos de comunicação. Esses exercícios possibilitam avaliar a capacitação dos colaboradores e manter a execução das ações de forma automática; identificar problemas de transferência de informações ou outra de-

ficiência de comunicação; destacar pressuposições que precisem ser questionadas; manter o nível de conscientização da organização e das partes envolvidas etc.

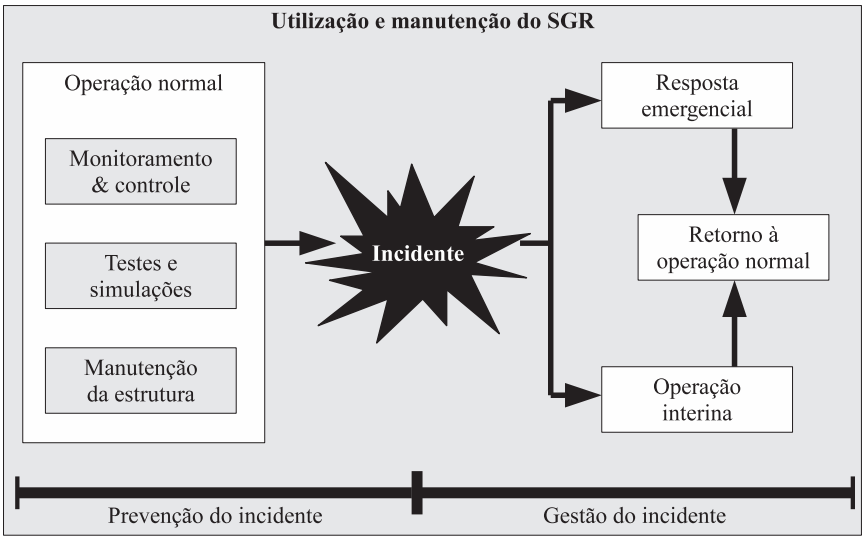


Figura 4.4 Utilização e manutenção da gestão de riscos (CALIL, 2009)

É importante monitorar as mudanças culturais para avaliar a qualidade e a eficácia da capacitação e da conscientização das partes afetadas. Caso se constate alguma deficiência, revisa-se os planos de capacitação.

Note-se que, além de evidenciar deficiências, a utilização dos planos também permite identificar possíveis melhorias. Essas devem desencadear a revisão da gestão de risco (GR).

Independentemente – por simulação ou por utilização durante um incidente – ao final da execução dos planos, elabora-se um relatório descrevendo as ações e lista-se as eventuais deficiências e as possíveis melhorias, como "lições aprendidas".

4.4 ETAPA DE REVISÃO DA GESTÃO DE RISCO

A etapa de revisão inicia pelo delineamento (Figura 4.1). É aconselhável fazer a revisão e atualização dos planos de gestão (também chamado de planos de gerenciamento de risco), mesmo que

nenhum evento de risco, ou incidente tenha ocorrido. A revisão é fortemente recomendável quando houver mudanças na organização pela inclusão, retirada ou atualização tecnológica na organização, alteração no ambiente, alteração no contexto da administração, do gerenciamento, da operação ou da manutenção. A ação de revisão é obrigatória se algum incidente tenha ocorrido no contexto da estrutura organizacional ou em parte dela.

Consiste no redelineamento do sistema de gerenciamento de risco e na implementação das alterações a serem feitas para seu aprimoramento e atualização.

As atualizações são recomendáveis sempre que houver alteração significativa na organização ou quando novas informações relevantes surgirem, tais como: alteração das condições econômicas, surgimento de novas tecnologias, exigências legais, alterações no planejamento estratégico da organização, uma nova possível barreira identificada, e novos riscos identificados. A ação de aprimoramento visa corrigir deficiências identificadas e alcançar a melhoria contínua (sempre que for identificada alguma possível melhoria ou periodicamente) para aperfeiçoar os planos, ampliar o escopo (identificando novos riscos), revisar as tomadas de decisões anteriores.

O objetivo da revisão do sistema de gerenciamento de risco (SGR) é garantir que os riscos sejam tratados de forma adequada, e que se planeje, da melhor maneira possível, para os riscos aceitos – além de manter o sistema de gerenciamento de risco coerente com a situação real da organização, o que inclui a desativação da parte do SGR, quando aplicável.

Note-se que, na revisão do SGR, os processos da metodologia, as técnicas e as ferramentas já são conhecidos pelos colaboradores, e a revisão tende a ser facilitada. Também não é necessário repetir todos os processos do delineamento e implementação, e sim concentrar-se nos pontos que foram influenciados pelo fator que deflagrou a revisão (no caso de uma revisão geral, todos os processos devem ser contemplados).

É interessante destacar que também podem ser feitas alterações nos processos em relação ao delineamento e a implementação, utilizando, por exemplo, outras técnicas para se ter outra visão na análise. Por exemplo, em uma revisão, opta-se pelo uso das estruturas das técnicas FTA e ETA em substituição à técnica CNEA.

Em última análise, a busca por novas informações deve ser constante, e a revisão do SGR não deve restringir-se às informações disponíveis, geradas no delineamento e na implementação ou em revisões anteriores. Nesse sentido, deve haver um comprometimento dos colaboradores na busca do aprimoramento contínuo.

4.5 ETAPA DE DESATIVAÇÃO

A etapa de desativação consiste em descontinuar o plano de utilização de um risco que ao longo do tempo foi eliminado ou considerado desprezível. É pouco razoável pensar que pode ser desativada a gestão de risco de todo um sistema. Assim, o processo de desativação em si compreende no arquivamento das informações e "lições aprendidas" para que elas possam ser reaproveitadas no futuro.

Faz pouco sentido pensar na desativação de todo o sistema de gerenciamento de risco, mas é razoável pensar em desativar a parte referente a um risco que, ao longo do tempo, foi eliminado ou passou a ser considerado desprezível devido, por exemplo, a uma mudança de tecnologia. A desativação de uma parte do sistema de gestão de risco é razoável no contexto da revisão do processo de gerenciamento de risco (GR).

O processo de desativação em si compreende o arquivamento das informações e "lições aprendidas", para que elas possam ser reaproveitadas no futuro. Já a capacitação continuada dos colaboradores, divulgação para as partes envolvidas e outras ações para readequação da gestão de risco fazem parte não só da etapa de revisão, mas sim de todo o processo de gerenciamento.

4.6 CONSIDERAÇÕES FINAIS

A abordagem desenvolvida neste capítulo procurou apresentar conceitos e diretrizes para o gerenciamento de risco, bem com técnicas que serão apresentadas ao longo do livro. A metodologia trouxe um formato de desenvolvimento aderente ao de desenvolvimento de produtos por acreditar-se que um plano para gerenciamento de risco é um produto para a organização. Note-se que a análise de risco está inserida, destacadamente, na fase do delineamento conceitual.

No entanto, todo o processo de gerenciamento de risco deve ser considerado no momento de se fazer a análise.

Dado a complexidade do tema, não foi objeto do capítulo detalhar os processos relacionados à gestão de risco, mas sim apresentar o processo e a motivação (ou momento) em que a análise de risco deve ser desenvolvida. Isto porque, tendo bem definido o momento, torna-se mais fácil entender as entradas e possíveis saídas do processo.

Mas como executar o processo de análise de risco? Quais técnicas são necessárias para dar suporte a este processo?

Mais uma vez, não existe apenas uma resposta para estas perguntas. As técnicas são a base da análise e, por isso, serão destacadas na forma de capítulos. No Capítulo 14 será abordado e exemplificado algumas ações aqui expressas. Além das técnicas, o conhecimento da organização quanto à gestão, o capital tangível e não tangível, as metas existentes, o contexto industrial onde está inserida e a legislação de referência formam o arcabouço que servirá de base para trabalhar as saídas objetivas da análise de risco.

Evidentemente, de nada adianta a análise de risco se não houver uma decisão de gerenciamento do risco. Assim, dispor de uma metodologia de gestão de risco dominada em todos os níveis da organização é muito importante para a continuidade da função principal da mesma. Em alguns casos, a gestão de risco tem se destacado como um diferencial competitivo, principalmente quando se trata de sistemas complexos, e cuja função é importante para a sociedade, como por exemplo: eletricidade, água, comunicação, combustível etc. Há também situações em que a gestão de risco é uma imposição legal e, quando bem gerida, proporciona ganhos financeiros nas negociações com seguradoras.

Os capítulos seguintes apresentam as principais técnicas recomendadas para desenvolver a análise de risco e as informações para a gestão do risco.

Capítulo 5

IDEFØ

IDEF (*integrated definition for function modeling*) é uma família de técnicas que tem o objetivo de representar modelos para auxiliar a tomada de decisões, ações e atividades a serem racionalizadas dentro de uma organização. Algumas das técnicas IDEFs já estão maduras, a exemplo da IDEFØ (para modelagem funcional), a IDEF1 (modelagem de informação) e a IDEF2 (modelagem de sistemas dinâmicos).

A técnica IDEFØ é uma técnica de modelagem funcional originada de um programa para auxiliar a manufatura chamada de ICAM (*integrated computer aided manufacturing*), que contribuiu para a modernização tecnológica e aumentou a produtividade na indústria aeronáutica estadunidense, pelo emprego sistemático de tecnologias computacionais, durante os anos de 1970 (NIST, 1993).

Quando bem desenvolvida, a técnica IDEFØ ajuda a organizar a análise dos processos e promove uma boa comunicação entre os vários agentes destes processos (pelo uso de recursos gráficos simplificados), como, por exemplo, entre o analista e o cliente – ou entre especialistas – e a busca de consenso na tomada de decisões. Define-se processo como a combinação de um grupo de atividades dentro de uma organização cuja ordem e dependência lógica é definida por uma dada estrutura, com o objetivo de produzir um resultado esperado. Um modelo adequado permite o bom entendimento dos processos dentro de uma organização e a forma de interação entre os mesmos. A utilização da técnica visa identificar as variáveis principais que exercem influência sobre o desempenho dos agentes envolvidos no processo analisado, permitindo assim formalizar argumentos para planejar ações que atuem em cada uma das variáveis. Ao estudar a técnica IDEFØ, verifica-se que ela também é eficaz para a capacitação, em face dos modelos representarem uma síntese do processo, interrelacionando as funções que se quer analisar, as respectivas entradas e saídas, os controles externos e os mecanismos específicos que atuam sobre estas funções.

5.1 CONSIDERAÇÕES SOBRE A TÉCNICA IDEFØ

De maneira geral, o objetivo da IDEFØ é orientar ações de melhoria baseadas em argumentos racionais, fundamentados na função de entrada e na de saída desejável de processos, a partir dos mecanismos para executar a função e dos respectivos controles para garantir a saída desejável.

A Figura 5.1 sintetiza o modelo de representação da técnica IDEFØ. É importante destacar que a IDEFØ é uma linguagem de documentação e para isso utiliza elementos de linguagem padronizados para representar os processos. Para tanto, as caixas representam funções – definidas como atividades, processos ou transformações – que são detalhadas em caixas de nível inferior (subfunções). O código da função principal é A0, e de suas subfunções A1, A2, A3, e assim por diante. A partir do segundo nível, acrescenta-se um número a mais para identificar cada caixa, como está representado na Figura 5.1.

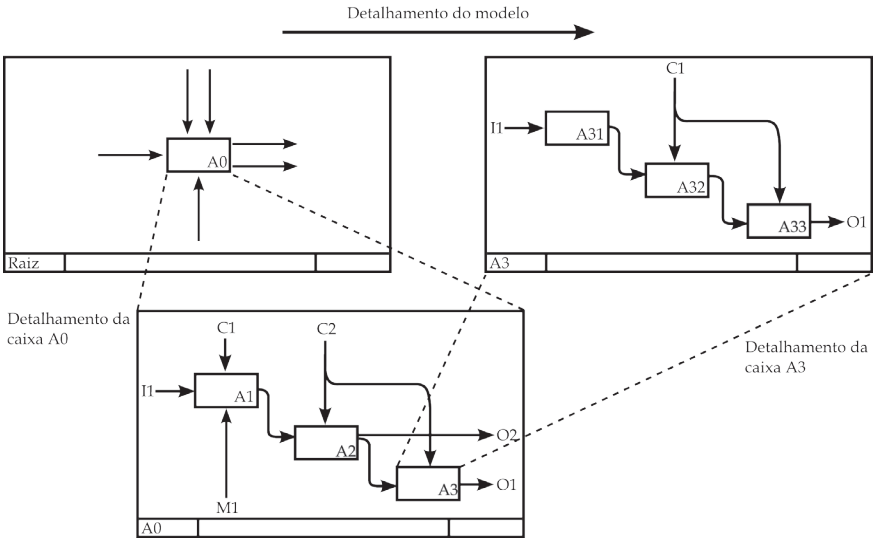


Figura 5.1 Desdobramento das atividades do modelo

O nível de desdobramento depende da complexidade do processo a ser analisado e do detalhamento requerido para a decisão do planejador. Evidentemente, quanto maior for o detalhamento mais complexa fica a análise.

As setas representam informações ou objetos relacionados às funções a serem executadas. As setas horizontais são as entradas e

saídas das funções. As primeiras representam as entradas necessárias para o desenvolvimento da função especificada na caixa, e as de saída representam os dados ou objetos que foram produzidos. Setas de controle definem as condições requeridas para a produção das saídas adequadas e são conectadas no lado de cima de uma caixa. Finalmente, as setas de mecanismo definem os meios ou ferramentas a partir dos quais será exercida a função especificada pela caixa. Devem apontar para cima e estão conectadas no lado de baixo da caixa.

As regras de sintaxe definem como os componentes são utilizados. Os diagramas fornecem o formato para descrever o modelo graficamente, que é, em si, o fundamento da IDEFØ. Em outras palavras, representam a escrita, ou a grafia da análise das funções pelo uso desta técnica. Para um melhor entendimento do modelo, faz-se uso de textos explicativos que descrevem as funções modeladas e os respectivos controles, mecanismos, entradas e saídas. Adicionalmente, também é recomendado que seja feito um glossário com a definição de palavras-chave, frases ou acrônimos utilizados.

Observa-se que a representação de um processo, a partir desta técnica, ocorre tanto no sentido das entradas para saídas quanto no sentido contrário, partindo das saídas para as entradas, podendo assim representar todos os parâmetros presentes no processo em análise.

O objetivo da técnica é representar o processo como um todo. Por vezes, o analista comete o erro de enxergar as setas, simplesmente, como uma sequência de atividades. Isso, por vezes, ocorre em face das atividades estarem organizadas da esquerda para a direita, conectadas pelas linhas de fluxo. Assim, é natural assumir, de maneira equivocada, que os componentes do modelo representam uma sequência.

Os componentes da sintaxe IDEFØ são caixas, setas, regras e diagramas. Regras definem como os componentes são usados, e os diagramas fornecem um formato para descrever modelos tanto verbal quanto graficamente. Cada caixa representa uma parte de um processo. Um processo sempre tem um nome ou um rótulo que o descreve. É normalmente representado por um verbo e um substantivo, por exemplo: gerar energia. É também sabido que um processo transforma ou cria. Assim, todo o processo tem o propósito de produzir uma saída específica, que é o resultado de uma transformação de alguma entrada, com a utilização de algum recurso (mecanismo) e sob alguma condição (controle).

5.1.1 CAIXAS

A caixa representa a função modelada, sintetizando as informações de entrada e de saída, como indicada na Figura 5.2. Para efeito de sintaxe, os seguintes pontos são levados em consideração:

- A caixa deve ser retangular e composta de linhas contínuas.
- Cada caixa terá dentro dos seus limites o nome da função que a representa. O nome deve ser um verbo ativo ou frase verbal que descreva a função, tais como: projetar eixo, fazer orçamento, dentre outros.
- Cada caixa recebe uma identificação do tipo alfanumérica, denominada de rótulo (TAG), localizada no canto inferior direito da caixa, Figura 5.2. Por exemplo, o rótulo da função principal deve ser A0, de suas subfunções A1, A2, A3 e assim por diante. A partir do segundo nível, acrescenta-se um número a mais para identificar cada caixa, como é observado na Figura 5.1.

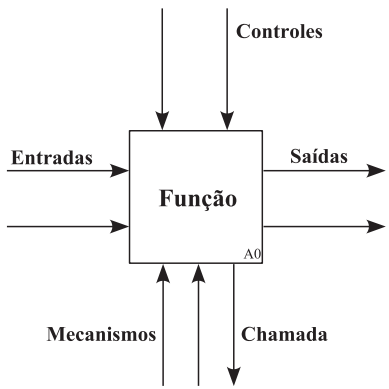


Figura 5.2 Exemplo de caixa, setas e demais elementos do IDEFØ

Com exceção da caixa única A0, um diagrama deve conter no mínimo três e no máximo seis caixas, que são organizadas do canto esquerdo superior para o canto direito inferior, como degraus de uma escada. Qualquer seta de saída de uma determinada caixa pode prover uma entrada, um controle e/ou um mecanismo para qualquer outra caixa, sendo possível que uma mesma seta forneça dados ou objetos para múltiplas caixas, pelas ramificações, como está indicado na Figura 5.1.

5.1.2 SETAS

As setas no IDEFØ não representam fluxo ou sucessão como nos fluxogramas de processo tradicionais. Carregam dados ou objetos relacionados às funções a serem executadas, e, para efeito de sintaxe, os seguintes aspectos são levados em consideração:

- serem compostas de um ou mais segmentos de linhas contínuas;
- ter uma ponta de flecha na extremidade terminal;
- serem verticais ou horizontais, nunca diagonais;
- extremidades das setas devem tocar o perímetro exterior da caixa;
- serem conectadas nos lados da caixa, não nas diagonais;
- segmentos de seta podem se ramificar ou unir;
- segmentos de seta devem ser retos, com a possibilidade de mudar de direção por meio de um pequeno arco de 90°.

Na Figura 5.3 tem-se a sintaxe das setas, qual seja: serem compostas de um ou mais segmentos de linhas contínuas; ter um rótulo; ter uma ponta de flecha na extremidade terminal; serem verticais ou horizontais (nunca diagonais) com a possibilidade de mudar de direção por um arco de 90º; ser conectada ao perímetro exterior nos lados da caixa (não nos cantos) e o segmento de seta pode se ramificar ou unir.

A obediência à sintaxe é muito importante na uniformização da comunicação no IDEFØ para garantir o registro da representação da análise a partir das informações dos especialistas. No diagrama, as setas carregam informações de entrada, mecanismo, controle e saída.

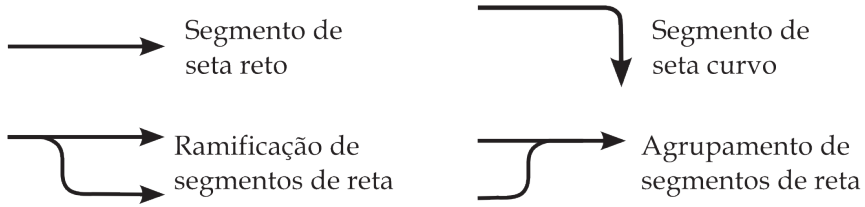


Figura 5.3 Representação de setas

A Figura 5.4 é um exemplo de representação das setas ligadas às caixas do modelo.

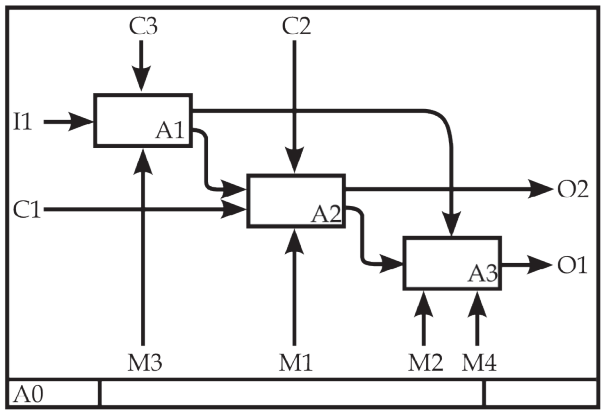


Figura 5.4 Ligação entre setas e caixas

O modelo IDEFØ é composto por sete tipos de setas: entrada, saída, mecanismo, controle, chamada, encapsulada e limite.

Cada uma das setas é rotulada para possibilitar sua identificação. A rotulação representa uma denominação da seta, que segue a seguinte sintaxe:

- Os segmentos de setas, com exceção de setas de chamada, são rotuladas com um substantivo ou frase substantiva, a menos que um único rótulo identifique claramente a seta (os vários segmentos) em sua totalidade.
- As setas de chamada devem conter o rótulo do diagrama em que a função é detalhada.
- Um "ziguezague" é usado para unir uma seta, com seu rótulo, associada, a menos que a relação de flecha/rótulo seja óbvia.
- Os rótulos das setas não devem possuir os seguintes termos: função, entrada, controle, saída, mecanismo ou chamada.

Setas de entrada

As setas de entrada apresentam as entradas necessárias para o desenvolvimento da função especificada na caixa, tais como insumos, matérias primas, documentos, dentre outros. As setas de entrada são observadas na Figura 5.2. Setas de entrada se conectam no lado esquerdo de uma caixa.

Setas de saída

As setas de saída representam os dados ou objetos que foram produzidos por uma determinada função especificada na caixa, como,

por exemplo, eixos usinados, produtos acabados, entre outros. Na Figura 5.2 é observado um exemplo de representação de setas de saída. As setas de saída conectam-se no lado direito da caixa.

Setas de controle

Setas de controle definem as condições requeridas para a produção das saídas adequadas, como, por exemplo, procedimentos ou normas especificados pela empresa, informações sobre os produtos de um determinado fornecedor etc.

Informações ou objetos definidos como controles são transformados pelas funções definidas nas caixas, criando saídas. Um exemplo de seta de controle é observado na Figura 5.2.

Setas de controle conectam-se no lado de cima de uma caixa.

Setas de mecanismo

Setas de mecanismo definem os meios ou ferramentas pelos quais será exercida a função especificada pela caixa, tais como máquinas, *software* ou até mesmo pessoas. Tais setas (menos setas de chamada) devem apontar para cima e se conectar no lado de baixo da caixa. Sua representação é observada no exemplo da Figura 5.2.

Setas de chamada

Seta de chamada é um tipo especial de setas de mecanismo. Com esse tipo, pode-se partilhar detalhes sobre determinado mecanismo entre diferentes modelos (fazendo uma conexão entre si) ou dentro de um mesmo modelo. Tais elementos se conectam embaixo da caixa e apontam para baixo. São rotuladas com a expressão de referência (título do modelo e número de identificação da caixa) do diagrama que detalha a função apresentada na caixa.

Setas encapsuladas

Setas encapsuladas são setas especiais (por serem especialmente denotadas) de um diagrama, que não necessitam serem relacionadas em diagramas de níveis superiores ou inferiores. São informações que, apesar de presentes em um determinado nível do diagrama, não são cruciais a ponto de serem mencionadas em diagramas de nível superior ou precisarem de detalhamento em níveis inferiores. Qualquer tipo de seta pode ser encapsulada, desde setas de entrada até setas de saída, respeitando a direção e o sentido do tipo de seta que estará

representando, diferindo delas apenas no tipo de notação, na qual se inclui um par de parênteses na extremidade referente ao diagrama que a seta não será representada – conforme ilustrado na Figura 5.5.

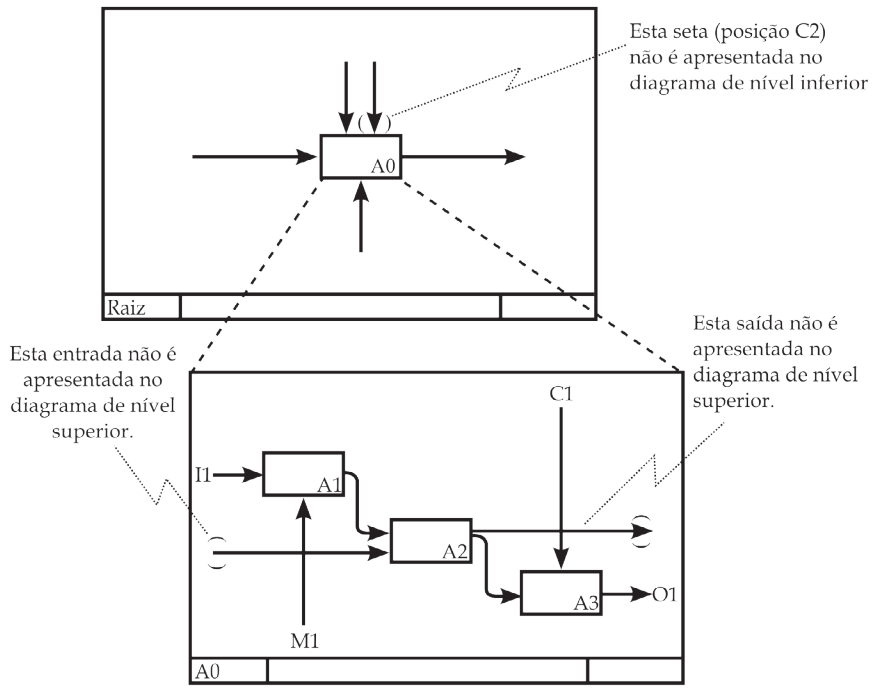


Figura 5.5 Exemplo de setas encapsuladas

Setas limite

São setas com uma das extremidades desconectada de qualquer caixa. Toda seta de limite em um diagrama representa entradas, controles, saídas e/ou mecanismos da caixa de nível superior do diagrama (com exceção de setas encapsuladas).

As setas limites recebem, além do rótulo, um código ICOM. Os códigos ICOM relacionam setas limites presentes em diagramas de nível inferior com as setas em um diagrama de nível superior, especificando as relações que conectam tais itens. As letras I, C, O ou M são escritas junto à extremidade livre de uma seta limite em um diagrama de nível inferior, especificando um tipo de seta como Entrada (I – *input*), Controle (C – *control*), Saída (O – *output*) ou Mecanismo (M – *mechanism*), presentes no diagrama de nível superior e acompanhada de um número, representando a posição relativa que

a seta ocupa no diagrama de nível superior, numeradas da esquerda para a direita ou de cima para baixo. Por exemplo, "C3", escrito em uma seta limite em um diagrama de nível inferior, indica que a seta corresponde à terceira seta de controle (a partir da esquerda) entrando no diagrama de nível superior. Vide Figura 5.6.

Essa codificação relaciona cada diagrama de nível superior à sua caixa superior imediata. Se caixas de um diagrama de nível inferior forem detalhadas em diagramas subsequentes, novos códigos ICOM são designados em cada diagrama de nível inferior, relacionando as setas limites daquele diagrama com as setas do diagrama de nível superior imediato.

Ao utilizar essas relações, as funções das setas (entrada, saída, controle, mecanismo) podem diferir de um diagrama de nível superior para um diagrama de nível inferior, isto é, uma seta de controle no diagrama de nível superior pode representar uma seta de entrada no diagrama de nível inferior.

Deve-se lembrar que as setas encapsuladas em um diagrama de nível inferior não necessitam ser representados no seu diagrama de nível superior, de acordo com a sua definição.

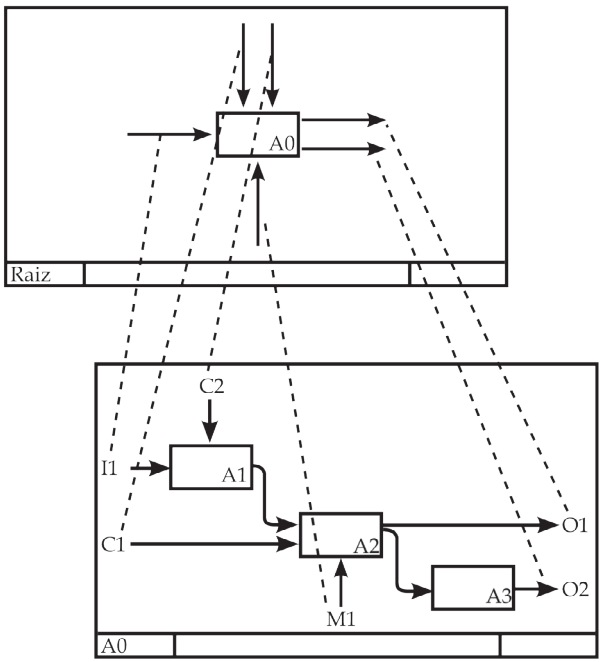


Figura 5.6 Exemplo de código ICOM de setas limites

5.1.3 TIPOS DE DIAGRAMAS

Modelos IDEFØ são compostos de três tipos de informações interrelacionadas: diagramas gráficos, textos e glossário. O diagrama gráfico representa a principal parte de um diagrama IDEFØ, contendo as caixas, setas e as respectivas conexões entre ambas. As caixas representam as principais funções de um determinado assunto, sendo essas funções subdivididas ou decompostas em diagramas mais detalhados, até que o assunto seja descrito em um nível necessário para a sua total compreensão. O diagrama de maior nível no modelo fornece as informações mais generalizadas ou descrições mais abstratas do assunto representado, sendo que esse diagrama é seguido de diversos diagramas mais detalhados sobre o assunto (diagramas de nível inferior).

Diagrama de origem

Todo modelo deve conter um diagrama de nível máximo, onde o assunto a ser tratado é representado em apenas uma caixa (função), sendo denominado diagrama A0. Como a função é descrita apenas com uma caixa, a nomenclatura é muito generalizada, assim como as funções representadas pelas setas, indicando também o ponto de vista sob o qual o modelo foi analisado.

Diagramas de nível inferior

A função única descrita no diagrama de nível máximo é decomposta em suas principais subfunções criando-se um diagrama de nível inferior e, por sua vez, cada uma das subfunções é também decomposta sucessivamente até o nível de detalhamento desejado. O diagrama de nível inferior que resulta da decomposição de uma função representa o mesmo escopo da caixa superior detalhada.

Diagrama de nível superior

Um diagrama de nível superior é aquele que contém uma ou mais caixas superiores. Todo diagrama comum (sem contexto) é também um diagrama de nível inferior, pois, por definição, detalha uma caixa superior. Assim, um diagrama pode ser um diagrama de nível superior (contendo caixas superiores) e um diagrama de nível inferior (detalhando a sua caixa superior), da mesma ma-

neira que uma caixa pode ser uma caixa superior (detalhada por uma caixa inferior) e uma caixa inferior (sendo decomposta em um diagrama de nível inferior). Os níveis dos diagramas estão exemplificados na Figura 5.1.

O fato de a caixa inferior ter sido detalhada, e também ser uma caixa superior, é indicado pela presença de uma expressão de referência de detalhe (*detail reference expression* – DRE). A DRE é um curto código escrito sob o canto direito da caixa detalhada (caixa-mãe), que direciona para o seu diagrama de nível inferior.

Texto e glossário

Os diagramas podem estar associados com textos estruturados, que consistem em um resumo geral do diagrama. Os textos são usados para destacar características, fluxos, conexões entre caixas para esclarecer os objetivos dos itens e padrões cuja significância deve ser considerada. Os textos não devem ser usados para descrever, de maneira redundante, os significados das caixas e setas. O glossário é usado para definir acrônimos, palavras-chave e frases que foram usadas em conjunto com os diagramas gráficos. O glossário define palavras usadas no modelo, permitindo a interpretação correta do conteúdo do modelo.

Diagramas apenas para exposição

Esses diagramas são usados quando um nível adicional contendo conhecimento extra é necessário para o entendimento de áreas específicas de um modelo. O detalhamento extra deve estar limitado às informações necessárias para viabilizar um bom entendimento por parte dos usuários do modelo. Tais diagramas não precisam cumprir as regras de sintaxe aplicadas no IDEFØ.

5.2 MÉTODO DE APLICAÇÃO DA IDEFØ

Assim como as outras técnicas, não existe um método único para se aplicar a técnica IDEFØ, no entanto, de maneira geral, pode-se listar uma série de ações para orientar o processo de modelagem utilizando esta técnica, conforme apresentado a seguir:

1) Definir a função global a ser modelada de forma mais precisa e clara do que o nome da função. Isto é feito por meio de uma lista de informações e dos elementos que atuam ou que são processados pela função.
2) Fazer o desdobramento da função global até a resolução desejada (fazer este desdobramento em uma estrutura em árvore ou mesmo utilizando WBS (*work breakdown structure*) ou *master logic diagram*. Alguns *software* disponibilizam uma visualização na forma de árvore que facilita esta modelagem. É importante lembrar-se da recomendação de modelar três até seis funções (ou caixas) por diagrama, ou nível de desdobramento.
3) Procurar relações naturais entre as subfunções listadas e dividir ou agrupar estas subfunções para que as caixas sejam adequadas.
4) Verificar a existência de funções comuns que podem ser modeladas em diagramas separados para simplificar o modelo final.
5) Para cada nível de desdobramento, elaborar um diagrama incluindo as setas de entradas, saídas, mecanismos e controles. Desenhar o diagrama com atenção especial à disposição das caixas e setas para que se tenha a maior clareza possível. Esta modelagem deve ocorrer do nível superior para o inferior. Note-se que, com exceção do diagrama A0, ao iniciar a modelagem do diagrama, já existe uma série de setas identificadas no diagrama de nível superior. Caso não sejam utilizadas no diagrama a ser modelado, deve-se indicá-las como setas encapsuladas.
6) Incluir as setas de chamada, como as utilizadas para referenciar as funções identificadas no Passo 2.
7) Revisar e refinar o modelo. É usual que durante a modelagem (ou ao final dela) se verifica a necessidade de se desdobrar mais algumas determinadas funções ou que outras não precisariam ser tão detalhadas.
8) Detalhar a descrição de cada elemento da IDEFØ e elaborar o glossário.
9) No caso da modelagem ser de um processo já existente, pode-se, adicionalmente, verificar a compatibilidade do modelo idealizado com a realidade, por exemplo, verificando se realmente existem todos os mecanismos e controles identificados como necessários e se não existem outros que não contribuem significativamente com o desempenho da função.

Note-se que, dependendo da utilização do modelo, será necessário um maior ou menor detalhamento, como, por exemplo, detalhar mais um modelo que será utilizado para capacitação que um modelo utilizado para melhoramento de um processo.

5.3 CONSIDERAÇÕES FINAIS

Um aspecto importante no uso da técnica IDEFØ é estar consciente da função qualitativa da análise. O IDEFØ tem o objetivo de mapear o processo e representar na forma gráfica, a maioria das variáveis significativas do processo em análise. Uma vez que o processo foi racionalizado em diagramas de IDEFØ, os mesmos servem como ferramenta de planejamento e de capacitação de pessoas sobre o processo; sobre as ações a serem desenvolvidas; sobre as redundâncias existentes ou a serem construídas e sobre as compensações requeridas, tanto para clarear as funções dentro do processo, quanto para reorganizar alguns mecanismos que atuam nas funções ou para sistematizar os controles para domínio da função.

O fato da técnica ser recomendada para análise qualitativa, pode ser confundida como falta de objetividade, dado a quantidade de desdobramentos possíveis, que por vezes dificulta a justificativa para mudanças substanciais dentro da operação de uma organização. Ressalta-se que esta é a grande vantagem da técnica, promover a racionalização de processos. Em outras palavras, racionalizar o conhecimento de especialistas numa perspectiva gerencial de processo. Pensando dessa forma, a técnica permite fazer uma fotografia do processo de análise, cujo resultado depende dos atores que participaram do processo e do momento de sua execução. Mudado o processo ou mudado os atores, os modelos podem se tornar ultrapassados. Contudo, ficou registrado um aprendizado com certezas a serem mantidas e erros a serem mitigados. Há que se tomar cuidado, pois se mantendo o foco no fluxo de material e na documentação, pode-se simplificar o resultado do planejamento das ações, dado que as influências culturais, sociais e técnicas do processo são variáveis consistentes sobre os resultados.

Assim, é fundamental que se represente o processo com coerência e de tal forma que a comunicação seja facilitada. De fato, um dos problemas da técnica IDEFØ é que muitas vezes os modelos

são tão concisos que apenas um especialista conseguiria entendê-los (uma alternativa a ser adotada para minimizar este problema é a elaboração de um glossário).

Por outro lado, uma vantagem de se adotar a técnica IDEFØ é que o modelo pode ser refinado à medida que se deseja, tanto pelo desdobramento das caixas (em subfunções) quanto pelo detalhamento das setas. Adicionalmente, pode-se aprimorar as informações associadas a cada elemento do diagrama, detalhando o glossário.

Por fim, destaca-se que, devido às regras existentes para o uso da técnica, é possível a implementação de ferramentas computacionais para auxiliar na modelagem, o que é muito conveniente para modelagem de sistemas complexos.

Capítulo 6

ANÁLISE FUNCIONAL DE PRODUTOS

A análise funcional de produtos é um conjunto de atividades realizadas com intuito de obter conhecimento a respeito do sistema em estudo. Ao final de uma análise é possível ter a estrutura de funções do sistema para acompanhar o fluxo de energia, material e sinal. É uma técnica bastante utilizada para o desenvolvimento de produtos, mas também tem outros objetivos. No contexto da análise de risco, o objetivo de bem caracterizar a função está vinculada ao estudo dos perigos inerentes a todas as funções. Com os perigos identificados é possivel, pelo uso da corrente causal, (Figura 3.3) estimar o potencial de se tornarem incidentes. É a partir daí que se definem as barreiras para diminuir ou até inibir a probabilidade do incidente ocorrer.

Para obter informações para a análise consulta-se catálogos e manuais, normas técnicas e leis, entrevistas com operadores, projetistas e usuários, desmontagem de equipamentos, ensaios experimentais nos equipamentos etc. Consequentemente, demanda-se um certo tempo para a obtenção e a sistematização das informações, que dependerão da disponibilidade das mesmas e da complexidade do sistema. Por outro lado, quanto maior for o detalhamento e a organização das informações obtidas, menor será o tempo requerido para a análise de falhas.

Para melhor orientar o leitor sobre a aplicação da técnica, inicia-se a descrição pela apresentação da estrutura de funções.

6.1 ESTRUTURA DE FUNÇÕES

A presente seção descreve, de forma resumida, as tarefas realizadas na análise funcional, quais sejam: descrição geral do sistema, desdobramento em subsistemas/componentes e identificação das funções.

A estrutura de funções representada na forma de diagrama na Figura 6.1 é uma sistemática importante para análise de falhas e de confiabilidade de sistemas. Ela permite verificar o relacionamento entre funções, componentes, subsistemas e ambiente. Esse tipo de representação gráfica facilita a compreensão do sistema e auxilia o desenvolvimento da análise funcional. É também utilizada para o desenvolvimento de produtos.

Uma das maneiras para se obter a estrutura é partir do desdobramento da função global. Esta é denominada de função principal do sistema, ou, em alguns casos, é uma função específica que se deseja decompor em funções mais simples, denominadas de parciais e elementares. Num processo de análise funcional, a função global é aquela a partir da qual desdobra-se funções parciais e elementares.

A Figura 6.1 ilustra o processo de desdobramento, no qual é possível acompanhar o fluxo de energia, material e sinal; e, assim, verificar o relacionamento entre os componentes e subsistemas que irão compor a função global.

Quando a estrutura de funções é desenvolvida para um novo produto, ou seja, um projeto de inovação, o processo de desdobramento é denominado síntese funcional. Esta atividade é um processo de criação onde são levantadas as funções que devem existir para atender a função global. Posteriormente, se relaciona e organiza as funções levantadas para montar a estrutura de funções.

Porém, se o produto já existe, as funções dos componentes e subsistemas estão previamente definidas. O processo de desenvolvimento da estrutura de funções para esse caso é denominado de análise funcional, sendo amplamente utilizada pela engenharia reversa.

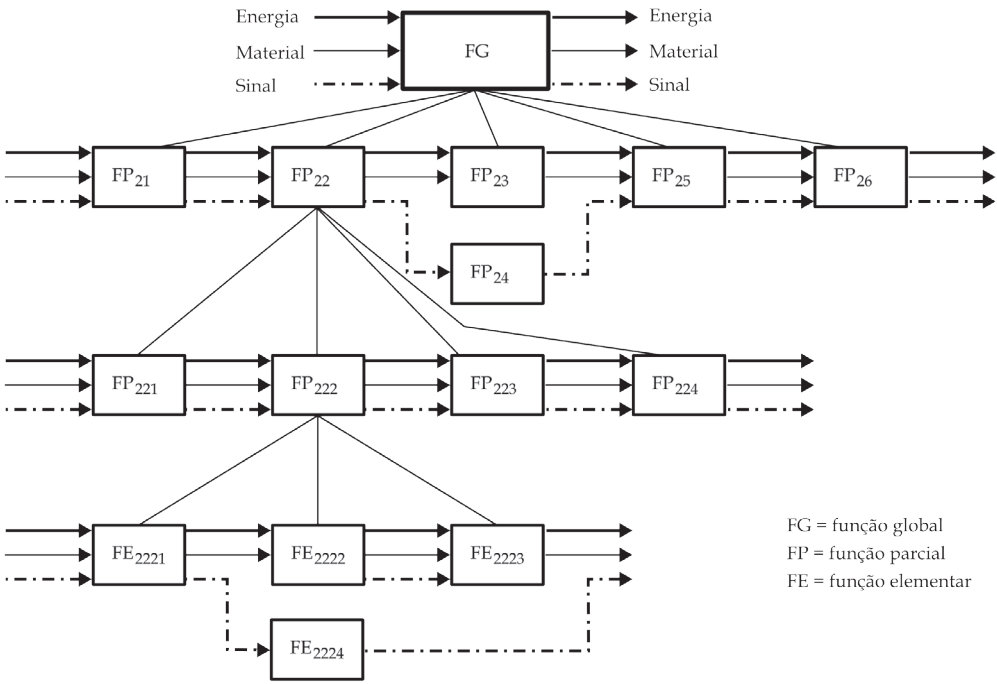


Figura 6.1 Desdobramento da função global (BACK et al., 2008)

Existem alguns recursos e técnicas utilizadas para auxiliar no desenvolvimento da estrutura de funções, a saber:

- Analogia com sistemas semelhantes;
- Tempestade de ideias (*Brainstorming*);
- Técnica de análise das funções do sistema – FAST (*functional analysis system technique*);
- Desmontagem sistematizada do sistema técnico (*teardown*);
- Procedimento de retirar e operar – Método SOP (*subtract and operate procedure*);
- Análise funcional IDEFØ (*Integration definition for function modeling*);
- Rede canal-agência; entre outras.

A representação da estrutura de funções é bastante variada. Pode ser representada como na Figura 6.1, ou usar a estrutura de um IDEFØ, ou, simplesmente, blocos interligados por setas simples. A forma de representar e o nível de resolução das funções dependerão do problema a ser analisado.

O desdobramento da função global parte de uma visão geral do sistema para detalhes mais específicos, até atingir as funções relacionadas com os componentes elementares do sistema. Assim, desdobramento da função global e decomposição do sistema em subsistemas/componentes são atividades muito próximas. Dessa forma, é também usada na técnica de desmontagem sistematizada de sistemas técnicos, ou seja, produtos conhecida como *teardown*. Essa técnica é muito aderente ao desdobramento da função global e pode ser utilizada para o desenvolvimento de estrutura de funções de produtos.

No projeto MitiSF_6 foram utilizadas as seguintes técnicas: *brainstorming*, desmontagem técnica do sistema técnico e o IDEFØ. A primeira, para organizar as discussões entre os membros das equipes e também entre as equipes quando da tomada de decisões em relação aos estudos realizados e na programação das ações a serem feitas. A segunda foi utilizada para estudo do disjuntor, enquanto um sistema técnico, cujo objetivo foi definir cada parte do disjuntor para melhor caracterizar a função e levantar os principais modos de falha. A IDEFØ serviu para compreender todo o processo do gás SF_6 dentro da empresa, desde a aquisição até a armazenagem, uso, purificação, reuso e descarte.

6.2 ANÁLISE DO SISTEMA

6.2.1 DESCRIÇÃO GERAL DO SISTEMA

A análise funcional é iniciada com uma descrição geral do sistema, onde é delimitado o escopo da análise, o ambiente e a interação com outros sistemas. A função global, apresentada na Figura 6.1, fica associada com esse nível da análise.

Posteriormente, é realizada a identificação e descrição dos subsistemas e componentes, bem como suas funções.

6.2.2 DESDOBRAMENTO EM SUBSISTEMAS E COMPONENTES

O nível de detalhamento da discretização varia de acordo com a complexidade dos sistemas. Nessa atividade verifica-se a existência de estruturas similares, que podem ser tratadas como um subsistema/componente único. Por outro lado, identificam-se também subsiste-

mas complexos, com várias funções agregadas, que são divididos em subsistemas menores e mais simples.

A Figura 6.2 apresenta o desdobramento do sistema em subsistemas e componentes.

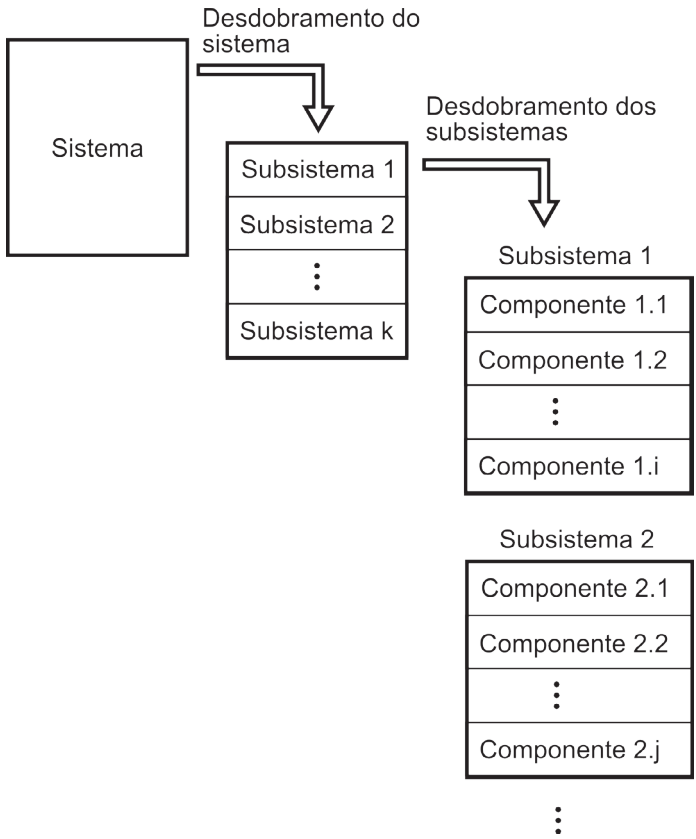


Figura 6.2 Desdobramento do sistema em subsistemas e componentes

O desdobramento deve parar quando se atinge um nível aceitável, onde um detalhamento maior não traz benefícios significativos. Claro que a granulometria do desdobramento depende do problema estudado.

6.2.3 IDENTIFICAÇÃO DAS FUNÇÕES

A identificação das funções de cada um dos subsistemas e componentes é uma tarefa que pode ser realizada depois da definição

dos subsistemas/componentes, ou pode ocorrer concomitantemente, enquanto o desdobramento está sendo desenvolvido.

Além de documentos como catálogos, manuais, dados de manutenção, deve-se acompanhar os processos como o de operação, montagem e manutenção do sistema, onde é possível obter fotos e informações com os técnicos ou colaboradores.

O Quadro 6.1 apresenta as funções associadas a cada um dos desdobramentos. Assim, a função global é associada ao sistema, a parcial aos subsistemas e a elementar aos componentes.

Quadro 6.1 Identificação das funções

Sistema: função global
Subsistema 1: função parcial 1
Componente 1.1: função elementar 1.1
Componente 1.2: função elementar 1.2
Componente 1.3: função elementar 1.3
...
Componente 1.i: função elementar 1.i
Subsistema 2: função parcial 2
Componente 2.1: função elementar 2.1
Componente 2.2: função elementar 2.2
Componente 2.3: função elementar 2.3
...
Componente 2.j: função elementar 2.j
Subsistema k: função parcial k
Componente k.1: função elementar k.1
Componente k.2: função elementar k.2
Componente k.3: função elementar k.3
...
Componente k.m: função elementar k.m

Com as funções bem definidas, tem-se um bom entendimento do funcionamento do sistema – o que permite o início da análise de falhas onde as partes mais críticas do sistema serão identificadas. Esta técnica, embora seja de simples aplicação, traz muitos benefícios, principalmente relacionados à uniformização na comunicação. Se a função ficar bem definida, torna-se mais fácil o processo de capacitação dos colaboradores, principalmente, para a operação e manutenção. No estudo de risco, a comunicação é importante, porque no momento crítico do incidente a linguagem precisa estar muito bem unificada para que todos compreendam as decisões tomadas e exerçam as ações definidas nos processos de capacitação, sem dupla interpretação.

6.3 EXEMPLO

O Quadro 6.2 exemplifica uma análise funcional, cujo objeto da análise (Sistema) é uma Subestação (SE), que pode ser definida como um conjunto de instalações elétricas em média ou alta tensão, cuja função é agrupar os equipamentos, condutores e acessórios destinados à proteção, medição, manobra e transformação de grandezas elétricas. No exemplo o foco da análise é a manutenção, e o objetivo é determinar os elementos que devem ser substituídos durante uma intervenção de manutenção devido a uma falha.

Para cumprir com a sua função, o Sistema SE é composto por Subsistemas com funções específicas, denominados vãos (em inglês *bays*) que permitem a decomposição da SE em módulos. São exemplos de vãos: Entrada de Linha (EL); Saída de Linha (SL); Transformação (TR); e Transferência (TF), entre outros.

O Subsistema Vão de Transferência (TF) é composto pelos Subsistemas Seccionadora (SEC) e Disjuntor (DJ), dentre outros equipamentos.

O Subsistema Disjuntor (DJ) é composto, por sua vez, nos elementos: Unidade de Comando (UC); Unidade de Acionamento (UA); Coluna de Isolação/Suporte(IS); Cárter (CT); Resistores de Pré-Inserção (R); Capacitores de Equalização (C) e Câmaras de Extinção (CE).

O Subsistema Câmara de Extinção (CE) é composto nos elementos: Isolador (I); Contato Móvel (CM) e Contato Fixo (CF).

O subsistema contato fixo (CF) possui os seguintes elementos: Cesto de alumina ativada; Suporte do contato fixo; Pinças do contato fixo; Contato fixo de arco, entre outros.

Em relação ao Sistema SE, objeto da análise, os vãos podem ser entendidos como Subsistemas (Nível 1), por exemplo o vão TF. Os equipamentos que compõem os vãos são entendidos como Subsistemas (Nível 2), por exemplo, o DJ pertencente ao vão TF. Os subsistemas dos equipamentos que compõem os vãos são entendidos como o Subsistemas (Nível 3), por exemplo, a CE pertencente ao DJ. Os subsistemas do nível hierárquico imediatamente inferior da CE são entendidos como Subsistemas (Nível 4) pertencentes ao Sistema SE, por exemplo, o CF pertencente a CE. A subdivisão de um sistema em subsistemas, para fins de manutenção, deve terminar nos componentes.

Os componentes são os elementos de menor mantenabilidade do sistema objeto da análise, ou seja, são aqueles que, se falharem, são substituídos em uma tarefa de manutenção. No exemplo, são componentes do CF: cesto de alumina ativada; suporte do contato fixo; pinças do contato fixo e contato fixo de arco, entre outros. Os componentes poderiam, ainda, serem subdivididos em elementos de menor nível hierárquico, menor granulometria. Porém, tal rigor só dificulta a análise, tirando o foco do objetivo principal, no caso do exemplo, visa identificar que itens serão substituídos durante uma ação de manutenção. Caso o objetivo da análise seja, por exemplo, a reengenharia de uma produto/componente, a subdivisão poderá ser exigida com maior detalhamento.

Observa-se no Quadro 6.2 que a função é explicitada por um verbo no infinitivo e, por vezes, vem acompanhado de um substantivo. O uso do verbo ocorre porque o mesmo explicita uma ação que a função deve cumprir. Se ocorrer uma não função, ou seja, a função não ocorrer, aí então se tem uma falha. A análise da falha pode seguir diferentes caminhos, por exemplo: da operação, da manutenção, da comunicação e também do risco que pode decorrer pela não função.

Quadro 6.2 Identificação das funções de uma Subestação

Subestação: conjunto de instalações elétricas cuja função é agrupar os equipamentos, condutores e acessórios, destinados à proteger, medir, manobrar e transformar grandezas elétricas.					
	Vão de Entrada de Linha (EL): agrupar os equipamentos de Entrada de Linha da subestação.				
		Subsistemas (EL) – Nível 2	Subsistemas (EL) – Nível 3	Subsistemas (EL) – Nível 4	Componentes (EL)
	Vão de Saída de Linha (SL): agrupar os equipamentos de Saída de Linha da subestação.				
		Subsistemas (SL) – Nível 2	Subsistemas (SL) – Nível 3	Subsistemas (SL) – Nível 4	Componentes (SL)
	Vão de Transformação: adequar dos níveis de tensão e proteger do transformador.				
		Subsistemas (TR) – Nível 2	Subsistemas (TR) – Nível 3	Subsistemas (TR) – Nível 4	Componentes (TR)
	Vão de Transferência (TF): transferir a carga do barramento principal para o barramento de transferência.				
		Chaves Seccionadoras (SEC): isolar o circuito.			
			Subsistemas (SEC) – Nível 3	Subsistemas (SEC) – Nível 4	Componentes (SEC)
		Disjuntor (DJ): estabelecer, conduzir e interromper correntes nas condições normais do circuito, assim como estabelecer, conduzir durante um tempo especificado e interromper correntes sob condições anormais especificadas do circuito, tais como as de curto circuito.			
			Unidade de Comando (UC): comandar, controlar e supervisionar o disjuntor.		
				Subsistemas (UC) – Nível 4	Componentes (UC)
			Unidade de Acionamento (UA): armazenar a energia necessária a operação mecânica do disjuntor, bem como liberar esta energia pela ação de mecanismos apropriados, quando do comando de abertura ou fechamento do disjuntor.		
				Subsistemas (UA) – Nível 4	Componentes (UA)
			Coluna de Isolação/Suporte (IS): transmitir o movimento da Unidade de Acionamento para o cárter; conter o SF_6; isolar a câmara de extinção, no caso de disjuntores de tanque vivo; suportar a estrutura, composta pela câmara de extinção, resistor, capacitor e cárter.		
				Subsistemas (IS) – Nível 4	Componentes (IS)
			Cárter (CT): transferir o movimento proveniente da haste de manobra para as câmaras de extinção e resistores de pré-inserção.		
				Subsistemas (CT) – Nível 4	Componentes (CT)

			Resistores de Pré-Inserção (R): equalizar as tensões nas câmaras de extinção; reduzir as sobre tensões devidas à abertura de cargas indutivas; reduzir a taxa de crescimento e o pico da TTR (Tensão Transitória de Restabelecimento) em faltas terminais e quilométricas; reduzir a TTR durante a abertura de correntes capacitivas; limitar a corrente durante o fechamento de cargas capacitivas; reduzir as sobre tensões que ocorrem durante o fechamento de linhas longas.		
				Subsistemas (R) – Nível 4	Componentes (R)
			Capacitores de Equalização (C): garantir que durante o processo de abertura e com o disjuntor aberto, a tensão sobre as câmaras de extinção seja a mais uniforme possível		
				Subsistemas (C) – Nível 4	Componentes (C)
			Câmara de Extinção (CE): conter o SF_6; confinar o arco elétrico; favorecer a sua extinção; resistir às solicitações térmicas e mecânicas do processo de extinção; e, suportar estruturalmente os terminais, os contratos principais e seus mecanismos de atuação.		
				Isolador (I): conter o SF_6, em uma faixa pré-fixada de pressão, estando e disjuntor Aberto ou Fechado, mantendo os níveis de pureza normatizados; conter o SF_6 durante o transitório de Abertura ou Fechamento do disjuntor, mantendo os níveis de pureza normatizados.	
					Componente do Isolador
				Contato Móvel (CM): conduzir a corrente transitória de separação dos contatos, com erosão limitada para manter os níveis de pureza normatizados; suportar a alta temperatura do arco, com erosão limitada para manter os níveis de pureza normatizados.	
					Componentes do Contato Móvel
				Contato Fixo (CF): conter SF_6, dentro dos níveis de pureza normatizados; pressurizar o SF_6, dentro dos níveis de pureza normatizados.	
					Cesto de alumina ativada: conter alumina ativada (Al_2O_3).
					Suporte do Contato Fixo: suportar o contato fixo e não reagir quimicamente com o FS_6.
					Pinças do contato fixo: Estabelecer conexão elétrica com o contato móvel e não reagir quimicamente com o SF_6.
					Contato fixo de arco: conduzir a corrente transitória de separação dos contatos; suportar a alta temperatura do arco; não reagir quimicamente com o SF_6.
					Outros componentes do Contato Fixo.
Sistema Objeto	**Subsistema Nível 1**	**Subsistema Nível 2**	**Subsistema Nível 3**	**Subsistema Nível 4**	**Componentes do Subsistema Nível 4 menor Mantenabilidade**

6.4 CONSIDERAÇÕES FINAIS

A análise funcional é uma tarefa que se desenvolve iterativamente, isto é, à medida que as informações vão sendo obtidas faz-se o desdobramento das funções. É iterativo porque a compreensão da estrutura de funções requer certo aprendizado e por isso é requerido a atualização no documento. A partir do desdobramento das funções tem início a análise de falhas, onde se busca identificar como os componentes podem deixar de cumprir as funções.

Durante o desenvolvimento da análise de falhas ainda é possível ter que retornar à análise funcional para investigar algumas informações que necessitam de maiores detalhes. Assim, dependendo da quantidade de componentes, estados de operação, complexidade do sistema, entre outras variáveis, a atividade de análise funcional demanda bastante tempo.

A técnica da análise funcional é mais apropriada para sistemas técnicos. O importante da análise funcional é a abordagem segundo as entradas e saídas, na forma de energia, material ou sinal. Por exemplo, para o caso do MitiSF_6, do ponto de vista da atmosfera, a função do disjuntor é conter o gás. Então, há uma entrada de material no disjuntor, na forma de gás SF_6 que tem a função dielétrica quando o disjuntor é acionado. A saída do material – de gás SF_6 – deve ser zero. Se assim não for, o disjuntor não cumpre a função de conter o gás. Assim, na atividade de análise funcional deve-se desdobrar todos os itens que fazem parte da função – conter gás – para demandar ações corretivas para eliminar a falha, ou interpor barreiras que possam não deixar o gás atingir o ambiente. Assim, no desdobramento da análise define-se a função principal e secundária (quando houver) de todos os itens que participam da função que está sendo analisada.

Como visto no capítulo 5, a técnica IDEFØ é mais aderente a análise dos processos, dado que promove uma boa comunicação entre os vários agentes de um ou mais processos. Em relação a análise de risco de vazamento de gás no processo, da mesma forma que a na análise funcional do disjuntor, poderia ser imaginado que existe um volume de controle sobre todo o processo, onde o gás deve estar contido. Assim sendo, nenhum gás deve sair desse volume. Todo o gás contido na empresa é para cumprir a função que ele desenvolve dentro do disjuntor ou em outro sistema técnico. Quando de manu-

tenção, ou diante de outra necessidade, o gás tiver de ser retirado do sistema técnico, admite-se que o mesmo seja armazenamento em cilindros, máquinas de purificação etc., sem perdas. Como visto no capítulo 5.2 a técnica IDEFØ é apropriada para identificar os pontos de falha que podem proporcionar perda de gás durante processos de manipulação para fora do volume de controle, no contexto da empresa ou das empresas. Dessa forma, todo o gás que sair desse volume é admitido que vá para a atmosfera.

Assim, a técnica de análise funcional objetivou identificar as funções para mitigar a perda do gás do sistema técnico para a atmosfera, e a técnica IDEFØ visa fazer o mesmo em relação ao processo de manipulação do gás.

Capítulo 7

ANÁLISE DOS MODOS DE FALHA E EFEITOS (FMEA)

FMEA (*failure mode and effects analysis*) é uma técnica utilizada para análise de falhas cujo objetivo é desenvolver conhecimento para orientar as ações visando a eliminação das causas dos modos de falha. É amplamente utilizada em processos de projeto de componente, sistemas, em serviços e em processos de fabricação. Esta técnica tornou-se muito importante para os atributos de qualidade, mantenabilidade e confiabilidade do produto e também está presente nos processos de análise de risco.

A técnica foi desenvolvida no departamento de defesa dos Estados Unidos e foi formalizada no procedimento militar MIL-P-1629, publicado originalmente em 9 de novembro de 1949 (MOHR, 1994) e substituído pelo MIL-P-1629A (*Military procedure* MIL-P-1629: *Procedures for performing a failure mode, effects and criticality analysis*), que também foi descontinuada.

Note-se que a MIL-P-1629A designa a técnica como FMECA (*failure mode, effects and criticality analysis*) que, por sua vez, se distingue da FMEA pelo fato de agregar um índice de criticidade que orienta a prioridade nas ações a serem executadas pela organização. No entanto, é comum utilizar o termo FMEA para ambos os casos, sem fazer distinção do uso do índice de criticidade. Assim, neste livro – por conveniência –, será adotado o termo FMEA indistintamente. Isso porque, na grande maioria das análises se considera no processo de análise a criticidade das causas e modos de falha.

7.1 CONSIDERAÇÕES SOBRE A TÉCNICA FMEA

Uma das grandes dificuldades de utilização da FMEA é o entendimento dos conceitos de modo de falha, causa e efeito. Isto

porque dependendo da abordagem e do tipo de FMEA, um mesmo fator pode ser tratado de maneira diferente, como, por exemplo, "fadiga", que pode ser uma causa ou um modo de falha, dependendo do objetivo da análise ou do tipo de FMEA.

Assim, além da clara definição dos elementos da FMEA, é necessário o entendimento dos tipos de FMEA e das abordagens a adotar. Nesta seção, apresenta-se algumas considerações sobre esses aspectos e, adicionalmente, alguns pontos importantes a serem observados na formação da equipe FMEA, dado a importância para a utilização da técnica.

7.1.1 DEFINIÇÕES UTILIZADAS NA TÉCNICA

Quando os conceitos sobre FMEA estão bem estabelecidos pelo grupo, a aplicação da técnica fica bastante simplificada. Uma das atividades mais importantes é a padronização dos termos utilizados.

Destaca-se que a clareza dos conceitos deve ocorrer em dois níveis. O primeiro refere-se ao conhecimento e aceitação da nomenclatura sobre a técnica. O segundo trata do domínio de aplicação da FMEA (i.e., a abordagem adotada) que tem relação direta com o tipo de FMEA. Assim sendo, a nomenclatura ganha um significado específico em função do domínio de aplicação. Para tanto apresenta-se a seguir alguns conceitos relacionados à nomenclatura e ao domínio de aplicação.

Modo de falha

Define-se "modo de falha" como a forma que ocorre a falha, a maneira pela qual ela se apresenta. Ou seja, a maneira do componente sob estudo deixar de executar a sua função ou desobedecer às especificações. O modo de falha é uma propriedade inerente a cada item, visto que cada um tem suas características particulares, como função, ambiente de trabalho, materiais, fabricação e qualidade.

Basicamente, existem duas abordagens para se conduzir uma FMEA: a funcional e a estrutural. A primeira está centrada nas funções do sistema técnico, ou, em outras palavras, no funcionamento do item. Em face disso, a abordagem é normalmente mais abrangente. Pode-se dizer que esta abordagem é, normalmente, mais utilizada

nas fases iniciais do processo de projeto (no projeto conceitual, por exemplo), pois a análise pode ser feita sem que os componentes do sistema técnico estejam totalmente definidos. Outro exemplo de aplicação dessa abordagem está na análise de processo, quando se quer implementar uma gestão de manutenção, como, por exemplo, a gestão de manutenção centrada na produtividade total (TPM – *total productive maintenance*) em um ambiente de fabricação. Nesse caso, o modo de falha pode ser simplesmente uma não função, como está apresentado no Quadro 7.1.

Quadro 7.1 Exemplos de modo de falha com abordagem funcional

Componente	**Função**	**Modo de falha**
Eixo	Transmitir torque	Não transmite torque

Na abordagem estrutural, por sua vez, o modo de falha normalmente está associado a aspectos mais específicos dos componentes, elementos, peças ou partes do sistema sob análise. Normalmente, está associado à resistência mecânica, carregamento ocorrido, tratamento superficial existente, medida de dureza etc. Por exemplo, os modos de falha de um eixo, numa abordagem estrutural, podem ser: ruptura, empenamento, desgaste etc. Já o modo de falha de um filtro de uma unidade hidráulica de potência pode ser ruptura ou entupimento. Para clarear a diferença entre a abordagem funcional e estrutural apresenta-se no Quadro 7.2 alguns modos de falha selecionados na abordagem estrutural para o mesmo eixo analisado anteriormente, no Quadro 7.1.

Assim, quanto mais "profunda" for a análise (quando se trata o item como componente ou parte de um componente, por exemplo), o foco na abordagem estrutural se mostra mais adequado. Por outro lado, para análises sistêmicas recomenda-se optar por uma abordagem funcional.

Destaca-se que tanto para abordagem funcional quanto para a estrutural, é muito importante que se tenha a função do componente bem descrita, pois é a partir dela que se inicia a análise do modo de falha.

Quadro 7.2 Exemplos de modo de falha com abordagem estrutural

Componente	Função	Modo de falha
Eixo	Transmitir torque	Ruptura, empenamento, desgaste, trinca

O Quadro 7.3 ilustra a relação entre a análise estrutural e a funcional. Note-se que a "causa", na abordagem funcional, passa a ser o "modo de falha" na abordagem estrutural.

Quadro 7.3 Relação entre FMEAs aplicadas na análise de anel de vedação em um disjuntor: a) abordagem funcional e b) abordagem estrutural

a) **FMEA funcional**

Item	Função	Modo de falha	Efeito	Causa
Anel de vedação	Vedar	Não veda	• Perda total – caso haja rompimento (explosão) da câmara – ou parcial do SF6. • Redução da pressão interna do SF6. • Abertura de arco elétrico nas partes condutoras internas. • Aumento dos danos causados pelo arco elétrico durante a abertura ou o fechamento do disjuntor. • Trip do disjuntor (com abertura do disjuntor). • Impossibilidade de fechamento do disjuntor. • Danos a pessoas e equipamentos próximos caso haja explosão.	Deformação permanente

b) **FMEA estrutural**

Item	Função	Modo de falha	Efeito	Causa
Anel de vedação	Vedar	Deformação permanente	• Perda total – caso haja rompimento (explosão) da câmara – ou parcial do SF6. • Redução da pressão interna do SF6. • Abertura de arco elétrico nas partes condutoras internas. • Aumento dos danos causados pelo arco elétrico durante a abertura ou o fechamento do disjuntor. • Trip do disjuntor (com abertura do disjuntor). • Impossibilidade de fechamento do disjuntor. • Danos a pessoas e equipamentos próximos caso haja explosão.	Pressão de aperto excessiva Temperatura excessiva Material do anel inadequado Envelhecimento

Na análise de um anel de vedação usado na câmara do disjuntor do Quadro 7.3, segundo a abordagem funcional, tem-se a função – vedar – e o modo de falha – não veda. A causa mais provável é deformação permanente, sendo que o modo de falha gera diversos efeitos, como está apresentado na parte "a" do Quadro 7.3.

Agora, na abordagem estrutural (Figuta 7.1.b) para o mesmo item e mesma função, o modo de falha do anel de vedação é deformação permanente, que, na abordagem anterior, era causa. As prováveis causas desse modo de falha são: pressão de aperto excessiva, temperatura excessiva, material do anel inadequado e envelhecimento. Como já se chamou atenção, o modo de falha na abordagem estrutural tem relação direta com a estrutura do item. Nesse caso, o modo de falha proporcionou uma deformação plástica, ou deformação permanente, cujas causas estão relacionadas com fatos que condicionaram o anel de vedação a uma situação de trabalho que gerou estresse, que provocou alteração em sua estrutura física.

Como se pode identificar o modo de falha numa ou noutra abordagem? Na abordagem funcional, o modo de falha "não veda" pode ser percebido a partir de um ensaio de estanqueidade no disjuntor. Já na abordagem estrutural, o modo de falha tem condições de ser caracterizado a partir de ensaio de deformação elástica do anel de vedação.

Note-se que, independentemente do nível da análise (componente, subsistema etc.), os efeitos devem ser identificados dentro do escopo de análise.

É importante destacar que não existe um consenso quanto à definição dos elementos que compõem a FMEA, particularmente, na denominação de modo de falha e causa. Por exemplo, as normas SAE JA1011 e JA1012 apresentam, respectivamente, critérios de avaliação para processos de Manutenção Centrada em Confiabilidade (RCM) e um guia para as normas de RCM. Essas normas definem "modo de falha" como sendo "um evento único que causa uma falha funcional" (SAE, 1999; SAE 2002a). Em relação à Manutenção Centrada em Confiabilidade destacam que "RCM faz distinção entre falha funcional, estado de falha e modo de falha que é um evento que provoca um estado de falha" (SAE, 2002a). Já a norma SAE J1739 define modo de falha como "a maneira pela qual um componente, um subsistema ou um sistema pode deixar de atender ou fornecer a

função desejada, descrita na coluna item/função (i.e., falha da função desejada)" (SAE, 2002b). Vale dizer ainda que, com freqüência, existe mais de um modo de falha para cada função. Assim, a condição final do estado do item dependerá de qual ou de quais modos de falhas levaram o item à falha.

A definição do que será tratado como modo de falha ou causa também está associado ao nível desejado de desdobramento do sistema. A Figura 7.1 ilustra esta situação. Note-se que um modo de falha identificado na FMEA de um componente passa a ser tratado como uma causa na FMEA de um subsistema, já o que for modo de falha, nesse último, passa a ser causa no FMEA seguinte, e assim por diante.

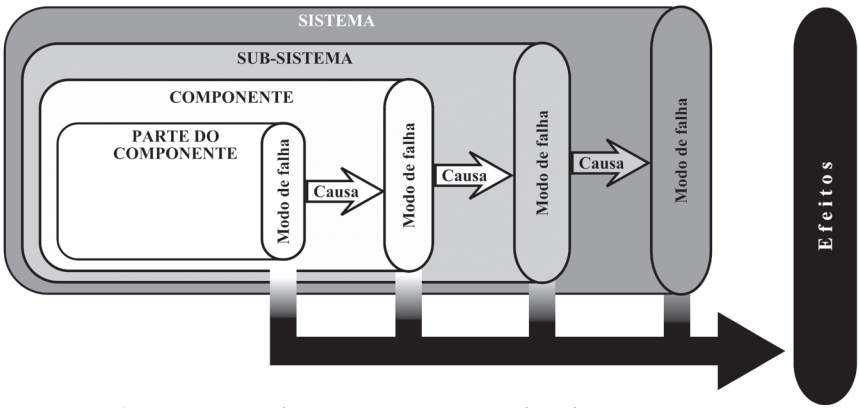


Figura 7.1 Análises sucessivas em abordagem *botton-up*

A Figura 7.2 traz um exemplo para a estrutura apresentada na Figura 7.1, onde a parte de componente que está sendo analisada é um anel de vedação, cuja deformação permanente é um dos modos de falha que pode ocorrer no anel. Dado que esse modo de falha possa ocorrer, surge uma sequência de possíveis eventos que irão atingir os níveis superiores, como descritos a seguir: componente (câmara de extinção), subsistema (disjuntor) e sistema (subestação). Assim, o modo de falha deformação permanente, no anel de vedação, pode causar uma baixa pressão de SF_6 na câmara de extinção, devido a vazamento, pela existência da deformação. Assim, a baixa pressão de SF_6 agora é o modo de falha do componente, cuja causa

é a deformação permanente do anel de vedação. O modo de falha do componente passa ser a causa dos modos de falha na interrupção de corrente elétrica, ou explosão do disjuntor. Finalmente, os modos de falha do subsistema passam a ser a causa dos modos de falha do sistema, sendo que um deles pode ser interrupção do fornecimento de energia elétrica na subestação.

Esse exemplo indica que, dependendo do ponto onde se inicia a análise, uma falha pode ser considerada como causa ou modo de falha. O efeito fica definido no momento em que se estabelece o limite mais externo da análise, onde está o cliente. Maiores detalhes sobre os efeitos estão apresentados na próxima seção.

	Parte de um componente	**Componente**	**Subsistema**	**Sistema**
	Anel de vedação	Câmara de extinção	Disjuntor	Subestação
Modo de falha associado ao item	Deformação permanente	Baixa pressão de SF_6	Falha na interrupção de corrente elétrica Explosão	Falha no fornecimento de energia elétrica

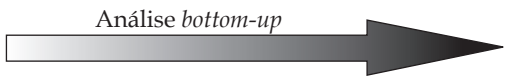


Figura 7.2 Exemplo de uma sequência de análise de falhas a partir do anel de vedação

Note-se que, nas normas de RCM (SAE JA1011 e JA1012), modo de falha é definido como causa, e a falha funcional é definida como a maneira pela qual o item falha. De fato, nestas duas normas, não se faz referência às causas do modo de falha. Nesta ótica, a FMEA consiste em identificar as falhas funcionais e os modos de falha (que são equivalentes aos modos de falha e às causas, no caso do Quadro 7.1). Assim, a orientação das normas SAE JA1011 e JA1012 é para fazer, de fato, uma FMEA funcional. No entanto, designa-se por "falha funcional" e "modo de falha" o que foi, respectivamente, chamado de "modo de falha" e "causas" na SAE J1739 (conforme ilustrado no Quadro 7.4).

Quadro 7.4 Exemplos de modo de falha com abordagem estrutural

Definição	**FMEA funcional pela norma SAE J1739**	**RCM pelas normas SAE JA1011 e JA1012**
Forma como ocorre falha funcional	Modo de falha	Falha funcional
Causa da falha funcional	Causa	Modo de falha

Esta particularidade entre as definições das normas acaba gerando uma considerável confusão durante a implementação de RCM. Assim, é comum a adoção de um FMEA "híbrido", no qual se insere uma nova coluna na tabela FMEA estrutural, entre a definição da função do item e o modo de falha, incluindo um campo denominado de "falha funcional". Chama-se atenção para o leitor tomar cuidado quando da adoção de uma norma. É sempre importante tomar o cuidado de uniformizar a nomenclatura e a taxonomia baseada no consenso, optando por uma norma que sirva de referência para aplicação da análise. Ganha-se tempo, confiança e facilita as revisões que ocorrem com frequência.

Efeitos

De alguma maneira, o modo de falha não pode ser visto de forma isolada dentro de um sistema. É preciso estabelecer uma relação com o efeito, como está apresentado nas Figuras 7.1 e 7.3.

O efeito é a forma ou maneira de como o modo de falha se manifesta para o observador ou como é percebido no âmbito do subsistema ou sistema. Enquanto o modo de falha ocorre internamente no item, o efeito manifesta-se externamente, indicando que existe uma degradação que é percebida do sistema. O observador é qualquer referencial indicador do efeito, baseado em vibração, ruído, temperatura, ou mesmo no conhecimento humano, como, um manutentor ou operador.

Se houver uma boa caracterização do efeito, se faz uso de suas primeiras manifestações, no sentido de tomar as providências para manutenção do item, antes que o modo de falha se desenvolva até a condição que leve à perda total da função do item.

A Figura 7.3 representa esquematicamente um sistema constituído de "n" itens, que precisam atuar para cumprir um conjunto

de funções (note-se que, por existir itens em paralelo, alguns deles podem falhar sem comprometer o funcionamento do sistema). Assim, ao ocorrer uma falha no item k_i tem-se o efeito da falha sobre o sistema. A característica do efeito que se manifesta sobre o sistema depende do modo de falha dominante do item k_i. Em se tratando de um sistema hidráulico, por exemplo, se o item k_i for um filtro e o modo de falha for ruptura da carcaça do filtro, o efeito mais provável no sistema será um vazamento. Contudo, dependendo da configuração, também pode aparecer ruído na bomba devido à cavitação, lentidão no deslocamento de um cilindro ou problemas de precisão de posicionamento. Por outro lado, se o modo de falha do filtro for entupimento, o efeito no sistema poderá ser aumento de temperatura, lentidão do deslocamento do cilindro etc.

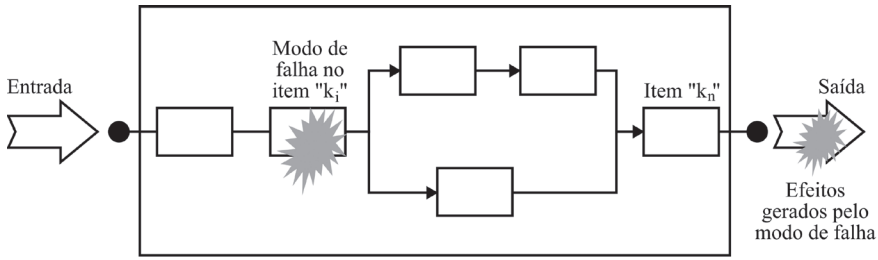


Figura 7.3 Relação entre modo de falha e efeito num sistema

De fato, é necessário estipular um limite para a análise dos efeitos de acordo com o escopo de análise definido. Por exemplo, se o escopo de análise inclui o usuário, levanta-se os efeitos que podem ser percebidos pelo mesmo. Caso o escopo se limite ao sistema técnico, os efeitos analisados serão restritos a este domínio.

Para ilustrar esta situação, suponha uma FMEA de uma bomba do sistema hidráulico de uma prensa. Se o escopo se restringir ao sistema técnico – i.e., a prensa hidráulica –, o efeito da falha da bomba leva ao não funcionamento adequado da mesma, o que provoca a dificuldade de movimentar a prensa hidráulica. Por outro lado, se o escopo incluir o operador, o efeito percebido por este é a incapacidade da prensa conformar a peça. Se o escopo considerar a linha de produção, o efeito será a redução da produtividade (ou até a interrupção da produção) e assim por diante. Dessa forma, destaca-se o quão importante é a definição do escopo de análise antes de se iniciar a FMEA.

Causa

Considerando a abordagem proposta na SAE J1739, todo modo de falha tem uma ou mais causas que potencializam sua ocorrência. As causas podem estar associadas a fatores ambientais, humanos, técnicos advindos do projeto, do processo de fabricação, do uso influenciado por itens da vizinhança ou serem intrínsecas à própria função do componente. Há várias denominações para as causas e diferentes formas de caracterizar sua dimensão ou importância.

O estudo das causas permite aprofundar a relação entre o item e a função. Com isso, é possível gerar procedimentos mais consistentes para eliminar as causas ou mitigar sua influência na geração do modo de falha.

É importante dizer que o levantamento das causas não é feito para todos os modos de falha, pois tal tipo de análise demanda bastante tempo e esforço. Assim, as causas são investigadas para os modos de falha mais relevantes, isto é, de acordo com a proporção de seus efeitos, considerando, por exemplo, a segurança e a continuidade da organização.

O exemplo do quadro 7.5 foi aplicado na análise de falha de um sistema de bombeamento de água, abordado nas normas de RCM, SAE JA1011 e JA1012 (SAE, 2002a). Como já comentado anteriormente, as normas de RCM (SAE JA1011 e JA1012) normalmente chamam de modo de falha, os mesmos eventos que a norma SAE J1739 (SAE 2002b) chama de causa. Neste exemplo, as normas categorizam os modos de falha em sete níveis, que serão chamadas de causas, coerentemente com a SAE J1739. A ideia é distribuir a percepção da causa do nível mais geral para o mais específico, até aproximar-se da causa raiz. No exemplo, os autores optaram por também chamar os eventos mostrados no Quadro 7.5 de causas.

Quadro 7.5 Detalhamentos de diferentes níveis de causas de falha para bombeamento de água segundo uma abordagem de RCM (Adaptado de SAE (2002a) e Moubray (2002))

Nível 1	Nível 2	Nível 3	Nível 4	Nível 5	Nível 6	Nível 7
Falha no sistema de bombeamento	Falha na bomba	Falha no rotor	Rotor à deriva	Porca de fixação solta	Porca com aperto incorreto	Erro de montagem
				Porca de fixação gasta	Porca corroída	
					Porca fabricada com material incorreto	Especificação incorreta do material
						Fornecimento incorreto do material

			Porca do rotor trincada	Excesso de aperto na porca	Erro de montagem
				Porca fabricada com material incorreto	Especificação incorreta do material
					Fornecimento incorreto do material
			Chaveta do rotor cisalhada	Material especificado incorretamente	Erro de projeto
				Material fornecido incorretamente	Erro de aquisição
					Erro de administração do almoxarifado
					Erro do pedido
		Objeto colide com o rotor	Peça no sistema após manutenção	Erro de montagem	Veja "erro humano"
			Corpo estranho no sistema	Filtro de sucção não instalado	Erro de montagem
				Filtro perfurado por corrosão	
	Ruptura da carcaça	Afrouxamento dos parafusos da carcaça	Alojamento dos parafusos com pouco aperto	Erro de montagem	Veja "erro humano"
			Afrouxamento por vibração		
			Corrosão dos parafusos		
			Falha devido a fadiga		
		Falha na junta da carcaça	Junta instalada incorretamente	Erro de montagem	Veja "erro humano"
			Falha na junta devido a fricção		
		Carcaça esmagada	Por um veículo	Erro de operação	Veja "erro humano"
			Por um objeto do céu	Carcaça atingida por um meteorito	
				Carcaça atingida por pedaço de aeronave	
	Falha na vedação da bomba	Desgaste normal	Vedação desgastada		
		Ausência de água no funcionamento	Veja "falha de fornecimento de água" abaixo		
		Vedação desalinhada	Erro de montagem	Veja "erro humano"	
		Sujeira na superfície da vedação	Erro de montagem	Veja "erro humano"	
		Instalação de vedação incorreta	Fornecimento de vedação incorreta	Erro de aquisição	Veja "erro humano"
				Erro de administração do almoxarifado	Veja "erro humano"
			Especificação errada da vedação	Erro de projeto	Veja "erro humano"
		Instalação de vedação danificada	Vedação danificada no armazenamento	Erro de administração do almoxarifado	Veja "erro humano"
			Vedação danificada no transporte	Erro de aquisição	Veja "erro humano"
Falha no motor	Etc.				
Falha na linha de recalque	Etc.				
Válvula fechada	Etc.				
Falha na alimentação de energia	Etc.				

Chama-se atenção do leitor que nem sempre é necessário detalhar em tantos níveis o processo de análise das causas, pois vai refletir-se na análise de modos de falhas, de efeitos e das ações que se deve fazer posteriormente. Outra forma de análise, seguindo o mesmo exemplo do quadro 7.5, faz-se a separação dos setes níveis de causas em três grupos: causas próximas, intermediárias e raízes. A causa próxima (ou causa imediata) é a mais evidente e, normalmente, é a causa relatada pelo operador do sistema técnico (uma máquina, por exemplo). No quadro 7.5, um operador conseguiria identificar os níveis um e dois com facilidade, e o nível três, para algumas causas. As causas intermediárias recebem esta denominação porque são vistas em um nível mais profundo da análise, e sua identificação e classificação dependem de especialistas no problema e de instrumentos de monitoramento adequados. Nesse caso, situam-se os níveis quatro até seis. Ou seja, muitos deles dependerão de instrumentos e bom conhecimento de especialista para serem identificados. Já as causas raízes, por sua vez, são consideradas o último nível de análise. Note-se que o desdobramento das causas intermediárias até suas causas raízes dependerá da definição do escopo de análise, de forma análoga ao apresentado na seção sobre efeitos. Em uma análise mais superficial, pode-se desdobrar as causas em apenas um nível, que, neste caso, seria a causa imediata. Contudo, na maioria das aplicações de FMEA é normal que se desdobre as causas em mais níveis, a fim de identificar a origem do problema, e o que era uma causa imediata passa a se tornar intermediária. De uma forma geral, a causa raiz está associada ao último nível de desdobramento. Teoricamente, resolvendo a causa raiz, resolvem-se todas as outras causas.

Os autores deste livro defendem que as causas raízes estão normalmente relacionadas ao contexto gerencial da organização, ou seja, não está centrada no sistema técnico, mas sim na parte organizacional da instituição. Por exemplo, a falha de um equipamento pode ter ocorrido por uma falha de manutenção. Esta, por sua vez, pode ter ocorrido pela falta de capacitação do manutentor. Nesse caso, a falha raiz está centrada na decisão gerencial de não ter propiciado a capacitação adequada na organização em relação à manutenção. No caso do quadro 7.5, a causa raiz está relacionada a erro humano, chamado de montagem, fabricação, operação etc., que pode estar no nível 5, 6 ou 7.

Na abordagem do FMEA "híbrido", utiliza-se uma coluna para a "falha funcional", outra para o "modo de falha" – que é a causa imediata da falha funcional –, e outra para as causas: imediata, intermediária ou, eventualmente, raiz. Dessa forma, contempla a nomenclatura de ambas as normas da SAE.

7.1.2 TIPOS DE FMEA

Na preparação de uma FMEA, a equipe deve fazer as seguintes perguntas: A quem interessa o resultado da análise? Quem é o cliente principal da FMEA? Qual é o sistema a ser analisado? É necessário abordar aspectos de segurança? Discutir estas e outras questões, e formalizar as respectivas respostas antes de iniciar uma FMEA, ajuda a equipe a identificar o "tipo" de FMEA mais apropriado, e que melhor resolverá o problema apresentado. Esta preparação é importante, porque para cada tipo de FMEA é requerido um conjunto de informações que a equipe técnica deve gerar para orientar adequadamente as ações e decisões gerenciais decorrentes da análise.

A definição do tipo de FMEA é importante para se fazer o preenchimento das ações a serem desenvolvidas. Assim, quanto melhor definido for o tipo de FMEA, mais aderente às necessidades do "cliente" serão as ações recomendadas. De modo geral, o tipo de FMEA está relacionado com o ciclo de vida do componente ou com o nível de detalhamento da análise.

Em relação ao ciclo de vida, a caracterização do tipo depende da fase do ciclo de vida em que se aplica a análise. Nesse caso existem os seguintes tipos: FMEA de projeto, FMEA de processo, FMEA de fabricação e FMEA de serviço. Assim, uma FMEA de serviço pode ser a aplicada à manutenção.

Em relação ao nível de detalhamento da análise, existem os tipos FMEA de sistema, FMEA de subsistema, FMEA de componente etc.

Para qualquer dos tipos aplica-se uma das abordagens explicitadas: funcional ou estrutural. A opção por um tipo e por uma abordagem depende do resultado que se quer obter, ou para quem serão destinadas as informações resultantes da análise. Adicionalmente, nos casos em que a análise envolve aspectos relacionados a riscos importantes (por exemplo, relativos à segurança de pessoas, do meio

ambiente, do negócio etc.), é usual – e recomendável – acrescentar a avaliação da criticidade dos modos de falha.

A Figura 7.4 ilustra tipos e abordagens de FMEA aplicada ao setor automobilístico (BERTSCHE, 2008), no caso, aplicado a um automóvel e parte dele. Como pode ser observado na figura, sobre o sistema completo do veículo e sobre o subsistema de transmissão, diferentes tipos de FMEA e abordagens podem ser aplicados.

Quando a análise se dá sobre um componente como, por exemplo, a engrenagem, é requerida uma FMEA de projeto (tipo de projeto) e a abordagem estrutural. Nesse caso, o detalhamento da análise considera aspectos relacionados com o material, tratamento térmico, análise da microestrutura etc. Ainda na Figura 7.4 tem-se a necessidade de analisar o processo de fabricação. Nesse caso, o tipo de FMEA é de processo, e a abordagem funcional é a mais recomendada.

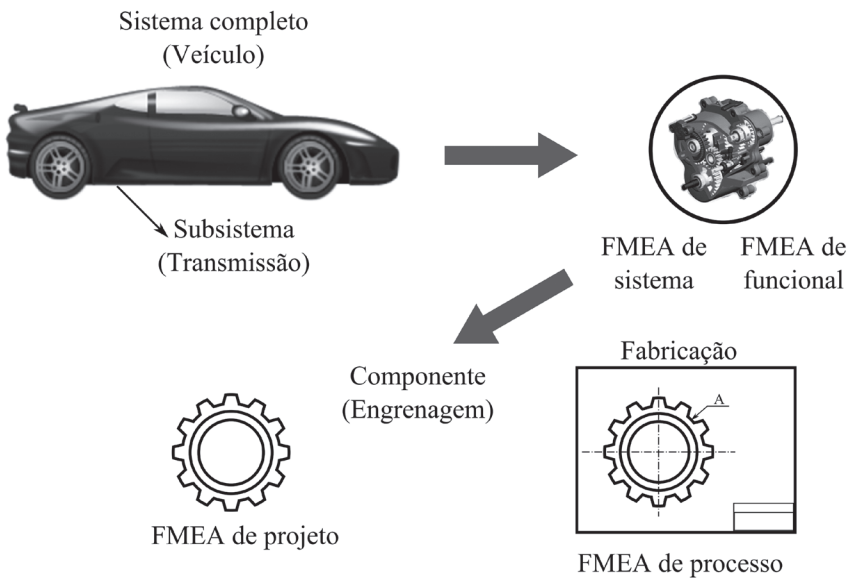


Figura 7.4 Tipos de FMEA para análise no setor automobilístico na abordagem funcional e estrutural (Adaptada de Bertsche (2008))

Os processos de análise são dinâmicos, e essas classificações nem sempre são possíveis ou fáceis de serem feitas. A definição do tipo de FMEA está presente na empresa que faz uso sistemático da técnica, e, de forma mais intensa, na empresa que vai adotar a técnica no seu planejamento de trabalho. Por vezes, o tipo de FMEA

que se apresenta não se enquadra no contexto da empresa, e, assim, recomenda-se fazer adequações, mas sempre com base em normas e referências consagradas. A mesma observação vale para as abordagens: funcional e estrutural. O prioritário é ter bom senso e centrar nos objetivos a serem obtidos com a análise.

É em função do tipo de FMEA e da abordagem que se faz a seleção dos especialistas que formarão a equipe de FMEA. Por sua vez, como já comentado, o tipo de FMEA é uma prerrogativa do problema a ser analisado e para quem servirá as informações. Assim, a análise deve sempre estar focada no cliente que vai implementar as ações.

7.1.3 EQUIPE DA FMEA

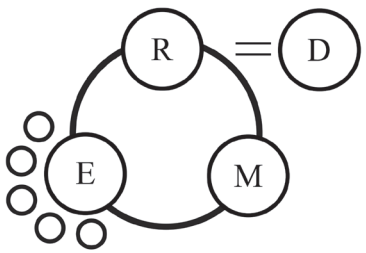
Como já comentado a técnica de FMEA, para ser desenvolvida com eficiência, deve ser constituída por uma equipe.

Eventualmente, a FMEA é desenvolvida por um especialista na técnica e um especialista no problema técnico a ser analisado, e, depois, ser submetida à apreciação de outros especialistas para que façam uma crítica do que foi produzido. Mas o trabalho em equipe é mais eficiente. Para tanto, é preciso ter uma liderança e profissionais de áreas específicas, correlatas ao tema em análise, requerendo do grupo objetividade e sinergia para atingir os objetivos propostos.

Não existe uma regra para definir o número de participantes. Sugere-se um número de cinco a nove, sendo considerado cinco um bom número. É ideal a presença de um engenheiro de projeto e de processo. E destaca-se que, embora a preparação da FMEA esteja designada a um indivíduo, a contribuição deve ser um esforço de todos. Durante o processo de trabalho, diferentes especialistas podem integrarem-se à equipe, num determinado instante específico da execução do FMEA. Outros especialistas participam em todo o ciclo de trabalho.

A Figura 7.5 apresenta a estrutura de uma equipe, na qual existe a presença de um responsável pelo desenvolvimento da FMEA (R), um grupo de especialistas (E) em campos de conhecimento de interesse da análise, um moderador (M) e o líder do projeto (D), que estipula a necessidade de se realizar a FMEA, e, eventualmente, também é o responsável pela FMEA. O moderador é um membro da equipe que tem conhecimento a respeito da técnica para orientar

as reuniões. No entanto, é importante que os membros do grupo de especialistas tenham conhecimento das definições utilizadas na FMEA, ou seja, tenham tido alguma capacitação sobre a técnica.



D: Departamento
(inicializador) líder do projeto

R: Resposável pelo desenvolvimento do FMEA

E: Grupo de especialistas
(Projetista, desenhista, operadores, fabricante, engenheiro de teste, etc.)

M: Moderador especialista em FMEA

Figura 7.5 Constituição da equipe de FMEA (BERTSCHE, 2008)

A escolha dos membros da equipe depende do problema a ser abordado, pois cada produto possui características particulares como função, projeto, materiais, processo de fabricação, cliente etc. Assim, cada membro participa com o conhecimento na respectiva área de atuação.

Sugere-se que a equipe contenha membros de áreas como pesquisa e desenvolvimento, engenharia de projeto, engenharia de confiabilidade, engenharia de processo, engenharia de qualidade, manutenção, engenharia de materiais, assistência técnica, técnicos, produção/manufatura, embalagem, clientes e fornecedores.

Outro ponto importante é a preparação da equipe, que deve estar comprometida, participando ativamente das reuniões. Assim, é fundamental que todos tenham conhecimento do sistema e da técnica FMEA, embora haja um moderador. Deve-se estabelecer as tarefas de forma objetiva, o que irá facilitar o processo de implantação das ações recomendadas. Por fim, salienta-se a importância da equipe estar preparada para situações inesperadas, reservando assim um tempo extra para esses imprevistos. Como consequência desses cuidados tomados, ganha-se tempo, reduz-se os erros causados por mal entendimento, retrabalho, dados incompletos e outros problemas (KUMAMOTO & HENLEY, 1996).

7.2 MÉTODO DE APLICAÇÃO DA FMEA

Existem vários métodos para a aplicação da FMEA que são apresentados por diversos autores. No entanto, de forma geral, se recomenda os seguintes passos:

a) Definição do item a ser analisado (sistema, subsistema, componentes etc.)
b) Definição da equipe
c) Análise funcional e identificação das funções do item a ser analisado
d) Identificação dos modos de falha e efeitos
e) Identificação das causas e controles atuais
f) Avaliação da criticidade (quando pertinente)
g) Levantamento das ações a serem executadas
h) Reavaliação dos índices de severidade, ocorrência e dificuldade de detecção, após a implementação das ações.

Note-se que a FMEA, propriamente dita, se inicia a partir do item "d". No entanto, os três primeiros passos são fundamentais para o sucesso da análise, e foram incluídos no método.

Uma vez que a função do item está claramente identificada, começa-se a fazer a análise de falha. O resultado da análise é registrado na forma de planilha, conforme ilustrado no Quadro 7.6, sendo que a quantidade de colunas necessárias tem relação direta com o nível de informação que se deseja registrar durante a FMEA. Evidentemente, tal qual ocorre em qualquer atividade de engenharia, cada coluna e cada registro efetuado demandam, ou devem demandar, ações específicas por parte dos analistas.

Observe-se que, no cabeçalho, são indicadas todas as informações para garantir a identificação do sistema em análise. Há sempre que se ter em mente que a planilha FMEA é um documento dinâmico e que precisa sofrer constantes atualizações. Por isso, a preocupação com a identificação correta, tanto do tipo de FMEA quanto dos itens que serão analisados. Veja que está sinalizado no cabeçalho do Quadro 7.6, que é FMEA de projeto. A abordagem está mesclada, já que as recomendações tratam de procedimentos a serem adotados, próprio da abordagem funcional e de testes específicos, como, por exemplo, de corrosão, próprio da abordagem estrutural.

Nas colunas têm-se os registros das atividades a serem desenvolvidas. Note-se que uma coluna pode estar constituída de várias linhas, e, em cada uma delas, existe uma especificação para o item e para a respectiva função (coluna 1). Para cada função pode-se ter mais de um modo de falha potencial. Na (coluna 2) tem-se o modo de falha que identifica que o painel inferior de dentro da porta está corroído. Na coluna 3 registram-se os efeitos relacionados a cada modo de falha e, na coluna 4, atribui-se um valor de severidade desses efeitos (que é usado caso opte-se pela análise de criticidade). A causa potencial vem registrada na coluna 5, e o índice de ocorrência é registrado na coluna 6. Na coluna 7, registram-se os controles já existentes para prevenir e detectar as causas que podem gerar modos de falha durante o processo de projeto. Na coluna 8, atribui-se um valor para o grau de dificuldade de se detectar a causa, ou mesmo o modo de falha, e, na coluna 9, registra-se o produtório dos valores atribuídos para os índices de severidade (4), ocorrência (6) e dificuldade de detecção (SOD) (9). O valor do produto é chamado de "número de prioridade de risco" (NPR). Como regra, os maiores valores estão relacionados com a prioridade de análise.

Quadro 7.6 Exemplo de planilha FMEA (SAE, 2002a)

ANÁLISE DOS MODOS DE FALHA E EFEITOS (FMEA DE PROJETO)

☐ Sistema — FMEA nº **1234** — **Página 1 de 1**
☒ Sub-sistema — Responsável pelo projeto **Body Engineering**
☐ Componente **01.03/Body Closures** — Preparado por **A. Tate - X6412 - Body Engr**
Ano(s)/programa(s) **199X/Lion 4dr/Wagon** — Data chave **9X 03 01 ER** — Data (Orig.) **8X 03 22 (Rev.) 8X 07 14**
Equipe principal **T. Fender-Car Product Dev., Childers-Manuf., J. Ford-Assy Ops (Dalton, Fraser, Henley Assembly Plants)**

Item / Função	Modo de falha potencial	Efeito potencial	S	Causas / Mecanismos potenciais	O	Controles atuais	D	NPR	Ações recomendadas	Responsável e meta para finalização	Ações executadas	S	O	D	NPR
1 Porta dianteira L.H H8HX-0000-A ▪ Entrar e sair do veículo ▪ Proteção dos ocupantes contra o tempo, ruído, e impacto lateral	2 Painel inferior de dentro da porta corroído	3 Deterioração da porta, levando a: ▪ Aparência insatisfatória devido à ferrugem através da pintura ao longo do tempo ▪ Função da porta no interior prejudicada	7	Gume superior da aplicação da proteção de cera especificado para o interior o painel é muito baixo	6	Teste de durabilidade geral do veículo T-118, T-109, T-301	7	294	Adicionar um teste de corrosão acelerada em laboratório	Tate-Boby Engrg 8X 09 30	Baseado nos resultados do teste (nº 1481) a especificação para o gume superior subiu 125mm	7	2	2	28
5 Especificação da espessura da cera é insuficiente					4	7 Teste de durabilidade geral do veículo – como acima	7	8 196	▪ Adicionar um teste de corrosão acelerada em laboratório ▪ Fazer um DOE (*Design of Experiments*) da espessura da cera	▪ Combinar x/testes para a verificação do gume superior da cera ▪ Tate-Body Ergrg 9X 01 15	Os resultados do teste (nº 1481) mostraram que a espessura especificada é adequada. DOE mostrou que variação de 25% na espessura é aceitável	7	2	2	28

A partir desta priorização, pelo valor do NPR relata-se na coluna 10 as recomendações para a equipe de projetistas, já que o FMEA é de projeto. Faz-se também a indicação do responsável por implementar as ações na coluna 11. Na coluna 11, termina-se o FMEA, mas é preciso fazer um acompanhamento das ações e verificação dos resultados. Assim, na coluna 12, registra-se as ações desenvolvidas e acompanha-se a implementação com nova análise de NPR na coluna 16, atribuindo-se novos índices de severidade, ocorrência e detecção nas colunas 13, 14, 15, respectivamente.

As recomendações, responsabilidades e ações são desenvolvidas somente para valores de NPR significativos, por exemplo, onde a média dos NPR for superior a 70% do valor máximo do NPR. Noutros casos isso ocorre na combinação do valor de NPR associado ao valor atribuído de severidade. Por exemplo, se severidade for igual ou superior a 8 ou 9 deve-se fazer análise, independente da ocorrência e detecção. No entanto, estas regras ou normas de condutas para as ações vão depender da equipe de FMEA e do tipo de FMEA.

7.3 CONSIDERAÇÕES FINAIS

Por ser uma técnica intensivamente utilizada, pode-se ter a falsa impressão de que todos os casos em que técnica for utilizada se darão de uma maneira naturalmente simples.

Embora a FMEA seja uma técnica consagrada, algumas limitações, de natureza administrativa e técnica, são observadas na sua aplicação prática. As questões administrativas referem-se às dificuldades no relacionamento interpessoal, às falhas no planejamento e na condução das reuniões. As questões técnicas, por sua vez, referem-se principalmente ao desconhecimento dos aspectos teóricos e práticos da aplicação da FMEA, à falta de conhecimento técnico dos participantes da equipe, às limitações diversas relacionadas à representação na forma de planilha e à dificuldade de se definir o que é modo de falha, efeito e causa. Vale ressaltar aqui que nem sempre a falha irá se ajustar às definições. As definições encontradas de modos de falha, causas e efeitos são bastante simples mas quando não estão bem definidas, geram discussões infindáveis durante as reuniões.

Além das questões citadas anteriormente, o caráter exaustivo da FMEA constitui em um dos principais entraves da técnica, pela

morosidade e, consequentemente, pelo custo de aplicação. A técnica também não está adaptada para levar em conta falhas dependentes ou resultantes de uma sucessão de acontecimentos. Nestes casos, é necessário utilizar outros métodos e técnicas, tais como a análise de Markov (BILLINTON & ALLAN, 1992) ou a análise por árvores de falhas (FTA).

Destaca-se, ainda, que o desenvolvimento de FMEA é um processo iterativo e precisa ser repetidamente revisto e realimentado, o que, por um lado, demanda uma constante dedicação da equipe, e, por outro, garante um aprimoramento contínuo do conhecimento relacionado ao item analisado. De fato, a característica iterativa é um dos pontos fortes da técnica.

A FMEA permite sistematizar o conhecimento gerado durante a análise, pois classifica e ordena o conhecimento dos especialistas consultados. Assim, a planilha FMEA institucionaliza o conhecimento e permite que este seja utilizado para o aprimoramento do item em análise e para futuros projetos, o que resulta em benefícios como:

- Redução dos riscos relativos à confiabilidade e à segurança.
- Melhoria da qualidade e da mantenabilidade.
- Redução do custo e do tempo de desenvolvimento de novos produtos.
- Os participantes da equipe da FMEA passam a conhecer melhor o sistema analisado.
- A documentação gerada institucionaliza o conhecimento, podendo ser utilizada – por exemplo – para capacitação dos colaboradores da organização.

Por fim, considera-se que FMEA é uma técnica institucional. Tem o objetivo de organizar o conhecimento dos especialistas na instituição. Por isso é dinâmica, e a cada mudança do cenário técnico (produto, processo, serviço etc.) e dos especialistas, recomenda-se que seja feito um novo processo de análise a partir da recuperação do conhecimento existente, com o fim de estruturar-se um novo resultado e novas tomadas de decisão.

Capítulo 8

ANÁLISE DA ÁRVORE DE FALHAS (FTA)

A técnica de análise da árvore de falhas (FTA - *Fault Tree Analysis*) foi desenvolvida por H. A. Watson dos laboratórios Bell Telephone, que, em 1962, utilizou a FTA para análise do sistema de lançamento do míssil intercontinental Minuteman (RAUSAND & HOYLAND, 2004). Os primeiros artigos abordando a FTA foram publicados em 1965, no Simpósio de Segurança patrocinado pela Universidade de Washington e a Boeing Company (REASON, 1997).

A FTA é uma técnica dedutiva (de pensamento reverso), ou seja, a partir de um evento inicial, o qual se quer analisar (chamado de evento topo), identificam-se os eventos intermediários resultantes da associação lógica das causas básicas ou raízes, que geraram o evento de topo. O exame e a estratificação dos eventos intermediários seguem até que se tenha identificado as causas básicas para a ocorrência do evento de topo, ponto onde se tem o limite de resolução da FTA. A estruturação e a combinação das causas que resultarão no evento de topo são feitas por meio de operadores lógicos utilizados na análise de álgebra booleana, em portas lógicas do tipo: "E", "OU" etc. Deste modo, a FTA permite tanto a análise qualitativa da relação causa-efeito quanto à análise quantitativa, a partir da determinação da probabilidade de ocorrência das causas básicas e de seu relacionamento lógico, os quais determinarão a probabilidade de ocorrência do evento de topo. Para a análise quantitativa de sistemas mais complexos, outros métodos de cálculo podem ser utilizados, como por exemplo, o método de Monte Carlo. Nos casos em que se deseja tratar a incerteza por imprecisão, presente nas causas básicas, métodos heurísticos são utilizados para modelagem do relacionamento entre as causas e sua participação na ocorrência do evento de topo, a lógica *fuzzy* é um exemplo de ferramenta utilizada nesses casos.

A FTA permite estabelecer uma relação causa/efeito aplicável tanto em estudos do atributo confiabilidade quanto no estabelecimen-

to de cenários, normalmente utilizados em análise de risco. A representação gráfica padronizada das causas básicas e sua estruturação lógica, a partir do uso de portas lógicos, permitem ao analista:

- Em análises qualitativas, determinar os fatores bem como seu relacionamento lógico, que contribuem para a ocorrência do evento de topo ou do efeito indesejado para o sistema;
- Em análises quantitativas, determinar a probabilidade de ocorrência do evento de topo ou do efeito indesejado para o sistema, em função da probabilidade da ocorrência das causas básicas e seu relacionamento lógico;
- Identificar os eventos e/ou causas que são mais significativos para a ocorrência do evento de topo e seu impacto para a funcionalidade e confiabilidade do sistema. Desta forma é possível antever quais eventos e/ou causas afetam mais de uma funcionalidade do sistema ou aqueles que podem anular os benefícios de redundâncias específicas que visem evitar o efeito indesejado, contribuindo para a priorização de ações preventivas ou corretivas;
- Entender o sistema sob análise e identificar novas concepções de projeto ou oportunidades de melhoria, a partir da interposição de barreiras que minimizem o impacto das causas e/ou eventos que contribuem para a ocorrência do evento de topo; e
- Organizar a informação e explicitar o conhecimento de especialistas no sistema sob análise para auxiliar o planejamento e a tomada de decisão em intervenções de manutenção, operação e capacitação.

8.1 DESENVOLVIMENTO DA ÁRVORE DE FALHAS

No desenvolvimento da árvore de falhas são consideradas quaisquer causas pertinentes que conduzam ao evento topo, tais como: falha de equipamento, erro humano ou erro de *software*. Contudo, é importante perceber que a árvore de falhas é um modelo; portanto, o analista considera apenas as causas mais significativas, desprezando as consideráveis irrelevantes.

A Figura 8.1 apresenta a estrutura básica de uma árvore de falhas, na qual é possível identificar o evento de topo, localizado no

ponto mais alto da árvore e um evento intermediário cuja combinação lógica das causas básicas resulta no evento de topo. Esta forma de estruturação da FTA é denominada de pensamento reverso ou *top-down*, uma vez que, inicia-se com o evento de topo e, a partir dele, desenvolve-se a análise buscando identificar as causas básicas, cuja combinação lógica resulta no evento de topo. A árvore deste exemplo apresenta dois níveis hierárquicos; entretanto, em sistemas reais existem diversos níveis hierárquicos, cada qual com vários eventos. O primeiro nível hierárquico trata dos eventos e/ou causas imediatas que resultam no evento de topo e que, por vezes, pode ser tratado como o efeito indesejado para o sistema o qual se quer analisar. O evento de topo pode ser tratado também como uma causa particular, pertencente a uma árvore de falhas maior, a qual se queira detalhar. Nos níveis hierárquicos inferiores estão os eventos intermediários resultantes da combinação lógica das causas básicas e/ou de outros eventos intermediários. Na base da árvore de falhas estão as causas básicas as quais devem ser controladas para mitigar ou eliminar os eventos intermediários que conduzem ao evento de topo ou efeito indesejado sob análise. É comum referir-se às causas básicas como causas raízes. Normalmente, a causa raiz está associada à organização empresarial, mas nem sempre é isso que está presente na bibliografia.

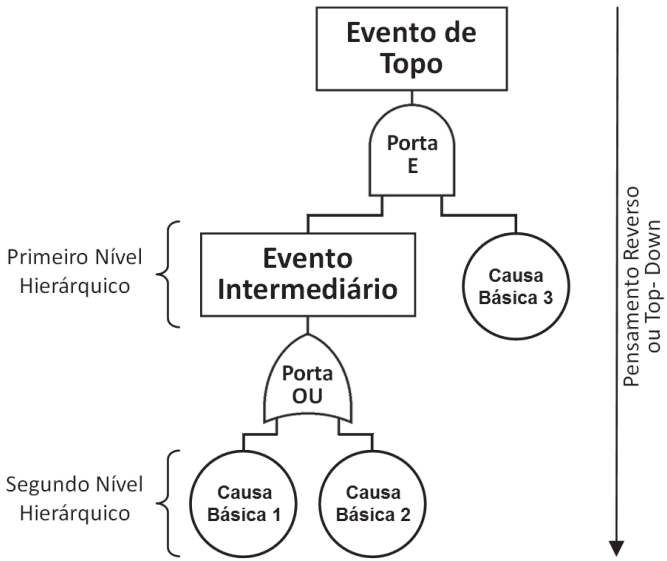


Figura 8.1: Estrutura de uma árvore de falhas.

As etapas a serem cumpridas para desenvolvimento de uma FTA são:

- Planejamento para condução da FTA, incluindo definição da equipe de desenvolvimento da FTA, a qual deve contar com especialistas na técnica e no sistema o qual se pretende analisar; recursos financeiros para estruturação da equipe, incluindo uma previsão orçamentária para treinamentos e infraestrutura, caso necessária; e definição de um cronograma de desenvolvimento;
- Definição do sistema que será analisado e, deste, coleta das informações necessárias para sua análise funcional e seleção dos eventos de topo e/ou efeitos indesejados que serão analisados. Nesta etapa, pode ser útil a utilização concomitante de técnicas como Diagrama de Ishikawa ou Diagrama de Pareto. Tais técnicas podem auxiliar a identificação dos eventos de topo e/ou efeitos mais relevantes para a falha do sistema e que, portanto, ratificam a necessidade da FTA para detalhamento das causas. Todos os fatores contribuintes para ocorrência do evento de topo e/ou efeito indesejado devem ser previstos, tais como: questões ambientais, operacionais, de segurança, de controle, erros humanos e exigências específicas do sistema;
- Desenvolvimento e validação das árvores de falha do sistema selecionado. Nesta etapa a equipe deve desenvolver as árvores de falha dos eventos de topo ou efeitos indesejados do sistema até chegar às causas básicas. O processo inicia-se com os eventos que podem, diretamente, causar o evento de topo ou efeito indesejado sob análise, constituindo o primeiro nível hierárquico da árvore de falhas. No segundo nível hierárquico são representados os eventos ou causas básicas que resultam nos eventos ou efeitos indesejados relacionados no primeiro nível hierárquico. O processo continua até o último nível hierárquico de análise, no qual se têm somente causas básicas. Concluído o processo, especialistas no sistema sob análise devem validar os resultados obtidos;
- Análise e síntese dos resultados obtidos. Com a árvore de falhas estruturada e validada procedem-se as análises qualitativas e quantitativas da mesma. A análise qualitativa consiste em

determinar o grupo mínimo de corte, eliminando causas e/ou eventos redundantes; explicitar as partes críticas do sistema, as quais demandam atenção especial; determinar, com base no relacionamento lógico, o impacto das causas e/ou eventos intermediários no evento de topo ou efeito indesejado sob análise. Já a análise quantitativa consiste em desenvolver as equações booleanas dos eventos intermediários e do evento de topo; determinar a probabilidade de ocorrência das causas básicas com base na taxa de falhas (λ) ou no tempo médio entre falhas (MTBF - *Mean Time Between Failure*); determinar a probabilidade de ocorrência dos eventos intermediários e de topo em função da probabilidade de ocorrência das causas básicas; calcular a confiabilidade do sistema e verificar sua aderência aos critérios de segurança, de legislação, técnicos, ambientais e outros que estabeleçam os requisitos para o sistema sob análise; e

- Planejamento das ações. A partir dos resultados das análises qualitativas e/ou quantitativas devem ser planejadas as ações, melhorias e/ou barreiras para prevenir a ocorrência dos eventos de topo ou efeitos indesejados; ou, um plano com regras de conduta para o caso de ações corretivas.

A complexidade da FTA tem uma relação direta com a complexidade do sistema sob análise e o nível de detalhamento desejado. Árvores de falhas complexas, com grande número de causas básicas associadas a um relacionamento lógico muito hierarquizado, podem exigir a utilização de ferramentas computacionais para auxiliar o seu desenvolvimento e sua resolução e análise. Quando isso ocorre, é comum utilizar processos de simplificação da árvore de falha como, por exemplo, o método do grupo mínimo de corte (*Cut Set*), a ser abordado ao longo deste texto.

8.2 REPRESENTAÇÃO GRÁFICA DA ÁRVORE DE FALHAS

Para a construção da árvore de falhas são utilizados símbolos que representam as portas lógicas, os eventos intermediários e de topo e as causas básicas, além de outros símbolos específicos para organização e correta representação do conhecimento inerente à relação causal que se quer explicitar. Tal simbologia segue convenções

normatizadas como, por exemplo, a norma IEC 61025 (*Fault Tree Analysis*), ou então manuais para desenvolvimento da FTA, como é o caso do NUREG-0492 (*Risk Assessment Review Group Report - Fault Tree Handbook*), proposto pela comissão americana de regulamentação nuclear (NRC - *Nuclear Regulatory Commission*) e do manual proposto pela agência espacial americana (NASA - *National Aeronautics and Space Administration - Fault Tree Handbook with Aerospace Applications*).

As portas lógicas conectam os eventos e/ou causas de acordo com suas relações causais. As entradas situam-se na parte inferior da porta lógica enquanto que o evento de saída situa-se na parte superior, conforme a Figura 8.2. Independentemente do número de entradas, a associação lógica estabelecida por uma porta lógica resulta em um único evento de saída.

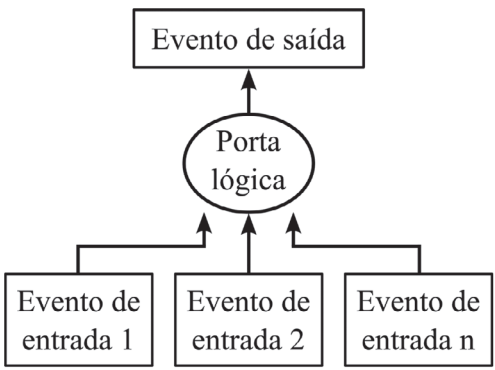


Figura 8.2: Eventos de entrada e saída em uma porta lógica (SAKURADA, 2001).

O Quadro 8.1 sintetiza os principais parâmetros relacionados às portas lógicas comumente utilizadas na construção de uma árvore de falhas, com base no anexo A da IEC 61025. A última coluna pode ser utilizada na análise quantitativa da árvore de falhas para determinação da probabilidade de ocorrência do evento de saída (F(t) - Probabilidade de Falha) das respectivas portas lógicas. Neste caso, após a determinação da probabilidade de ocorrência do evento de topo $F_T(t)$ e, considerando que as causas básicas sejam independentes, a probabilidade de sucesso ou a confiabilidade (R(t)) do sistema sob análise pode ser determinada pela equação 8.1.

$$R(t)=1-F_T(t) \qquad (8.1)$$

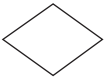
Quadro 8.1: Portas lógicas, descrição e probabilidade de ocorrência (IEC, 2006).

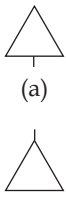
Símbolo	Nome da porta lógica	Descrição	Probabilidade de ocorrência do evento de saída F(t)
	E	O evento de saída só ocorre se todos os eventos de entrada ocorrerem simultaneamente. Caracteriza um sistema paralelo simples.	$F(t) = \prod_{i=1}^{n} F_i(t)$
	E com Prioridade	O evento de saída só ocorre se todos os eventos de entrada ocorrerem em uma ordem seqüencial da esquerda para a direita.	Requer análise por cadeias de Markov ou probabilidade condicional
	OU	O evento de saída ocorre quando pelo menos um dos eventos de entrada ocorrer. Caracteriza um sistema série.	$F(t) = 1 - \prod_{i=1}^{n} [1 - F_i(t)]$
	OU Exclusivo	O evento de saída ocorre se um e apenas um dos eventos da entrada ocorrer.	Supondo apenas 2 eventos de entrada, tem-se: $F(t) = F_1(t).[1 - F_2(t)]$
	M de N	O evento de saída ocorre se pelo menos "m" dos "n" eventos possíveis de entrada ocorrerem. Caracteriza um sistema paralelo parcial. Alguns autores o identificam como sistema complexo.	Supondo que todos os eventos de entrada tenham a mesma probabilidade de falha (F), tem-se: $F(t) = \sum_{i=0}^{k-1} \frac{n!}{i!.(n-i)!} \cdot (1-F)^i \cdot (F)^{n-i}$ Onde: $k = (n-m)+1$
	Inibição	O evento de saída só ocorre quando ocorrem simultaneamente o evento de entrada (F_E) e um evento condicional (F_C). Pode ser considerada como uma forma especial da porta "E".	$F(t) = F_E \cdot F_C$
	Não	O evento de saída só ocorre quando o evento de entrada (F_E) não ocorrer.	$F(t) = 1 - F_E$

Nota: As equações para determinação da probabilidade de ocorrência do evento de saída F(t) em função da probabilidade de ocorrência dos eventos de entrada $F_i(t)$ são válidas apenas para eventos e/ou causas básicas independentes. Neste caso, a ocorrência de um evento não afeta a probabilidade de ocorrência do outro.

O Quadro 8.2 sintetiza os principais aspectos relacionados aos eventos e complementa os símbolos comumente utilizados na construção de uma árvore de falhas, com base no anexo A da IEC 61025.

Quadro 8.2: Simbologia e descrição de outras representações de eventos para a construção de FTA (IEC, 2006).

Símbolo	Nome	Descrição
	Retângulo	Representa o evento de topo ou um evento intermediário resultante da associação lógica estabelecida entre as entradas presentes nas portas lógicas que compõem a árvore de falhas. No interior do retângulo identifica-se o efeito indesejado ou o modo de falha resultante naquele ponto da análise.
	Círculo	Representa as causas básicas ou raízes cujas associações lógicas estabelecidas na árvore de falhas resultarão no evento de topo. A profundidade da análise depende do limite de resolução da FTA estabelecido como satisfatório. Seja qual for esse limite, o círculo é utilizado para as causas pertencentes ao nível mais baixo da análise, das quais se tem sua probabilidade de ocorrência. Na análise de confiabilidade, a causa básica pode estar num primeiro ou segundo nível da análise, ou seja, imediata ou intermediária. Na análise de risco, leva-se a análise até a causa raiz, que, normalmente, está relacionada com aspectos organizacionais.
	Losango	Representa eventos não desenvolvidos ou não analisados. Os principais motivos para sua utilização são: não se tem um detalhamento das causas básicas do evento, falta de informação e/ou conhecimento sobre a conjunção de causas básicas que irá resultar no evento, falta de tempo para uma análise mais aprofundada do evento ou eventos para os quais não se tem os dados referentes à sua probabilidade de ocorrência. Neste último caso os eventos são removidos da árvore de falhas antes de uma análise quantitativa.
	Oval	Representa eventos condicionais, ou seja, os que, ocorrendo juntamente com outro pré-existente, produziram um resultado (evento de topo ou intermediário). É a condição para que outros eventos ocorram, podendo ser utilizada juntamente com outras portas lógicas para representar uma condição especial ou evento gatilho (utilizada particularmente em conjunto com a porta lógica "Inibição").
	Pentágono ou Casa	Representa a possibilidade do analista, de simular a ocorrência ou não de certos eventos representados na árvore de falhas. Neste caso, o evento representado pelo pentágono ou casa pode ser considerado como presente ou ausente da análise, o que irá desencadear associações lógicas diferentes nas ramificações subsequentes da árvore de falhas.

 (a) (b)	Triângulo	Representa a transferência ou a cópia de uma ramificação da árvore de falhas. A ramificação transferida pode ser uma parte da árvore de falhas sob análise ou outra desenvolvida externamente à mesma. Os triângulos são identificados com um número em seu interior, sendo que, os de mesmo número se referem à mesma cadeia de eventos (ramificação). O triângulo *transfer out* (a) é utilizado na ramificação a ser copiada ou naquela desenvolvida externamente à árvore de falhas sob análise. O triângulo *transfer in* (b) é utilizado no ponto de "chegada", o qual recebe a cópia feita pelo *transfer out*. A utilização do triângulo de transferência evita a repetição de eventos e/ou ramificações iguais e simplifica a representação da árvore de falhas.

Vale ressaltar que a simbologia para representação da árvore de falhas pode divergir entre as normas ou procedimentos existentes. Cabe à equipe de análise escolher, antes do início da etapa de desenvolvimento da FTA, a norma ou procedimento mais aderente ao contexto da empresa ou sistema a ser analisado.

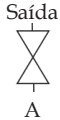
8.3 ASPECTOS DA ÁLGEBRA BOOLEANA APLICADA À FTA

Os conceitos da álgebra booleana foram formulados pelo matemático inglês George Boole, por volta de 1850. A álgebra booleana é utilizada na FTA para sintetizar em uma equação a combinação lógica das causas básicas que resultará no evento de topo. Tal equação considera que as causas básicas da FTA são independentes entre si. O equacionamento da álgebra booleana, comumente utilizado na FTA, é mostrado no Quadro 8.3. Para síntese das equações relativas às portas lógicas utilizadas na FTA a álgebra booleana compreende:

- Um conjunto representativo das causas básicas e/ou eventos intermediários ou de topo: B={a, b, c, ...};
- Duas operações binárias: o sinal de soma (+) é representativo da operação lógica "OU" e o de multiplicação ($\cdot$) é representativo da operação lógica "E". Além do símbolo específico ($\oplus$) representativo da operação lógica "OU Exclusivo";
- Uma operação singular de negação é identificada por uma barra ($^{-}$);

- Dois elementos distintos: zero "0" é representativo da ausência da causa e/ou evento e a unidade "1" é representativa da presença da causa e/ou evento.

Quadro 8.3: Equacionamento da álgebra booleana utilizado na FTA

Porta	Eventos	Equação Booleana	Tabela Verdade		
E		Saída = A · B	A	B	Saída
			0	0	0
			0	1	0
			1	0	0
			1	1	1
OU		Saída = A + B	A	B	Saída
			0	0	0
			0	1	1
			1	0	1
			1	1	1
OU Exclusivo		Saída = A ⊕ B	A	B	Saída
			0	0	0
			0	1	1
			1	0	1
			1	1	0
Não		Saída = $\bar{a}$	A		Saída
			0		1
			1		0

A partir da equação representativa do evento de topo é possível, com a aplicação das propriedades da álgebra booleana (Quadro 8.4), simplificar a árvore de falhas e desenvolver a análise quantitativa da mesma.

Quadro 8.4: Propriedades da álgebra booleana

Propriedade	Desenvolvimento	
Associativa	$(A + B) + C = A + (B + C)$	$(A \cdot B) \cdot C = A \cdot (B \cdot C)$
Comutativa	$A + B = B + A$	$A \cdot B = B \cdot A$
Idempotente	$A + A = A$	$A \cdot A = A$
Absorção	$A + (A \cdot B) = A$	$A \cdot (A + B) = A$
Distributiva	$A + (B \cdot C) = (A + B) \cdot (A + C)$	$A \cdot (B + C) = (A \cdot B) + (A \cdot C)$
Identidade	$A + 1 = 1$ | $A + 0 = A$	$A \cdot 1 = A$ | $A \cdot 0 = 0$
Complementar	$A + \overline{A} = 1$	$A \cdot \overline{A} = 0$
Teorema de Morgan	$\overline{(A + B)} = \overline{A} \cdot \overline{B}$	$\overline{(A \cdot B)} = \overline{A} + \overline{B}$

Para análise quantitativa de uma árvore de falha, como apresentada na Figura 8.1, é necessário operar por meio de álgebra booleana as informações qualitativas de relacionamento entre causas e efeito, os eventos intermediários e os operadores condicionantes dos eventos, que são representados pelas portas lógicas. Assim, com as regras para formatar o equacionamento das árvores de falha do Quadro 8.3 combinado com as propriedades do Quadro 8.4, pode-se construir aplicações como o apresentado no exemplo 8.1 e 8.2.

Exemplo 8.1: Utilizando os conceitos da álgebra booleana, determinar a equação do evento de topo e simplificar a árvore de falha da Figura 8.3.

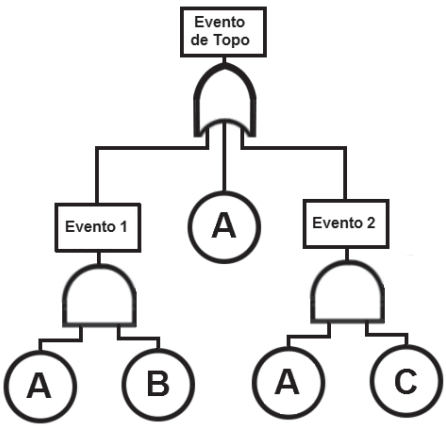


Figura 8.3: Estrutura do FTA para exemplo 8.1

Equação dos Eventos:
$Evento1 = A \cdot B$ $Evento2 = A \cdot C$

Equação do Evento de Topo:
$Evento\ de\ Topo = A + Evento1 + Evento2$
$Evento\ de\ Topo = A + (A \cdot B) + (A \cdot C)$

Aplicando a propriedade da Absorção:
$A + (A \cdot B) = A$ $Evento\ de\ Topo = A + (A \cdot C)$

Aplicando novamente a propriedade da Absorção:
$A + (A \cdot C) = A$ Portanto $Evento\ de\ Topo = A$

A árvore de falhas do exemplo 8.1 é equivalente à árvore de falha da Figura 8.4. Isso significa que o evento de topo é dependente apenas da causa básica "A". A tabela "verdade" abaixo comprova esse fato.

Quadro 8.5: Tabela verdade de análise da FTA do exemplo 8.

Figura 8.4: Estrutura síntese do FTA do exemplo 8.1

A	B	**Evento 1** A · B	C	**Evento 2** A · C	**Evento de Topo** A + Evento 1 + Evento 2
0	0	0	0	0	0
0	1	0	1	0	0
1	0	0	0	0	1
1	1	1	1	1	1

=

Exemplo 8.2: Dada a árvore de falha da Figura 8.5 e considerando a independência das causas básicas (A, B e C) determinar a equação do evento de topo, sua probabilidade de ocorrência ($F_{Evento\ de\ Topo}$) e a confiabilidade do sistema ($R_{Sistema}$).

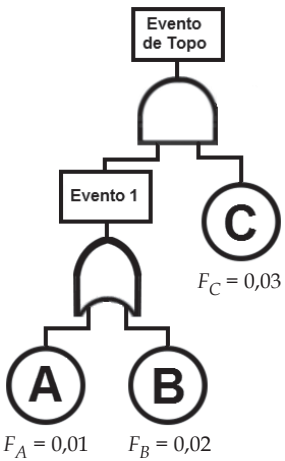


Figura 8.5: Estrutura do FTA para exemplo 8.2

Equação booleana dos eventos:

Evento1 = A + B Evento de Topo = (A + B) · C

De acordo com o Quadro 8,1, tem-se:

Porta OU: $F(t) = 1 - \prod_{i=1}^{n} [1 - F_i(t)]$

Porta E: $F(t) = \prod_{i=1}^{n} F_i(t)$

Assim, tem-se:

$F_{Evento1} = A + B = 1-(1-0,01)\cdot(1-0,02) = 0,0298 = 2,98\%$

$F_{Evento\ de\ Topo} = F_{Evento1} \cdot C = 0,0298 \cdot 0,03 = 0,000894 = 0,0894\%$

$R_{Sistema} = 1 - F_{Evento\ de\ Topo} = 1 - 0,000894 = 0,999106 = 99,91\%$

No exemplo 8.2 foi possível obter a quantificação da probabilidade de ocorrência do evento de topo, na forma de probabilidade de insucesso, caracterizado pela função de probabilidade acumulada de falha, também denominada de não-confiabilidade F(evento) e a probabilidade de sucesso caracterizada pela confiabilidade R(sistema).

8.4 ASSOCIAÇÃO ENTRE FTA E OUTRAS TÉCNICAS

Para facilitar a explicitação do conhecimento inerente à estruturação e desenvolvimento da FTA, é comum a utilização de técnicas complementares de análise. Essas técnicas facilitam a elicitação das causas básicas que resultarão nos eventos intermediários e de topo ou efeito indesejado que se pretende analisar. Alguns exemplos de utilização concomitante da FTA com outras técnicas de análise são mostrados nos próximos itens.

8.4.1 FTA E DIAGRAMA DE ISHIKAWA

O diagrama de Ishikawa foi desenvolvido por Kaoru Ishikawa e é também conhecido como diagrama de causa e efeito ou diagrama espinha de peixe (SAKURADA, 2001). Na FTA, o diagrama de Ishikawa pode ser utilizado como ferramenta para estruturação de reuniões de *brainstorm* com o objetivo de identificar as causas básicas dos eventos intermediários e de topo. Uma combinação de árvore de falhas e diagrama de Ishikawa é ilustrada na Figura 8.3, da qual é possível depreender o relacionamento causa e efeito proporcionado pelo diagrama de Ishikawa e sua transposição para a árvore de falhas. O efeito (Interrupção do Sistema de Bombeamento) objeto de estudo do diagrama de Ishikawa foi transposto para a FTA como evento de topo, cujas causas básicas foram elicitadas no diagrama de Ishikawa e associadas na FTA com a utilização das portas lógicas.

O diagrama de Ishikawa mostra de forma gráfica a relação entre determinado evento ou efeito e suas causas potenciais ou básicas, no entanto, não estabelece a relação lógica entre estas causas a qual resultará na ocorrência do evento. Esta relação lógica é justamente a característica peculiar da FTA que a difere do diagrama de Ishikawa acrescentando-lhe funcionalidades.

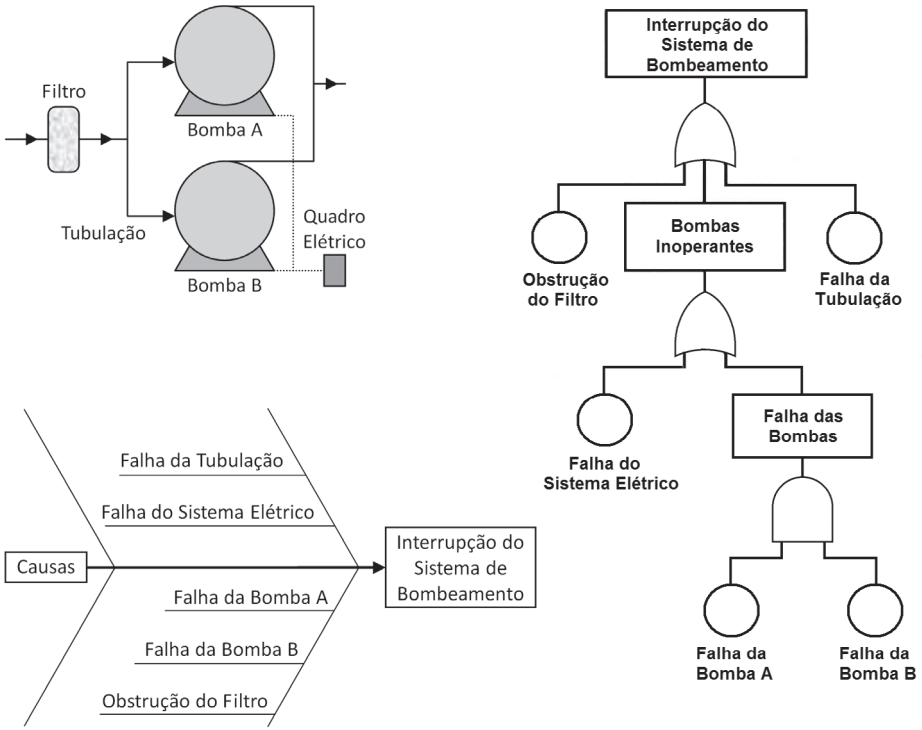


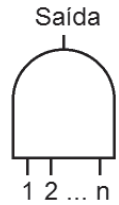
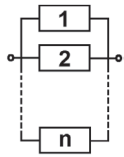
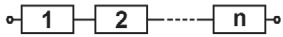
Figura 8.3: Associação entre diagrama de Ishikawa e FTA.

8.4.2 FTA E DIAGRAMA DE BLOCOS DE CONFIABILIDADE

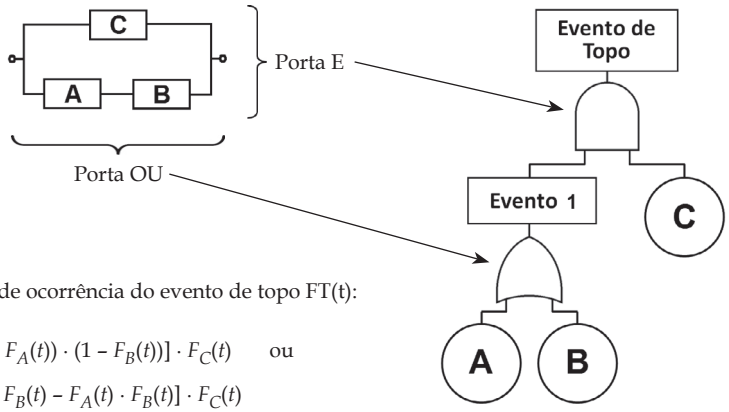
O diagrama de bloco de confiabilidade (RBD - *Reliability Block Diagrams*), assim como a árvore de falhas, auxilia a representação gráfica do sistema. Garantida a independência das causas básicas, a árvore de falhas pode ser convertida em um diagrama de blocos de confiabilidade e vice-versa. Convém ressaltar, no entanto, a contraposição dos conceitos envolvidos, uma vez que o diagrama de bloco é utilizado para determinar a confiabilidade do sistema (probabilidade de sucesso) e a árvore de falhas, o relacionamento lógico entre as causas básicas que leva o sistema a falhar (probabilidade de falha). Para garantir a sinergia com a FTA, o diagrama de blocos deve consistir apenas de configurações em Série, Paralelo ou Misto, excluindo-se, portanto, as estruturas complexas às quais não admitem uma configuração em série ou em paralelo de

seus blocos constituintes. O Quadro 8.5 resume os critérios para a conversão de uma árvore de falhas em um diagrama de blocos de confiabilidade equivalente.

Quadro 8.5: Conversão Árvore de Falha em Diagrama de Blocos de Confiabilidade.

Árvore de Falhas	Diagrama de Blocos Equivalente	Confiabilidade (R(t)) e Probabilidade de Falhas (F(t))
		$R(t) = 1 - \prod_{i=1}^{n} [1 - R_i(t)]$ $F(t) = \prod_{i=1}^{n} F_i(t)$
		$R(t) = \prod_{i=1}^{n} R_i(t)$ $F(t) = 1 - \prod_{i=1}^{n} [1 - F_i(t)]$

A Figura 8.4 exemplifica a conversão de um diagrama de blocos de confiabilidade em uma árvore de falhas equivalente. A configuração série do diagrama de blocos é transposta para a árvore de falhas como uma porta lógica "OU", o que equivale dizer que basta que um dos blocos falhe (A ou B) para que ocorra o evento 1. A configuração paralela do diagrama de blocos é transposta para a árvore de falhas como uma porta lógica "E", o que equivale dizer que é necessário que ambas as ramificações do diagrama de blocos falhem (A ou B e C) para que ocorra o evento de topo.



Probabilidade de ocorrência do evento de topo FT(t):

$F_T(t) = [1 - (1 - F_A(t)) \cdot (1 - F_B(t))] \cdot F_C(t)$ ou

$F_T(t) = [F_A(t) + F_B(t) - F_A(t) \cdot F_B(t)] \cdot F_C(t)$

Figura 8.4: Associação entre diagrama de blocos de confiabilidade e FTA.

Sistemas complexos exigem uma conversão prévia para configurações em série ou paralelo equivalente, para posterior conversão para árvore de falhas. Os próximos itens abordam dois métodos comumente utilizados para esta finalidade.

8.4.2.1 MÉTODO DO GRUPO DE CORTE

O método do Grupo de Corte (*Cut Set*) consiste em dispor em série os grupos de componentes do sistema cuja falha (de todos os componentes do grupo) resulta na falha do sistema. Esse grupo de componentes é chamado de grupo de corte. Um grupo de corte é dito mínimo se seus eventos constituintes não puderem ser reduzidos em número, e cuja ocorrência do grupo resulta na ocorrência do evento de topo. Na FTA a aplicação da álgebra booleana permite reduzir a árvore de falhas a uma forma logicamente equivalente, composta apenas pelos grupos mínimos de corte. Os componentes de cada grupo de corte são selecionados passando uma linha transversal ao caminho que liga a entrada à saída do sistema. Cada linha que corta transversalmente o caminho da entrada à saída forma um grupo de corte. O método é ilustrado na Figura 8.5, que ilustra também a árvore de falhas resultante da conversão do diagrama de blocos formado pelos grupos de corte. Neste caso, para a estrutura em ponte representada, foram identificados quatro grupos de corte (C1, C2, C3 e C4), os quais são conectados em série. A falha simultânea de todos

os componentes de pelo menos um destes grupos resultará na falha do sistema (BILLINTON e ALLAN, 1987).

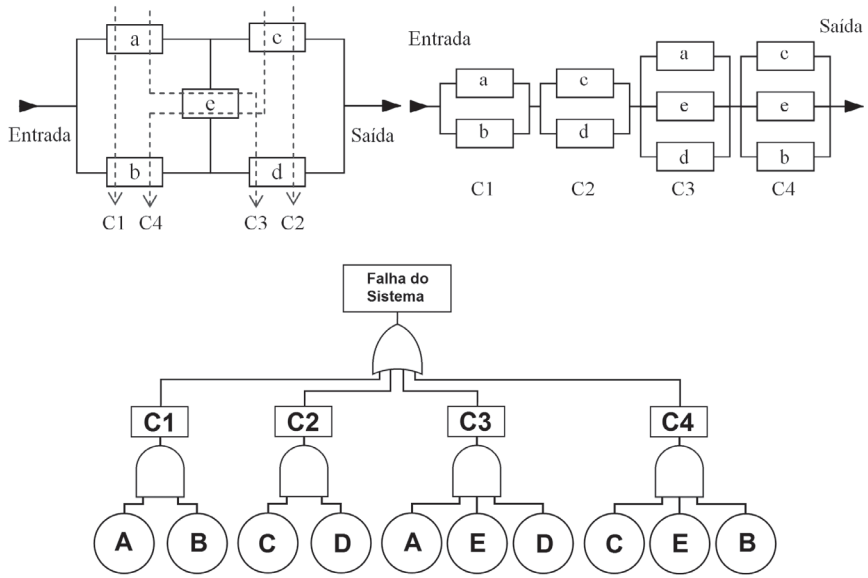


Figura 8.5: Grupo de Corte (BILLINTON e ALLAN, 1987).

Embora os grupos de corte estejam em série, o conceito de sistema série para o cálculo da confiabilidade não pode ser aplicado, porque um mesmo componente aparece em mais de um grupo. Isto mostra que os grupos não são independentes. Esse conceito também deve ser considerado na determinação da probabilidade de falha do sistema, definida pela união das probabilidades de falha de cada um dos grupos conforme a equação 8.2.

$$F_{Sistema} = \text{Probabilidade}(F_{C1} \cup F_{C2} \cup F_{C3} \cup F_{C4}) \qquad (8.2)$$

Onde: F_{Ci} é a probabilidade de falha de cada grupo de corte.

Este método é conveniente para avaliar a probabilidade de falha ou a não confiabilidade do sistema a partir dos grupos de corte. O cálculo da confiabilidade de cada grupo de corte permite identificar os grupos mais críticos, ou mais sensíveis às falhas. A partir daí planeja-se ações para aumentar a robustez do sistema.

8.4.2.2 MÉTODO DO GRUPO DE LIGAÇÃO

O método do Grupo de Ligação (*Tie Set* ou *Path Set*) consiste em dispor em paralelo os grupos de componentes do sistema cuja falha resulta na falha do grupo. Contudo, cada grupo de ligação é constituído de itens ordenados em série. Assim, a falha de um item resulta na falha do grupo, e a falha de todos os grupos resulta na falha do sistema. Os componentes de cada grupo são selecionados passando uma linha paralela ao caminho que liga a entrada à saída do sistema. O método é ilustrado na Figura 8.6, que ilustra também a árvore de falhas resultante da conversão do diagrama de blocos formada pelos grupos de ligação. Neste caso, para a estrutura em ponte representada, foram identificados quatro grupos de ligação (L1, L2, L3 e L4), os quais são conectados em paralelo (BILLINTON e ALLAN, 1987).

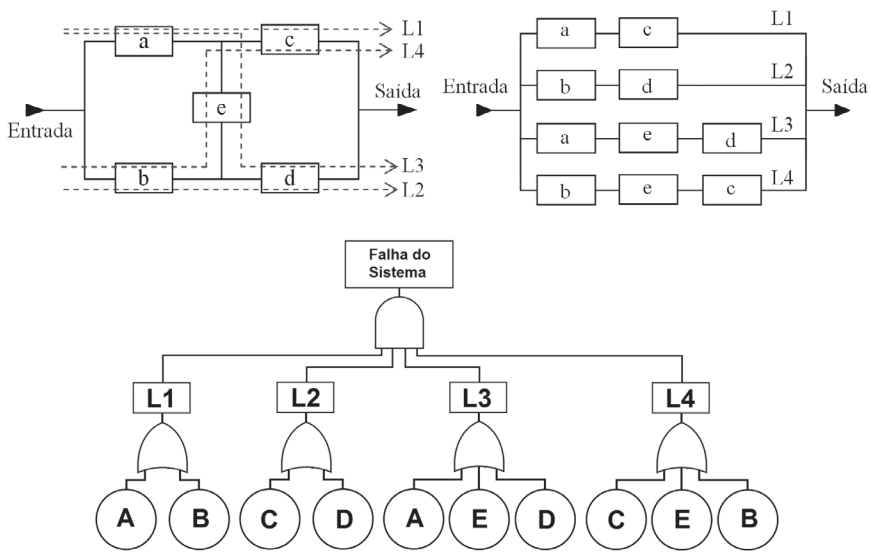


Figura 8.6: Grupo de Ligação (BILLINTON e ALLAN, 1987).

Embora os grupos de ligação estejam em paralelo, o conceito de sistema paralelo para o cálculo da confiabilidade não pode ser aplicado, porque um mesmo componente aparece em mais de um grupo. Isto mostra que os grupos não são independentes. A confiabilidade do sistema ($R_{Sistema}$) pode ser calculada pela equação 8.3.

$$R_{Sistema} = Probabilidade(C_{L1} \cup C_{L2} \cup C_{L3} \cup C_{L4}) \quad 8.3$$

Onde: R_{Li} é a Confiabilidade de cada grupo de ligação.

Este é uma análise recomendável quando se deseja avaliar a confiabilidade de um sistema de segurança. A preocupação é que pelo menos um item continue funcionando.

8.4.3 FTA E FMEA

As técnicas Árvore de Falhas (FTA - *Fault Tree Analysis*), Análise dos Modos de Falha e Efeitos (FMEA - *Failure Modes and Effects Analysis*) e Análise dos Modos de Falha, Efeitos e Criticidade (FMECA - *Failure Modes, Effects and Criticality Analysis*) são técnicas frequentemente utilizadas em conjunto, dado que são normalmente complementares. Observa-se que FMECA é a FMEA com o cálculo da criticidade. Assim, em todo texto será usado apenas a denominação de FMEA.

Enquanto a FTA é mais visual e é possível quantificar as probabilidades de ocorrência ou não de um evento de topo, a FMEA permite detalhar os eventos a partir da função de cada um dos itens do sistema, e os respectivos modos de falha, efeito e criticidade para o produto em análise ou para parte dele.

Na FTA a abordagem é *top-down* (de cima para baixo), ou seja, a análise parte de um evento/efeito indesejado (evento de topo) e investiga associação lógica das causas (causas básicas) que resulta no evento/efeito indesejado. Na FMEA, a abordagem é *bottom-up* (de baixo para cima), ou seja, a análise parte de um modo de falha e investiga os efeitos que a sua ocorrência pode gerar no sistema. A Figura 8.7 exemplifica a relação entre FTA, cuja análise segue na direção das causas, e da FMEA, cuja análise segue na direção dos efeitos.

Figura 8.7: Relação entre FTA e FMEA

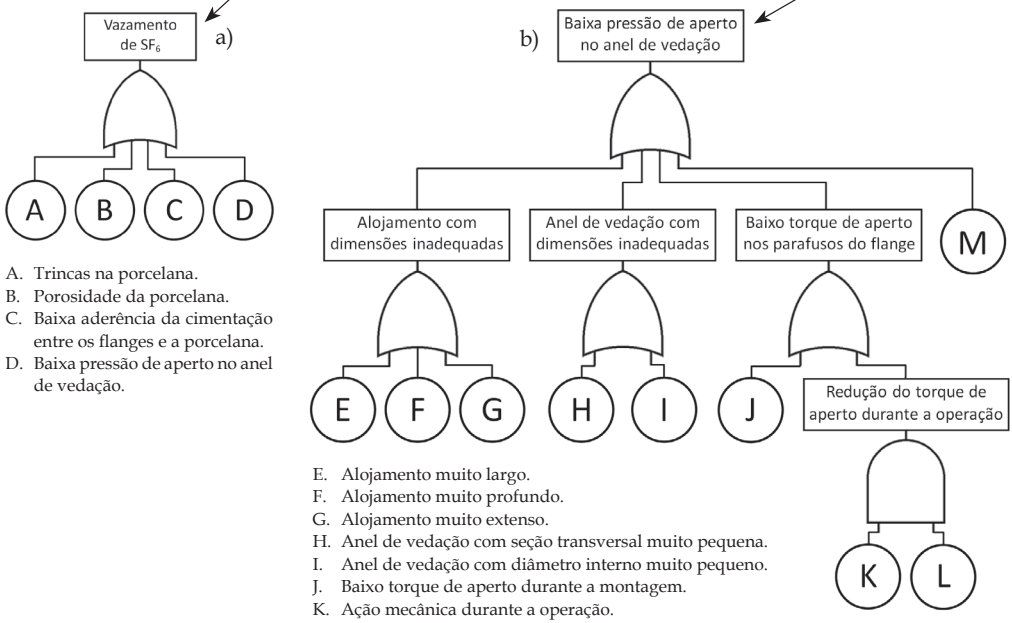
Na abordagem qualitativa, a análise proporcionada pela FMEA relaciona todos os modos de falha, suas causas e efeitos resultantes para o sistema. Já a FTA concentra-se em um único efeito indesejado ou falha (evento de topo) de cada vez para, então, estabelecer o relacionamento lógico de todas as causas básicas que irão resultar no evento de topo, característica não contemplada pela FMEA. Vale salientar que é possível desdobrar, por meio da FTA, qualquer evento ao longo de uma cadeia causal presente na FMEA, e isso significa que um evento de topo pode ser um efeito indesejado, um modo de falha de um componente, ou até mesmo uma causa raiz que se deseja analisar com profundidade. A Figura 8.8 ilustra o desdobramento onde, no caso (a) as causas presentes na planilha de FMEA foram relacionadas logicamente resultando no efeito indesejado (Vazamento de SF_6) tratado como evento de topo. De maneira semelhante cada um dos modos de falha da FMEA poderia ser analisado individualmente como evento de topo resultante do relacionamento lógico das causas presentes na FMEA; no caso (b) uma causa particular (Baixa pressão de aperto no anel de vedação), presente na planilha de FMEA, foi detalhada para elicitação e explicitação do conhecimento relativo às causas básicas daquela causa particular, tratada como evento de topo.

Do ponto de vista quantitativo, na FMEA, o modo de falha é classificado de acordo com a sua criticidade. Estes dois últimos podem estar mais relacionados com as causas. Na FTA, a quantificação se processa pela determinação da probabilidade da ocorrência do evento de topo em função da probabilidade de ocorrência das causas básicas. A

natureza complementar destas ferramentas permite, neste caso, mapear a probabilidade de ocorrência de todos os modos de falha relevantes da FMEA, classificados com altos índices de criticidade ou severidade.

Responsável pela Análise:	Equipe:	Data:
xxxxxxxxxx	NEDIP / UFSC	xx/xx/xxxx
Auditado por:		**Página / De:**
SEMAE / Eletrosul		1/1
Sistema:		**Id_Sistema:**
Disjuntor FA4 Merlin Gerin		DJ1
Subsistema Analisado:		**Id_Subsistema:**
Isolador de Porcelana da Câmara de Extinção: Compartimento que envolve os contatos do circuito principal do disjuntor, capaz de resistir às solicitações devidas ao arco, e destinado a conter o SF_6 e impedir a entrada de umidade no interior da câmara de extinção do disjuntor. No caso do disjuntor FA4 da Merlin Gerin está hermeticamente selada e isolada do cárter, possuindo comunicação com o gás contido na coluna isolante através de tubulação e acoplador flexível.		DJ141

Função	Modo de Falha	Efeito			Causas do Modo de Falha
		Local	Sistema	Planta	
Conter o SF_6, em uma faixa de pressão de 5,5 à 7 bar durante todo o ciclo operacional do disjuntor.	Não consegue conter o SF_6.	Vazamento de SF_6.	Redução da pressão interna do SF_6. Explosão da Câmara de Extinção.	Impossibilidade de operação do disjuntor. Danos em equipamentos próximos.	Trincas na porcelana. Porosidade da porcelana. Baixa aderência da cimentação entre os flanges e a porcelana. Baixa pressão de aperto no anel de vedação.



A. Trincas na porcelana.
B. Porosidade da porcelana.
C. Baixa aderência da cimentação entre os flanges e a porcelana.
D. Baixa pressão de aperto no anel de vedação.

E. Alojamento muito largo.
F. Alojamento muito profundo.
G. Alojamento muito extenso.
H. Anel de vedação com seção transversal muito pequena.
I. Anel de vedação com diâmetro interno muito pequeno.
J. Baixo torque de aperto durante a montagem.
K. Ação mecânica durante a operação.
L. Falta de trava mecânica ou química nos parafusos do flange.
M. Jogo diametral – folga entre as peça acima do especificado.

Figura 8.8: FTA como elementar complementar a FMEA.

Independentemente da abordagem (qualitativa e/ou quantitativa), a FMEA/ e a FTA podem ser utilizadas de maneira complementar para facilitar a análise, detalhar pontos de interesse e/ou validar o conhecimento (HELMAN & ANDERY, 1995 e SCAPIN, 1999). Ambas as ferramentas são amplamente aplicadas em análises de confiabilidade e citadas textualmente nas normas ISO 9000 e em particular na ISO 9004 (2009), subitem 8.4 (Qualificação e Validação de Projeto).

8.4.4 FTA E ETA

A Árvore de Eventos (ETA - *Event Tree Analysis*) é uma técnica indutiva de análise dos possíveis resultados (saídas ou efeitos para o sistema) decorrentes de um evento inicial próprio para descrição de cenários que envolvam sistemas técnicos, ambiente e/ou eventos humanos. Quando se relacionada com a FTA, é possível, ou melhor, facilita a explicitação de determinar a causa básica que foi geradora, ou a principal geradora do evento de saída, ou de topo.

Uma combinação de FTA - ETA - FMEA está ilustrada na Figura 8.9, onde, na parte superior da figura tem-se uma planilha de FMEA que identifica a função a ser analisada, o modo de falha e os efeitos em nível local do disjuntor, no sistema, na planta e a descrição das causas.

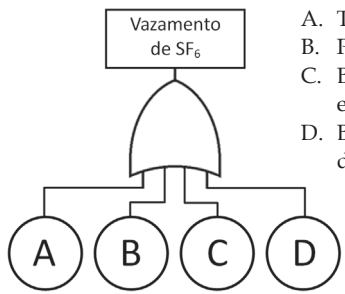
Para um melhor detalhamento do efeito em nível local no disjuntor, aplicou-se uma análise a partir da árvore de eventos (ETA) com o fim de obter os cenários possíveis a partir do evento iniciante até o estado geral da planta. O diferencial em relação ao FMEA está no fato de poder quantificar cada um dos cenários em termos de probabilidade de ocorrência. Observa-se que a partir do evento iniciante, cada um dos eventos subsequentes é mutuamente exclusivo. Ou seja, ou está na condição sucesso ou insucesso em relação à função que deve cumprir no sistema.

Assim, para analisar os casos de insucesso, ou falha, utiliza-se uma árvore de falha (FTA) para melhor estudar a relação entre o evento de topo (falha) e as causas que contribuíram para a ocorrência do evento.

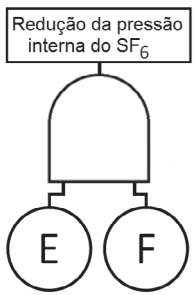
Responsável pela Análise:	Equipe:	Data:
xxxxxxxxxx	NEDIP / UFSC	xx/xx/xxxx
Auditado por:		**Página / De:**
SEMAE / Eletrosul		1/1
Sistema:		**Id_Sistema:**
Disjuntor FA4 Merlin Gerin		DJ1
Subsistema Analisado:		**Id_Subsistema:**
Isolador de Porcelana da Câmara de Extinção: Compartimento que envolve os contatos do circuito principal do disjuntor, capaz de resistir às solicitações devidas ao arco, e destinado a conter o SF_6 e impedir a entrada de umidade no interior da câmara de extinção do disjuntor. No caso do disjuntor FA4 da Merlin Gerin está hermeticamente selada e isolada do cárter, possuindo comunicação com o gás contido na coluna isolante através de tubulação e acoplador flexível.		DJ141

Função	Modo de Falha	Efeito			Causas do Modo de Falha
		Local	Sistema	Planta	
Conter o SF_6, em uma faixa de pressão de 5,5 à 7 bar durante todo o ciclo operacional do disjuntor.	Não consegue conter o SF_6.	Vazamento de SF_6.	Redução da pressão interna do SF_6. Explosão da Câmara de Extinção.	Impossibilidade de operação do disjuntor. Danos em equipamentos próximos.	Trincas na porcelana. Porosidade da porcelana. Baixa aderência da cimentação entre os flanges e a porcelana. Baixa pressão de aperto no anel de vedação.

Evento Iniciante	Redução da pressão interna do SF_6	Abertura do disjuntor	Estado da Planta	Combinação de Eventos
VSF6 Vazamento de SF_6	Sim (RP)	Sim (AD)	Desligamento de circuitos e impossibilidade de nova operação do disjuntor (fechamento).	$VSF6 \cap RP \cap AD$
		Não $(\overline{AD})$	Possibilidade de explosão do disjuntor e danos em equipamentos próximos durante uma abertura forçada com baixa pressão de SF_6.	$VSF6 \cap RP \cap \overline{AD}$
	Não $(\overline{RP})$	Sim (AD)	Desligamento de circuitos e bloqueio de nova operação do disjuntor (fechamento).	$VSF6 \cap \overline{RP} \cap AD$
		Não $(\overline{AD})$	Consumo excessivo de SF_6 para manutenção da pressão interna.	$VSF6 \cap \overline{RP} \cap \overline{AD}$



A. Trincas na porcelana.
B. Porosidade da porcelana.
C. Baixa aderência da cimentação entre os flanges e a porcelana.
D. Baixa pressão de aperto no anel de vedação.



E. Perda de estanqueidade.
F. Falha na complementação do SF_6 para manutenção da pressão interna.

Figura 8.9: Exemplo de utilização das técnicas FTA – ETA – FMEA para aprofundar análise de falhas em sistemas

8.5 CONSIDERAÇÕES FINAIS

Além dos conceitos abordados neste capítulo, cabe ressaltar a utilização da FTA como ferramenta de comunicação visual. É utilizada para explicitar os caminhos das causas até o evento de falha, e, devido a distribuição dos eventos, torna-se muito didática, facilitando a compreensão durante os processos de capacitação. Para isso deve-se procurar manter a representação simplificada, uma vez que facilita o entendimento do sistema e oportuniza melhorias.

A interação facilitada com outras ferramentas, aliada à sua abordagem sistêmica, torna a FTA especialmente útil para apoio às atividades de manutenção, tanto para tratamento da informação e explicitação do conhecimento quanto para priorização de ações corretivas e preventivas.

A interação lógica entre as causas básicas pode auxiliar a análise detalhada de problemas inerentes ao desenvolvimento de produtos ou processos, auxiliando a tomada de decisão por ocasião da implementação de redundâncias, simplificações, aperfeiçoamentos e demais ações com o objetivo de solucionar problemas que possam impactar negativamente o produto.

A FTA permite analisar e projetar sistemas de segurança, identificar componentes críticos ou condições críticas de operação, além de, organizar a informação para auxiliar o treinamento na operação de equipamentos, testes e inspeções.

É importante destacar que a FTA também é utillizada para racionaliar o conhecimento. É uma forma explícita de abstrair o conhecimento da equipe de projeto ou de manutenção em relação aos eventos de falha que ocorrem num item. Item, aqui, é entendido como sistema, subsistema, ou mesmo componente. O resultado das análise a partir da FTA pode ser usado como memória organizacional, para ser recuperada a qualquer momento, seja para rever a solução adotada, para utilizar como exemplo ou para agregar melhorias.

De outro modo, a técnica é também utilizada para testar o conhecimento da equipe em relação a um dado processo de falha, ou análise de um sistema que está em operação, visando organizar programas de capacitação.

Como qualquer outra técnica, a mesma tem que estar coerente com o que está operando, ou seja, o próprio sistema físico. Assim,

dado a dinâmica dos sistemas técnicos, a cada atualização tecnológica há que também atualizar o FTA correspondente, no que se refere à relação causas e efeitos. Contudo, para as organizações com baixa mobilidade de pessoal (*turn-over*), os processos de atualização tornam-se simples, rápidos e mais completos.

Capítulo 9

ANÁLISE POR ÁRVORE DE EVENTOS (ETA)

A técnica de análise por Árvore de Evento (*ETA - Event Tree Analysis*) foi desenvolvida no início dos anos 70 para apoiar o desenvolvimento de análises de risco em centrais nucleares, e, atualmente, é utilizada nas mais diversas áreas (ERICSON, 2005). Trata-se de uma técnica indutiva de análise dos possíveis resultados (saídas ou efeitos para o sistema) decorrentes de um evento inicial, chamado de "evento inicializador" (normalmente um acidente ou fato indesejado) levando-se em consideração as barreiras de segurança, eventos complementares e/ou fatores externos.

A ETA pode ser utilizada tanto para análise qualitativa quanto quantitativa. Na análise qualitativa, o foco é a possibilidade de se visualizar os eventos e sua interação. No caso da análise quantitativa, as probabilidades de ocorrência de cada evento são incluídas na análise, o que permite calcular a probabilidade de ocorrência de explicação de um cenário.

A árvore de eventos é útil para a descrição de cenários proporcionados pelos eventos de origem distinta. Ou seja, permite associar a probabilidade de ocorrência de eventos de falha do sistema técnico com eventos da natureza ou de ações humanas na estimativa um cenário.

9.1 DEFINIÇÕES E CONCEITOS SOBRE ETA

A ETA é particularmente adequada para análises de risco e de sistemas onde haja a interação entre diversos tipos de eventos, entre outros: falha de um componente, intervenção humana, fenômeno ambiental ou falha de *software*. A sequência de acontecimentos/resultados referente às diversas interações possíveis entre os eventos que compõem a ETA é chamada de cenário e seus eventos constituintes são, na maioria das vezes, independentes, podendo ainda ser sequen-

ciais ou não. Dois eventos são independentes se a ocorrência de um não afeta a probabilidade de ocorrência do outro. Assim, dados os eventos A e B, tem-se:

$$P(B \mid A) = P(B) \text{ e } P(B \cap A) = P(A) \cdot P(B) \qquad 9.1$$

Eventos sequenciais são aqueles que respeitam uma ordem de ocorrência. Assim, por exemplo, o evento B só poderia ocorrer se o evento A tivesse ocorrido. No caso de se delinear uma ETA com eventos sequenciais, não existiria a imposição de que eles sejam independentes. Contudo, deve-se levar em consideração as probabilidades condicionais, conforme apresentado na Figura 9.1. Nesta figura a simbologia (a, b, c) indica a ocorrência dos eventos A, B e C respectivamente, enquanto que a simbologia ($\bar{b}$, $\bar{c}$) indica a não ocorrência dos eventos B e C, na configuração dos respectivos cenários indicados.

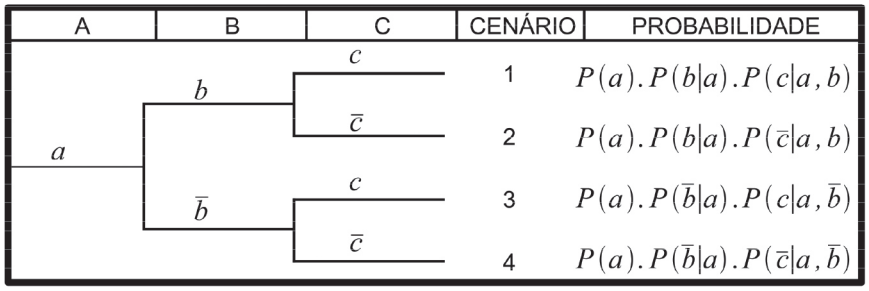


Figura 9.1: ETA de eventos sequenciais, onde o evento A é o evento inicializador

A probabilidade de ocorrência de cada cenário leva em consideração as dependências entre os eventos. No caso dos eventos serem independentes, ilustrado na Figura 9.2, tem-se:

$$P(B \mid A) = P(B) \text{ e } P(C \mid B, A) = P(C) \qquad (9.1)$$

Assim, a ordem em que os eventos ocorrem é irrelevante, pois a probabilidade de ocorrência de cada cenário não seria modificada, por exemplo: $P(A) \cdot P(B) \cdot P(C) = P(A) \cdot P(C) \cdot P(B)$. Resumindo:

- Se os eventos são independentes podem ou não ser sequenciais;
- Se os eventos são dependentes, obrigatoriamente, devem ser sequenciais.

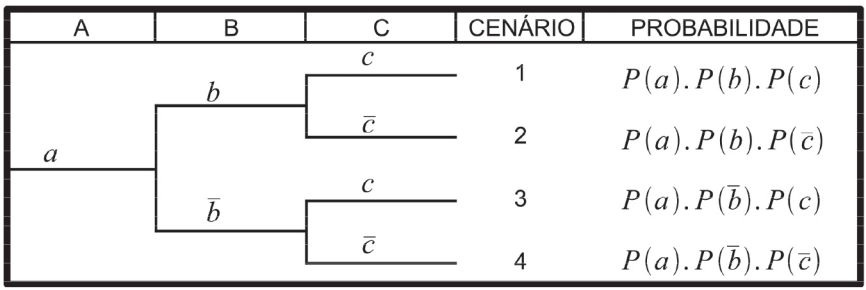


Figura 9.2: ETA de eventos independentes, onde o evento A é o inicializador.

A ocorrência de um cenário indesejado pode ser entendida como a quebra de uma barreira de segurança ou dos mecanismos que impedem a sua ocorrência. Tais barreiras são utilizadas para impedir a interação entre os diversos eventos (relativos aos sistemas técnicos, erros humanos, fatores ambientais etc.) que corroboram para a ocorrência do cenário indesejado ou para impedir os efeitos decorrentes do cenário indesejado, conforme apresentado na Figura 9.3.

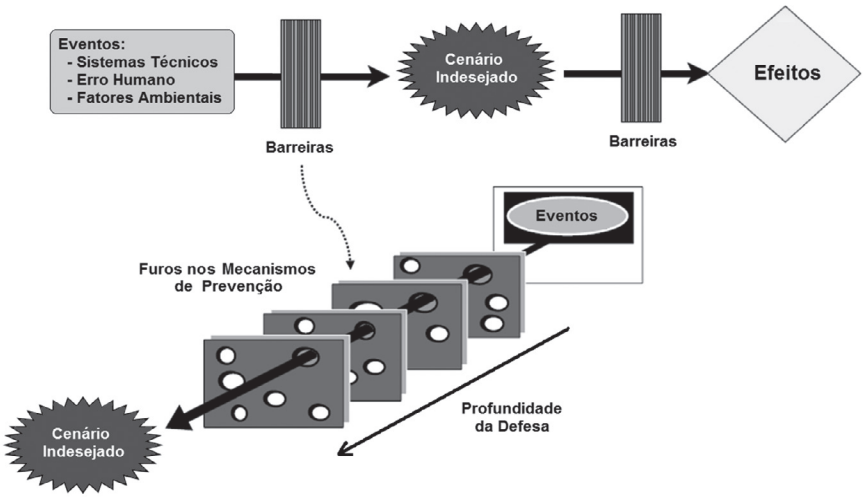


Figura 9.3: Eventos, cenário indesejado e barreiras de proteção.

Como exemplo de barreiras interpostas para evitar um cenário indesejado tem-se: barreiras físicas, procedimentos, manuais, educação, leis, capacitação, motivação ou qualquer medida que vise atuar na corrente causal evitando o cenário indesejado ou os seus efeitos. No entanto, as barreiras não são perfeitas e seus "furos", quer seja por uma falha ativa ou por uma condição latente, permitem que o cenário indesejado ou os seus efeitos ocorram. Para reduzir a probabilidade de ocorrência de um cenário indesejado ou mitigar suas consequências/efeitos, recomenda-se a adoção de mais de uma barreira, o que, segundo Reason (1997), resulta em agir na "profundidade da defesa".

9.2 METODOLOGIA PARA APLICAÇÃO DA ETA

Para aplicação da ETA, a análise parte de um evento inicial tomado como referência, o qual pode ser, por exemplo: uma falha no sistema técnico, um erro humano ou fatores ambientais (Figura 9.3). A partir do evento inicializador se estabelece as combinações dos eventos cuja interação desencadeará um determinado resultado ou cenário. Usualmente, a ETA é modelada com eventos cujo estado são binários, os quais podem ser assumidos como "presentes" ou "não presentes" na cadeia causal que resultará no cenário a ser analisado. Assim, o número de resultados ou cenários obtidos será igual a 2^n, onde "n" é o número de eventos representados na ETA. Quando há eventos com mais de dois possíveis estados, pode-se, ainda, utilizar o artifício de agrupar resultados, chamando-os de sucesso (favoráveis) ou falha (desfavorável). O Exemplo da Figura 9.4 ilustra o processo de delineamento de cenários utilizando a ETA, apresentado por Kumamoto & Henley (1996).

Exemplo 9.1: Suponha um vaso de pressão alimentado por um compressor, conforme a Figura 9.4. O processo se inicia quando o operador, manualmente, zera o contador de tempo (*timer*). Assim, os contatos do *timer* se fecham e o motor do compressor é alimentado. Em série com os contatos do *timer* existe uma chave, normalmente fechada, de acionamento manual. Para não haver ruptura do vaso de pressão, o *timer* é regulado para abrir antes de qualquer possível sobrepressão. Caso o *timer* não desligue o motor do compressor, o operador é instruído para abrir a chave manual, resultando

na parada do compressor, sempre que observar sobrepressão por meio do manômetro. O vaso de pressão possui, ainda, uma válvula de alívio que se abre antes de ocorrer ruptura de sua estrutura, para o caso de falha simultânea do *timer* e do operador.

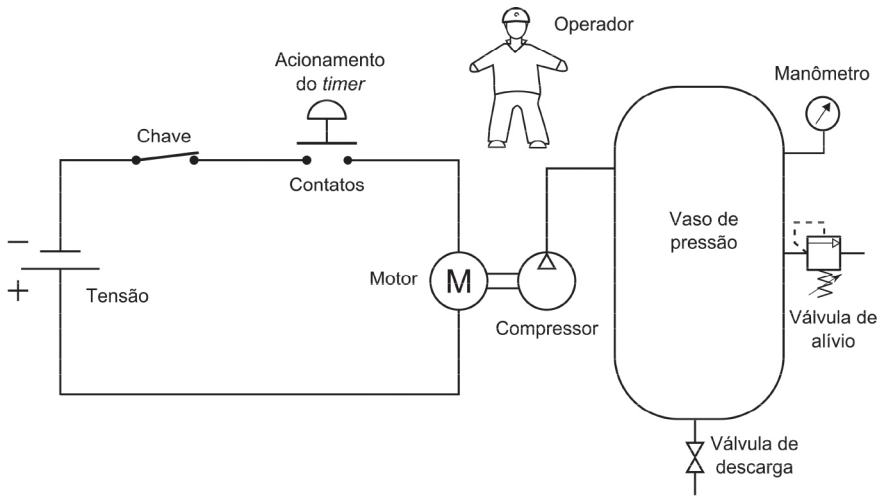


Figura 9.4: Diagrama do sistema de pressurização do vaso de pressão (Adaptada de Kumamoto & Henley (1996))

Para montar a árvore de eventos os seguintes passos devem ser seguidos:

- Identificar o evento inicializador;
- Identificar os eventos que podem influenciar (positivamente ou negativamente) para que o evento inicial desencadeie nos cenários a serem analisados;
- Estruturar a árvore seguindo uma lógica de acontecimentos que podem surgir a partir do evento inicial;
- Simplificar a árvore de eventos; e
- Uma vez construída a árvore de eventos, calcular a probabilidade de ocorrência de cada cenário delineado (se aplicável) a partir da probabilidade de ocorrência de cada evento.

9.2.1 IDENTIFICAÇÃO DO EVENTO INICIALIZADOR

A identificação do evento inicializador é fundamental, pois é a partir da interação deste evento com outros subsequentes que se

desencadeará um determinado resultado ou cenário. A partir da análise de tais cenários serão inventariados os perfis do risco na análise probabilística (*Probabilistic risk assessment* - PRA). É necessária uma compreensão das funções e das características gerais de segurança do sistema para fornecer a informação inicial necessária para selecionar e agrupar os eventos iniciais.

Duas aproximações podem ser feitas para identificar eventos iniciais. A primeira é uma avaliação geral de engenharia, a partir de históricos dos eventos e levantamento de experiências adquiridas. As informações são analisadas e uma lista de eventos (inicializadores ou não) é gerada. A segunda é uma aproximação mais formal. Isso inclui técnicas como listas de verificação, análise do modo de falha e dos efeitos (FMEA), estudo do perigo operacional (HAZOP - *hazard and operability studies*), entre outros. Embora estas técnicas não sejam usadas exclusivamente para a identificação do evento inicial, também são úteis no processo. No exemplo utilizado neste capítulo, o evento inicializador é o "motor do compressor permanece ligado" quando já deveria estar desligado. Em outras palavras, falha do sensor de tempo (FT- falha de *timer*).

9.2.2 LISTA DOS EVENTOS QUE INFLUENCIARAM OS CENÁRIOS DA ETA

Identificado o evento inicializador da ETA, lista-se os eventos subsequentes, também chamados pivotais, cuja interação entre si e com o evento inicializador compõe-se os cenários a serem analisados. Esses eventos podem ser: falhas nas barreiras interpostas na tentativa de coibir um acidente ou mitigar suas consequências; eventos que aumentam as proporções do acidente; ou que propiciam uma condição perigosa que, aliadas ao evento inicializador (evento gatilho), resultariam em acidente. Assim, é fundamental que se conheça bem a situação em que está envolvida a análise. Recomenda-se que seja elaborada uma lista dos eventos que podem influenciar nos cenários. Desta lista, extraem-se os eventos relevantes para a análise que passam a integrar a ETA.

9.2.3 ESTRUTURAÇÃO DA ÁRVORE DE EVENTOS

A Figura 9.5 mostra a árvore de eventos completa para o Exemplo 9.1, referente à análise dos cenários que resultam na ruptura do vaso de pressão.

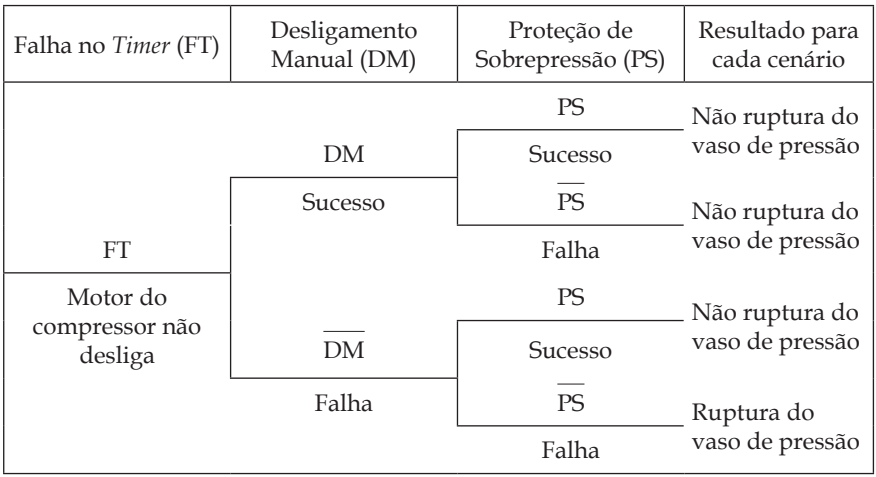


Figura 9.5: Árvore de eventos completa com os cenários resultantes para o Exemplo 9.1.

Tomado como evento inicial a falha do *timer* (FT), o qual pode causar a impossibilidade de desligamento do motor do compressor (motor do compressor não desliga), lista-se os eventos que podem resultar no cenário de ruptura ou não do vaso de pressão. São eles:

- Operador desligar o motor do compressor (desligamento manual - DM);
- Proteção de sobrepressão é acionada (proteção de sobrepressão - PS).

Analisa-se, então, o sucesso (parte superior da árvore de eventos) e falha (parte inferior da árvore de eventos) de cada um dos eventos e o impacto obtido no resultado final do processo. Note-se que os dois eventos de proteção são no sentido de evitar a ocorrência do acidente, portanto, são barreiras na corrente causal. O evento poderia, também, estar relacionado a uma condição perigosa, como, por exemplo, a existência de uma espessura reduzida na parede do

vaso de pressão que poderia provocar a ruptura do mesmo, sem que uma sobrepressão efetivamente ocorresse.

9.2.4 SIMPLIFICAÇÃO DA ÁRVORE DE EVENTOS

A simplificação da árvore de eventos traz uma visualização mais rápida dos cenários de acordo com a ocorrência de cada evento. Para simplificar a árvore de eventos, deve-se ter a certeza de que a partir do evento no qual a árvore foi simplificada (eventos subsequentes eliminados) até o fim dos eventos, não haveria qualquer alteração no resultado final, ou seja, independentemente do que acontecer nos eventos subsequentes, aquele resultado é atingido da mesma forma. Para o Exemplo 9.1, a árvore simplificada está apresentada na Figura 9.6.

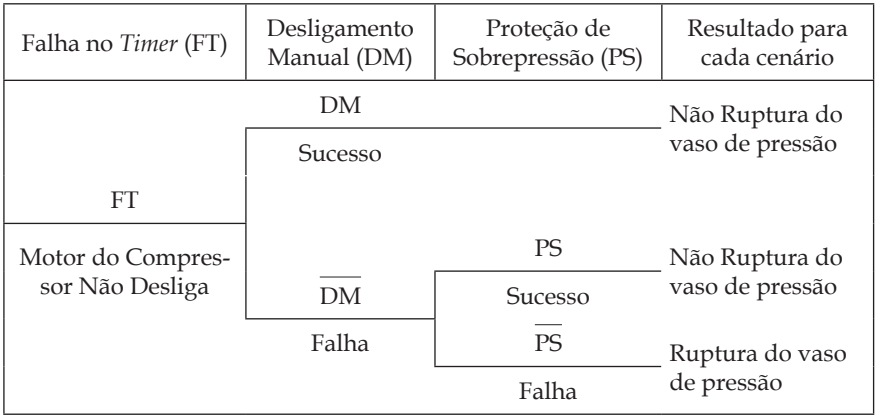


Figura 9.6: Árvore de eventos simplificada do Exemplo 9.1.

Da Figura 9.6 é possível depreender que, a partir do momento que o operador desliga o motor do compressor (Desligamento Manual - DM), não importa se a proteção de sobrepressão (Proteção de Sobrepressão - PS) falhe ou não, o vaso de pressão não irá romper. Portanto, na Figura 9.6 simplifica-se a árvore a partir do evento (Desligamento Manual - DM). De fato, no caso do operador desligar o motor do compressor, a proteção de sobrepressão perde a função. Contudo, observa-se, que muitas vezes, uma situação como esta pode levar a uma falha oculta. Ou seja, se a proteção falhar enquanto o

compressor estiver desligado, não se saberá até que se acione a proteção. Esta consideração é difícil de visualizar na ETA.

9.2.5 CÁLCULO DA PROBABILIDADE DE CADA CENÁRIO

Tendo as probabilidades individuais dos eventos, é possível proceder com a análise quantitativa de cada cenário da ETA. Neste contexto, se os eventos forem dependentes há que se considerar a probabilidade condicional dos eventos que compõem cada cenário, assim, para se determinar a probabilidade de ocorrência dos eventos subsequentes deve-se considerar a probabilidade de ocorrência dos eventos antecedentes. Caso os eventos sejam independentes, a probabilidade de ocorrência de cada cenário pode ser determinada pelo produto das probabilidades individuais dos eventos que compõem cada cenário.

Para o Exemplo 9.1, e com base na Figura 9.5, considera-se como evento inicializador a Falha no *Timer* (FT), a independência dos eventos e supõe-se que a probabilidade de cada evento ter sucesso é de 95%. A probabilidade de ocorrência dos cenários analisados pode ser determinada conforme a Figura 9.7, que são divididos em dois: probabilidade de não ruptura e probabilidade de ruptura do vaso de pressão.

Falha no *Timer* (FT)	Desligamento Manual (DM)	Proteção de Sobrepressão (PS)	Resultado para cada cenário	Probabilidade de Ocorrência do Cenário
FT = 1,0	DM = 0,95	PS = 0,95	1) Não Ruptura do vaso de pressão	P1=1,0x0,95x0,95=0,9025
	Sucesso	Sucesso		
		$\overline{PS}$ = 0,05	2) Não Ruptura do vaso de pressão	P2=1,0x0,95x0,05=0,0475
		Falha		
Motor do Compressor Não Desliga	$\overline{DM}$ = 0,05	PS = 0,95	3) Não Ruptura do vaso de pressão	P3=1,0x0,05x0,95=0,0475
	Falha	Sucesso		
		$\overline{PS}$ = 0,05	4) Ruptura do vaso de pressão	P1=1,0x0,05x0,05=0,0025
		Falha		

Figura 9.7: Análise quantitativa da árvore de eventos do Exemplo 9.1.

Observa-se que para o cálculo de probabilidade de não ocorrência da ruptura é obtido com o somatório das probabilidades de cada um dos cenários descritos nos caminhos que levam a chance de não romper. Ou seja, no caso P1 tem chance de "não ruptura" de 90,25%, em P2 e P3 a chance de "não ruptura" é de 4,75% para cada. Assim, a chance de "não ruptura" para esta configuração é de 99,75%.

Já no caso P4, a chance de ocorrência de ruptura é de 0,25%, sendo o único caso em que pode ocorrer ruptura do vaso de pressão, e, para que isso seja possível, considera-se que após a falha no *timer* deve haver a falha no desligamento manual (DM) e na proteção de sobrepressão (PS).

9.3 CONSIDERAÇÕES FINAIS

Uma das vantagens de se utilizar a ETA é a flexibilidade de poder realizar a análise da ocorrência dos cenários de forma qualitativa e quantitativa. Ademais, a técnica possibilita uma boa representação do conhecimento, o que facilita a comunicação entre os analistas.

Para sistemas críticos, somente o conhecimento das probabilidades das falhas não é suficiente, pois é necessário ter conhecimento das possíveis cenários de falhas para elaborar barreiras que possam impedir a ocorrência delas, como dispositivos de proteção, capacitação dos colaboradores, alarmes, entre outros elementos.

Como desvantagem, pode ocorrer que, no desenvolvimento da árvore, existam muitos eventos que levem a geração de muitas ramificações, tornando o processo de análise mais difícil. No entanto, esse problema é reduzido agrupando os cenários de interesse, simplificando e reduzindo o tamanho da árvore a partir da técnica de simplificação. Em contrapartida, deve-se ter o cuidado para não descartar cenários de falhas importantes, os quais podem conduzir o sistema para estados inesperados, e consequentemente, a uma falha catastrófica.

Além do fato de permitir os cálculos das probabilidades, a técnica fornece ao analista outros referenciais a partir dos resultados das probabilidades. Em si, todos os sistemas têm chance de acontecer. A probabilidade de acontecer dependem das variáveis probabilísticas que se dispõe no instante da análise.

O grande atributo da técnica ETA está no princípio de estabelecer sinergia entre os eventos de falha de natureza técnica com os de natureza ambiental e/ou humana. Permite o analista visualizar o problema de forma mais integrada e ao mesmo tempo holística, portanto, com mais chance de empreender soluções para o sistema nas várias dimensões que é requerido, como é comum em sistemas complexos.

Capítulo 10

REDES BAYESIANAS

Redes bayesianas são modelos gráficos utilizados para avaliar a probabilidade de ocorrência de vários eventos simultaneamente. Em outras palavras, servem para analisar o comportamento de um conjunto de variáveis aleatórias. Para isso, associam aos modelos gráficos um conjunto de probabilidades que estabelecem as relações entre os eventos.

A Figura 10.1 é um exemplo de rede bayesiana com três eventos, também denominados de variáveis ou nódulos. O diagrama indica que existe uma relação dos eventos A e B com o evento C, sendo que a intensidade das relações entre as variáveis é estabelecida por probabilidades condicionais.

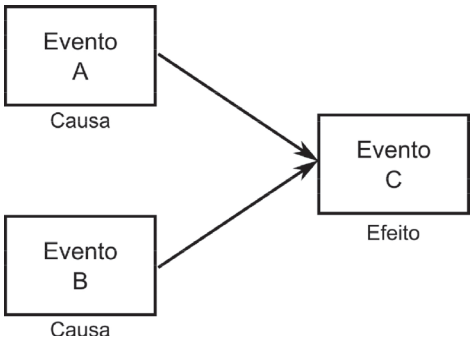


Figura 10.1 Exemplo de rede

Assim, as redes bayesianas auxiliam no mapeamento de causas e efeitos, orientando as decisões e predições, mesmo na ausência de algumas informações, pois os modelos desenvolvidos com essas redes são melhorados à medida em que são fornecidas informações mais precisas, o que é conhecido por "aprendizagem da rede". As redes bayesianas são utilizadas em análise de risco por permitirem analisar

a ocorrência dos vários eventos de falha, no cálculo da probabilidade dos mesmos causarem um incidente. Pode-se ainda associar a opinião dos especialistas sobre o processo de análise. É conveniente para o desenvolvimento de ferramentas computacionais, pois possui um formalismo bem estruturado.

10.1 CONSIDERAÇÕES SOBRE REDES BAYESIANAS

O termo redes bayesianas pode induzir a pensar que todas as redes bayesianas utilizam o teorema de Bayes nos cálculos de probabilidade. No entanto, em alguns casos, os cálculos podem ser feitos usando regras de probabilidade condicional de maneira direta. Isto ocorre porque as redes são utilizadas tanto para raciocínio preditivo (das causas para os efeitos, também chamado de encadeamento direto) quanto para raciocínio de diagnóstico (ou encadeamento reverso, dos efeitos para as causas).

10.1.1 PROBABILIDADE CONDICIONAL

Para compreender o que é uma probabilidade condicional é necessário inicialmente entender o que são eventos condicionais. Um evento é dito condicional, quando a sua probabilidade de ocorrência é alterada por outros eventos.

Por exemplo, considere dois eventos A e B dentro de um domínio de possíveis resultados S. Deseja-se saber qual a probabilidade de ocorrer A, dado que B tenha ocorrido, ou seja $P(A \mid B)$. Isso fica mais claro partindo da análise de um diagrama de Venn, Figura 10.2, onde A e B são dois eventos não mutuamente exclusivos[1].

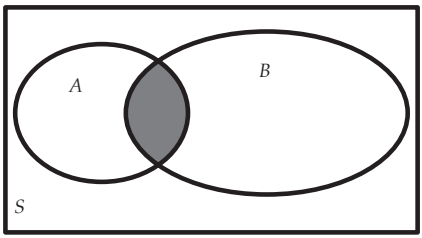


Figura 10.2 Eventos não mutuamente exclusivos

[1] Note-se que $P(A \mid B) = 0$, para eventos mutuamente exclusivos.

A partir disso, pode-se fazer a seguinte consideração: dado que B tenha ocorrido, existe uma probabilidade do evento A também ocorrer, que pode ser calculada com a equação 10.1.

$$P(A \mid B) = \frac{P(A,B)}{P(B)} \tag{10.1}$$

Onde,

$P(A,B)$ é a probabilidade de A e B ocorrer (intersecção),

$P(B)$ é a probabilidade de B ocorrer.

Na análise condicional, quando se afirma que o evento B ocorreu, o domínio de possíveis resultados fica reduzido, passa de S para B. Assim, $P(A \mid B)$ é uma proporção de eventos A que ocorrem dentro do domínio B. A Figura 10.2 ilustra essa transformação de domínios.

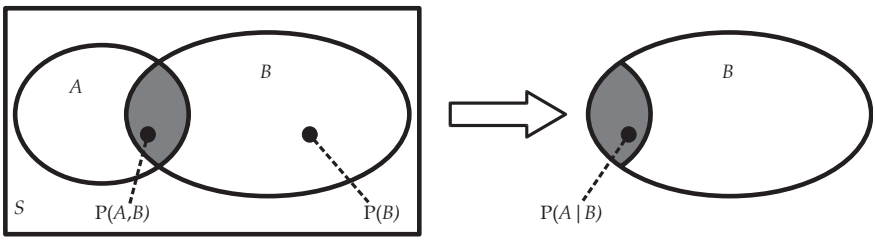


Figura 10.3 Probabilidade condicional $P(A \mid B)$

10.1.2 TEOREMA DE BAYES

O reverendo Thomas Bayes (1702 – 1761) era um matemático amador que teve poucos trabalhos publicados. Seu texto mais ilustre, *Essay towards solving a problem in the doctrine of chances*, foi publicado em 1763 (portanto, após sua morte), no Philosophical Transactions of the Royal Society of London, por seu amigo Richard Price. Nesse texto, é apresentado um caso especial do que é hoje denominado teorema de Bayes, apresentado em 1774 por Pierre-Simon Laplace, no texto *Mémoire sur la probabilité des causes par les événements* (FIENBERG, 2006).

O teorema de Bayes abriu novas possibilidades dentro da estatística e hoje é considerado como sendo uma abordagem distinta. Na abordagem clássica, também denominada de frequencista, a inferência é feita com base exclusivamente em dados experimentais. O que distingue a abordagem bayesiana é que a mesma possibilita utilizar – além

dos dados experimentais – o conhecimento prévio, mesmo que subjetivo. O teorema de Bayes fundamenta-se na teoria de probabilidade condicional. Assim, reescrevendo a equação 10.1, tem-se:

$$P(A,B) = P(A \mid B).P(B) \tag{10.2}$$

Isto é: a probabilidade de ocorrerem os dois eventos A e B (probabilidade conjunta) é igual à probabilidade de ocorrer o evento A dado que ocorreu o evento B, multiplicado pela probabilidade de ocorrer o evento B. De forma análoga, pode-se equacionar a probabilidade conjunta, dado que o evento A ocorreu primeiro.

$$P(A,B) = P(B \mid A).P(A) \tag{10.3}$$

Substituindo a Equação 10.2 na 10.3, chega-se à tradicional equação de Bayes:

$$P(B \mid A) = \frac{P(A \mid B).P(B)}{P(A)} \tag{10.4}$$

Onde $P(A)$ é denominada de "probabilidade marginal", e pode ser expandida usando o "teorema da probabilidade total", para o caso dos eventos B_i serem exaustivos e mutuamente exclusivos:

$$P(A) = \sum_{i=1}^{n} P(A \mid B_i).P(B_i) \tag{10.5}$$

O que resulta na seguinte equação:

$$P(B \mid A) = \frac{P(A \mid B).P(B)}{\sum_{i-1}^{n} P(A \mid B_i).P(B_i)} \tag{10.6}$$

A mesma equação pode se escrita em termos de distribuição de densidade de probabilidade.

$$f(\theta \mid x) = \frac{f(x \mid \theta).f(\theta)}{\int_{-\infty}^{\infty} f(x \mid \theta).f(\theta).d\theta} \tag{10.7}$$

Outra forma de apresentar a equação acima é omitindo o denominador do lado direito da equação, já que não depende de θ.

$$f(\theta \mid x) \propto f(x \mid \theta).f(\theta) \tag{10.8}$$

A expressão 10.8 pode ser lida como a distribuição *a posteriori* é proporcional à "verossimilhança" multiplicado pela função *a priori*.

Para ilustrar o uso da abordagem bayesiana, suponha que alguém está participando de um programa de televisão, no qual se deve escolher uma de três portas disponíveis[2]. Atrás de uma das portas tem um carro, e, das outras, pequenos prêmios de consolação. Assim, a probabilidade do carro estar em uma determinada porta é de $^1/_3$, i.e.:

$$p(A) = \frac{1}{3},\ p(B) = \frac{1}{3}\ e\ p(C) = \frac{1}{3} \tag{10.9}$$

Após escolher uma das portas, o apresentador do programa – que sabe onde está o carro – diz que dará mais uma oportunidade. Neste momento, o apresentador abre uma das outras duas portas (que tem um prêmio de consolação) e permite que seja revista a opção inicial.

Por exemplo: suponha que alguém tenha escolhido a Porta A e que o apresentador tenha aberto a Porta B. Neste caso, a pessoa poderia permanecer com a opção da Porta A ou trocar para a Porta C. O que deveria ser feito?

Se não for feita uma análise mais cuidadosa da situação, pode-se ter a impressão de que – quando o apresentador deixa apenas duas portas fechadas – a chance do carro estar em uma das portas seria de 50%.

Todavia, é possível demonstrar que é estatisticamente mais interessante alterar a opção para a Porta C – o que será apresentado a seguir.

Para o exemplo corrente, pode-se analisar a probabilidade do apresentador (Ap.) abrir a Porta B por meio de três probabilidades condicionais:

---

2 Chamado de Paradoxo de Monty Hall (que foi um célebre apresentador).

- A probabilidade de abrir a Porta B, se o carro está na Porta A: $P(B_{Ap.} \mid A) = ½$
- A probabilidade de abrir a Porta B, se o carro está na Porta B: $P(B_{Ap.} \mid B) = 0$
- A probabilidade de abrir a Porta B, se o carro está na Porta C: $P(B_{Ap.} \mid C) = 1$

Utilizando a Equação 10.6, pode-se calcular a probabilidade do carro estar em cada porta, após o apresentador ter aberto a Porta B:

$$P(A \mid B_{Ap.}) = \frac{P(B_{Ap.} \mid A).P(A)}{P(B_{Ap.} \mid A).P(A) + P(B_{Ap.} \mid B).P(B) + P(B_{Ap.} \mid C).P(C)}$$

$$= \frac{\frac{1}{2} \cdot \frac{1}{3}}{\frac{1}{2} \cdot \frac{1}{3} + 0 . \frac{1}{3} + 1 . \frac{1}{3}}$$

$$= \frac{1}{3} \qquad (10.10)$$

$$P(C \mid B_{Ap.}) = \frac{P(B_{Ap.} \mid C).P(C)}{P(B_{Ap.} \mid A).P(A) + P(B_{Ap.} \mid B).P(B) + P(B_{Ap.} \mid C).P(C)}$$

$$= \frac{1 . \frac{1}{3}}{\frac{1}{2} \cdot \frac{1}{3} + 0 . \frac{1}{3} + 1 . \frac{1}{3}}$$

$$= \frac{2}{3} \qquad (10.11)$$

Note-se que a probabilidade do carro estar na Porta C, dado que o apresentador abriu a Porta B, é o dobro de estar na Porta A. Assim, você deveria mudar a sua opção anterior, escolhendo a Porta C.

Este mesmo raciocínio pode ser utilizado nas redes bayesianas, conforme abordado na próxima seção.

10.2 MODELAGEM DA REDE BAYESIANA

Modelos são representações aproximadas da realidade, por definição. Assim, a rede deve levar em consideração apenas o que é

relevante para o delineamento do modelo, tanto em relação às variáveis quanto em suas interações.

Entre os vários tipos de modelos, existem os gráficos, que podem ser considerados como uma linguagem de comunicação, permitindo tanto a comunicação entre pessoas quanto entre pessoas e computadores. Desta forma, facilitam a visualização dos eventos e de suas interações. No que se refere à comunicação com computadores, a linguagem das redes bayesianas é bem definida, o que possibilitou a elaboração de diversos *software* sobre o assunto.

Redes bayesianas são grafos acíclicos direcionados (DAG – *directed acyclic graph*):

Grafo direcionado, pois são representações gráficas onde nódulos representam as variáveis e arcos direcionados representam a existência de uma influência direta entre as variáveis, com intensidade expressa por probabilidades condicionais.

Acíclicos, pois não pode existir um caminho $A_1 \rightarrow \ldots \rightarrow A_n$ onde $A_1 = A_n$, isto é, não existe um caminho que comece e termine no mesmo nódulo.

A Figura 10.4 ilustra a rede bayesiana para o problema do programa de auditório. Note-se que, na rede, os nódulos são os fatores de incerteza do problema, a saber: em que porta está o carro; qual a porta inicialmente selecionada; e qual a porta que o apresentador abrirá. As ligações entre os nódulos representam um grau de influência, expressos por probabilidades apresentadas no Quadro 10.1.

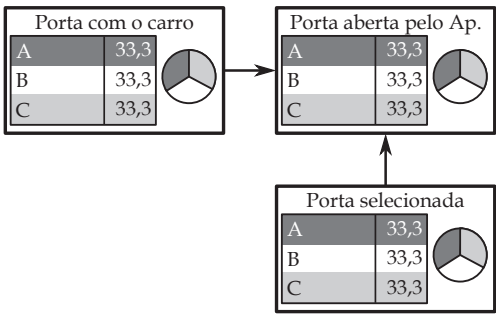


Figura 10.4 Rede antes de selecionar a porta

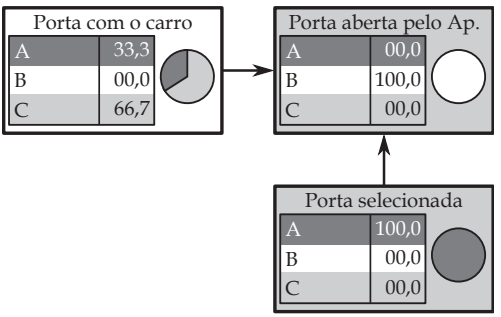


Figura 10.5 Rede após selecionar a Porta A e o apresentador abrir a B

O Quadro 10.1 traz, de forma condensada, as tabelas de entradas de probabilidades dos nódulos da rede da Figura 10.4 (e, por

consequência, da Figura 10.5). As tabelas à esquerda, respectivamente, apresentam as probabilidades de o carro estar em uma das três portas ($^1/_3$ para cada) e as probabilidades de se selecionar uma das três portas (também $^1/_3$ para cada).

A variável "Porta aberta pelo Apresentador", no entanto, exige uma tabela de probabilidade que a relacione com as outras variáveis, pois é ela quem "recebe" as setas de relação dos outros nódulos. Por exemplo, a última linha da tabela expressa a probabilidade de ocorrência desta variável quando inicialmente for selecionada a Porta C e o carro realmente estiver na Porta C; neste caso, a probabilidade do apresentador abrir a Porta C é, inevitavelmente, de 0% e a dele abrir as portas A e B é de 50% para cada uma delas.

Quadro 10.1 Tabelas de entradas de probabilidades, referente à rede da Figura 10.4

Tabela de probabilidades do nódulo "Porta com o carro"

A	B	C
0,33	0,33	0,33

Tabela de probabilidades do nódulo "Porta selecionada"

$A_{Sel.}$	$B_{Sel.}$	$C_{Sel.}$
0,33	0,33	0,33

Tabela de probabilidades do nódulo "Porta aberta pelo Ap."

Porta selecionada	Porta com o carro	$A_{Ap.}$	$B_{Ap.}$	$C_{Ap.}$
A	A	0,00	0,50	0,50
A	B	0,00	0,00	1,00
A	C	0,00	1,00	0,00
B	A	0,00	0,00	1,00
B	B	0,50	0,00	0,50
B	C	1,00	0,00	0,00
C	A	0,00	1,00	0,00
C	B	1,00	0,00	0,00
C	C	0,50	0,50	0,00

Para executar o exemplo ilustrado anteriormente, deve-se instanciar (definir o valor da variável) a "Porta selecionada" como sendo a Porta A e a "Porta aberta pelo Apresentador" como sendo a Porta B, conforme ilustrado na Figura 10.5. Assim, a probabilidade do carro

estar na Porta C é de 66,7% contra 33,3% de estar na Porta A, o que está de acordo com o calculado anteriormente, pois o cálculo realizado para este caso é exatamente o apresentado na Seção 10.1.2.

Note-se que, ao selecionar uma das três portas, a probabilidade do apresentador abrir uma das outras duas é de 50%. No entanto, a probabilidade do carro estar em uma das três portas não é alterada (conforme pode ser observado na Figura 10.6). Isso porque, sem definir a porta aberta pelo apresentador, as variáveis "Porta selecionada" e "Porta com o carro" são independentes. Nesse caso, diz-se que as variáveis estão "d-separadas".

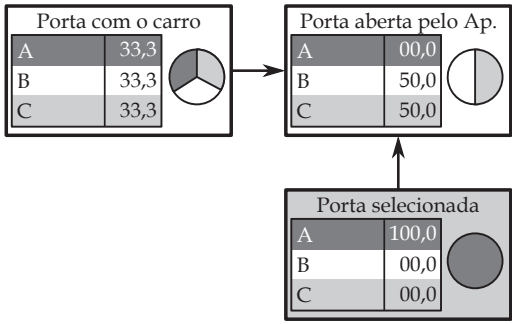


Figura 10.6 Rede após selecionar a Porta A

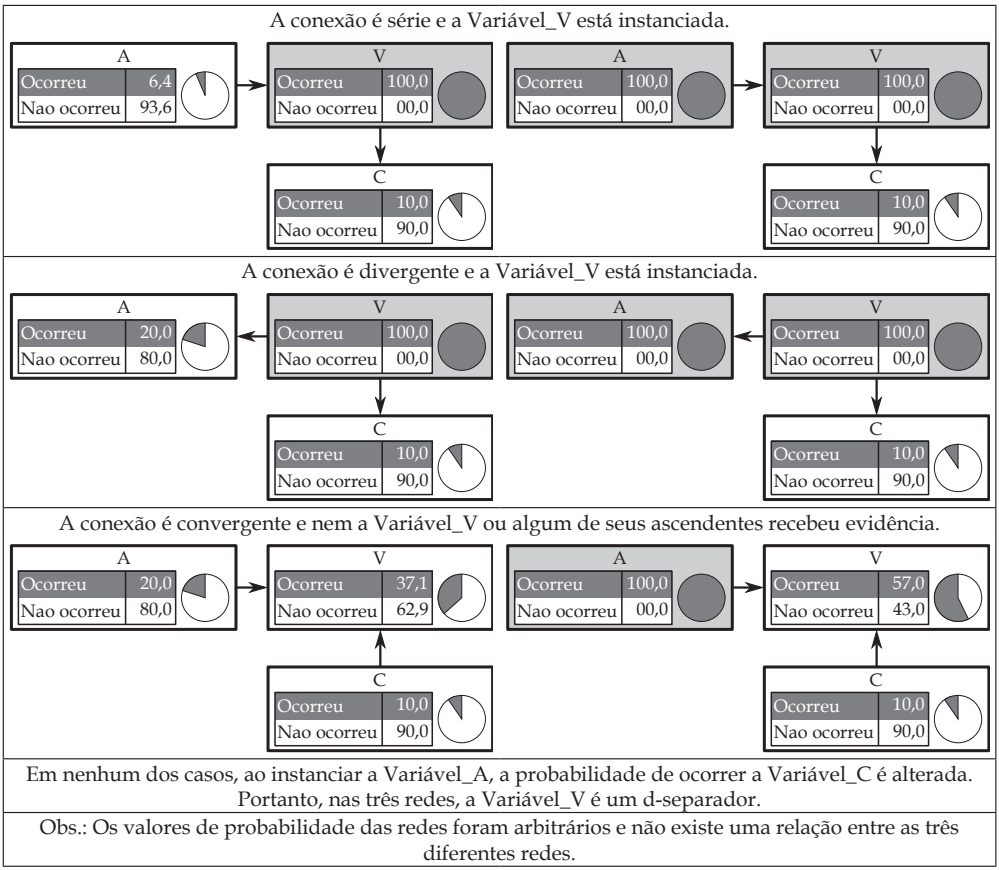
Duas variáveis estão "d-separadas" se, por todos os caminhos entre elas, existir uma Variável_V que:

- a conexão é série ou divergente e a Variável_V está instanciada; ou
- a conexão é convergente e nem a Variável_V ou algum de seus ascendentes recebeu evidência.

Caso contrário, diz-se que elas estão "d-conectadas".

O Quadro 10.2 ilustra os casos que uma Variável_V se torna um d-separador.

Quadro 10.2 Redes em que a Variável_V é um d-separador



Em nenhum dos casos, ao instanciar a Variável_A, a probabilidade de ocorrer a Variável_C é alterada. Portanto, nas três redes, a Variável_V é um d-separador.

Obs.: Os valores de probabilidade das redes foram arbitrários e não existe uma relação entre as três diferentes redes.

O conceito de variáveis d-separadas é determinante para o delineamento da rede, pois ela deve representar a realidade – como todo modelo –, sendo necessário adequar a coleta de informação a fim de atender suas necessidades.

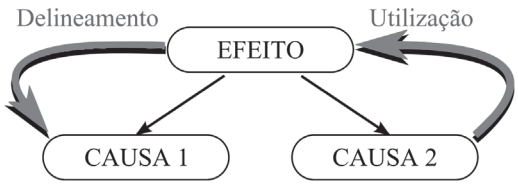
É importante destacar que, quando se constrói a estrutura do modelo da rede bayesiana, não deve-se insistir em ter as ligações na direção causal. Mas verificar as propriedades das d-separações para garantir que o modelo corresponda à percepção da realidade.

Note-se que, dependendo de como a rede é modelada e utilizada, ela pode ou não fazer uso do teorema de Bayes, conforme apresentado no Quadro 10.3.

No entanto, apesar de não fazer uso do teorema de Bayes, as redes que têm seu uso no mesmo sentido do delineamento (encadeamento direto) cumprem a utilidade de facilitar a comunicação, pois possibilitam visualizar a influência entre as variáveis e entre pessoas e computadores, automatizando o processo de cálculo.

Quadro 10.3 Redes podem ou não fazer uso do teorema de Bayes

Raciocínio de diagnóstico ou encadeamento reverso



Quando se deseja saber a probabilidade de ocorrer um Efeito dado que ocorreu uma Causa deve-se *a priori* delinear as relações de qual a probabilidade do Efeito ter sido gerado pela Causa.

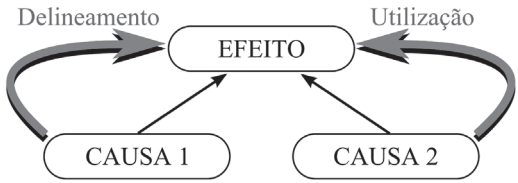
Assim, pelo teorema de Bayes, pode-se calcular – por exemplo – a probabilidade de ocorrer o Efeito dado que ocorreu a Causa 1:

$$P(E \mid C_1 = 0) = \frac{P(E).P(C_1 = 0 \mid E)}{P(C_1 = 0)}$$

sendo:
$C_{1,2}$ = O (O evento $C_{1,2}$ ocorreu),
$C_{1,2}$ = NO (O evento $C_{1,2}$ não ocorreu)

Nessa topologia, as causas 1 e 2 não são independentes – já que o nó Efeito não é um "d - separador". Isso significa que, ao instanciar o nódulo Causa 1, a probabilidade de ocorrência da Causa 2 será alterada.

Raciocínio preditivo ou encadeamento direto



Tanto o delineamento quanto a utilização se dá no sentido das Causas para o Efeito.

Assim, pela teoria de probabilidade condicional, pode-se calcular – por exemplo – a probabilidade de ocorrer o Efeito dado que ocorreu a Causa 1:

$$P(E \mid C_1 = O) = P(C_2 = O).P(E \mid C_1 = O \cap C_2 = O) + P(C_2 = NO).P(E \mid C_1 = O \cap C_2 = NO)$$

Observe-se que $P(E \mid C_1 = O \cap C_2 = O)$, $P(C_2 = O)$, $P(E \mid C_1 = O \cap C_2 = NO)$, e $P(C_2 = NO)$ são informações implementadas na rede durante o delineamento. Portanto, não é necessário o uso do teorema de Bayes, nesse caso.

10.3 INTERAÇÃO COM OUTRAS TÉCNICAS

As análises realizadas utilizando redes bayesianas podem complementar ou substituir outras técnicas, tais como diagramas de confiabilidade em blocos (RBD – *reliability block diagram*), árvores de evento (ETA – *event tree analysis*) e árvores de falha (FTA – *fault tree analysis*).

Note-se que estas três técnicas listadas fazem uso de relações determinísticas para fazer a análise. Por exemplo, em um RDB, ao se atribuir a um componente o estado de falha, determinará se o sistema estará em operação ou não (com certeza). Assim, ao elaborar uma rede que represente este RBD, pode-se até questionar se esse modelo em rede é realmente bayesiana, pois não existe incerteza nas relações condicionadas.

No entanto, o modelo de rede – por estar informatizado – traz algumas possibilidades que seriam enfadonhas se fossem realizadas em uma destas três técnicas, como, por exemplo:

- Verificar o impacto da falha de um, ou mais, dos componentes na probabilidade de falha do sistema.

- Verificar quais componentes são mais prováveis de causarem a falha do sistema, ao se instanciar: Sistema = Falha (nesse caso, o teorema de Bayes estaria sendo utilizado).

Todavia, para o caso de se querer avaliar a confiabilidade do sistema, o modelo em rede pode não ser vantajoso em relação ao RBD, pois esse último traz a informação de falha do sistema de forma mais simples e objetiva.

Entre as desvantagens de se representar uma árvore de falha (FTA) em forma de rede salienta-se a de não existir um grafo para os operadores lógicos ("E", "OU" etc.), pois as tabelas estão implícitas. Para contornar esse inconveniente pode-se indicar com um texto o operador utilizado, quando a relação é determinística.

Por fim, destaca-se que a representação da combinação de ETA e FTA em redes bayesianas se mostra especialmente interessante para avaliar o impacto da ocorrência de uma causa raiz nos possíveis cenários, pois conta com ferramentas computacionais que possibilitam isso. No entanto, existem *software* específicos para modelar ETA e FTA que também fazem essa análise, possibilitando, inclusive, avaliar causas comuns

10.4 CONSIDERAÇÕES FINAIS

Diante das considerações apresentadas neste capítulo, pode-se apresentar no Quadro 10.4 uma definição formal de redes bayesianas.

Quadro 10.4 Definição formal de redes bayesianas (JENSEN, 2001)

Uma rede bayesiana consiste no seguinte:

- Um conjunto de variáveis e ligações direcionadas entre elas.
- Cada variável tem um número finito de estados mutuamente exclusivos.
- O conjunto de variáveis e suas ligações formam um grafo acíclico direcionado (DAG – *directed acyclic graph*).
- Para cada variável A com parentes $B_1, \ldots, B_n$, existe uma tabela de probabilidades condicionais $P(A \mid B_1, \ldots, B_n)$.

Note-se que a definição apresentada não traz restrições quanto à direção de modelar e utilizar a rede e, tão pouco, quanto à obrigatoriedade de existir incertezas nas relações entre as variáveis. No entanto, apesar de existir a possibilidade de modelar sistemas determinísticos utilizando redes bayesianas, esta prática não é comum – talvez pelo fato de técnicas como RBD, FTA e ETA gerarem diagramas mais intuitivos.

O uso de redes bayesianas pode ser mais indicado, dependendo do que se deseja extrair do modelo, como no caso de existir incerteza nas relações entre as variáveis. Assim, existem várias alternativas de modelos para se representar um sistema, e a decisão de qual técnica será utilizada deve ser baseada no que se espera extrair do modelo.

Capítulo 11

ANÁLISE DE EVENTOS POR REDE CAUSAL (CNEA)

A análise de eventos por rede causal (CNEA – *causal network event analysis*) é uma técnica que estrutura a análise de risco por meio da representação das ligações entre o evento analisado (que fica no centro do diagrama), causas (à esquerda), efeitos (à direita) e as barreiras que atuam na corrente causal, na forma de redes causais (Figura 11.1).

É interessante observar que esta abordagem, de centralizar o evento analisado e dispor as causas e efeitos no mesmo diagrama também, é adotada por outras técnicas, destacadamente a BTA (*bow-tie analysis*). A BTA é vista como uma evolução dos diagramas causa/consequência dos anos de 1970 e dos diagramas de barreiras dos anos de 1980. Atualmente, a técnica é utilizada nas mais diversas áreas, a exemplo de Trbojevic (2001), no gerenciamento da navegação e outras operações portuárias; Ramzan (2006), na gestão de risco em usinas nucleares; Iannacchione, Esterhuizen & Tadolini (2007), na mitigação do risco de instabilidade estrutural e incêndios em minas; Trbojevic (2004), na análise de descarrilhamento de trens de passageiros; no projeto ARAMIS (*accidental risk assessment methodology for industries*), que visa desenvolver uma metodologia para avaliação de risco (DELVOSALLE et al., 2006; DIANOUS e GOWLAND, 2006); entre outras.

A necessidade de implementar melhorias e agregar conceitos na BTA se deveu ao fato de que a mesma apenas lista as causas e consequências, sem estruturá-las na forma de rede. Além disso, a BTA não permite considerar a barreira como um evento pivotal dos cenários. Esses aspectos são importantes e facilitadores para a análise do risco e posterior comunicação, além de ajudar na iteração com outras técnicas.

A percepção da necessidade de aproveitar a técnica BTA e agregar à mesma novos elementos de análise ocorreu durante o desenvolvimento do projeto MitiSF_6 e nos trabalhos de pesquisa que vinham sendo desenvolvido no NeDIP/UFSC (CALIL, 2009). Ao utilizar as diversas técnicas de análise de risco entendeu-se ser importante integrar a estrutura FTA/ETA com a técnica FMEA. Sentiu-se também a necessidade de melhor trabalhar os resultados das análises das referidas técnicas numa forma que facilitasse a comunicação dos resultados da análise. Assim, procurou-se associar a BTA com redes causais e, com a experiência acumulada pela equipe de pesquisadores do NeDIP na utilização de técnicas para análise de confiabilidade e segurança, surgiu uma outra forma de análise que foi denominada de CNEA - análise de eventos por rede causal (*causal network event analysis*). A seguir apresenta-se os conceitos relacionados à técnica, à taxonomia e exemplo de aplicação.

11.1 CONSIDERAÇÕES SOBRE A TÉCNICA CNEA

A técnica CNEA é utilizada para análise de eventos (e.g., incidentes), causas, efeitos e barreiras a serem interpostas para diminuir a chance das causas deflagrarem o evento central ou mitigar os seus efeitos – como está posto na Figura 11.1. O Quadro 11.1 apresenta a sintaxe que foi estabelecida visando estruturação da representação da técnica de forma simplificada para facilitar entendimento e uso.

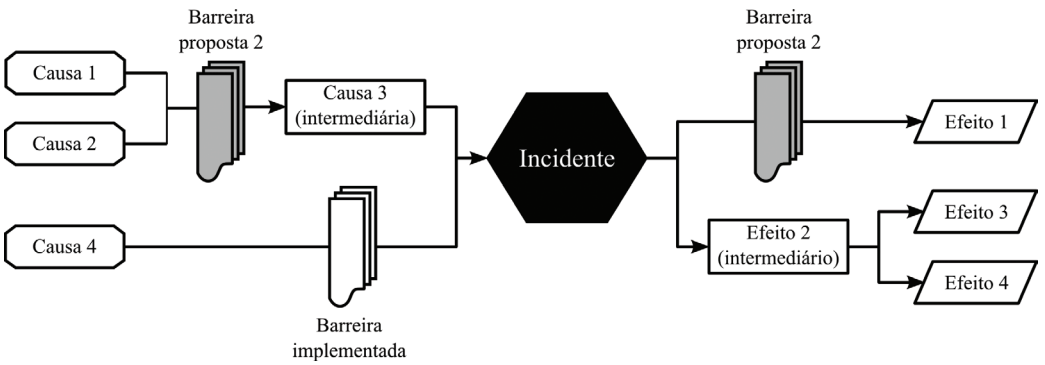
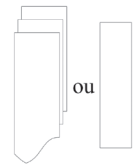
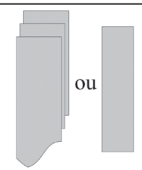


Figura 11.1: Diagrama de uma análise de eventos por rede causal (CNEA)

Quadro 11.1: Taxonomia da CNEA

FIGURA	DESCRIÇÃO	FIGURA	DESCRIÇÃO
	Evento a se analisar, no caso, um **incidente**. Alguns autores adotam um círculo. Optou-se pelo hexágono para diferenciar da representação de causa raiz na FTA.		**Barreiras** preventivas **já implementadas** que objetivam evitar a ocorrência do evento central ou mitigar seus efeitos.
	**Efeitos** potenciais que o evento central pode gerar, dentro do escopo de análise.		
	**Causa** raiz para a ocorrência do evento central, dentro do escopo de análise.		**Barreiras** preventivas **propostas**, que deverão ser implementadas.
	**Causa ou efeito intermediário**		

Destaca-se ainda que a CNEA é aderente a modelos de representação de incidentes baseado em correntes causais, como o proposto por Mosleh & Dias[1] – apresentado no Capítulo 3, Figura 3.3. No entanto, em uma CNEA pode-se modelar várias correntes causais referentes a um determinado incidente, conforme ilustrado na Figura 11.2.

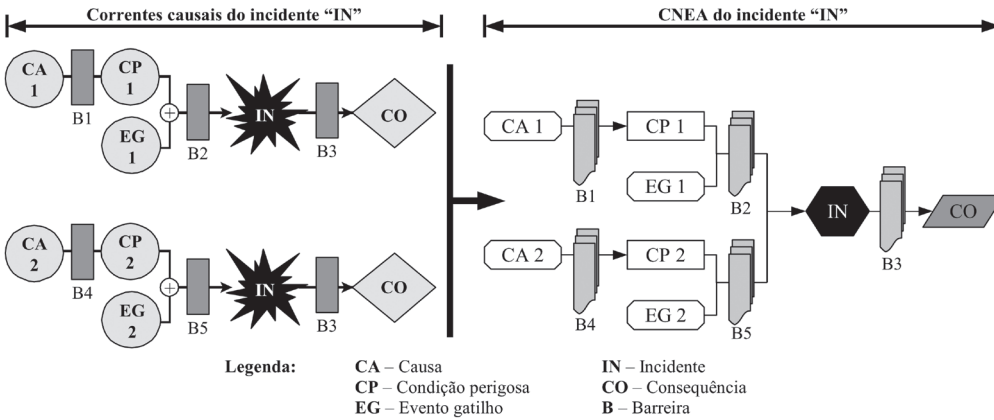


Figura 11.2 Correntes causais, modeladas conforme Mosleh & Dias, combinadas em uma rede causal CNEA

[1] Deve-se avaliar a possibilidade de utilizar a técnica CNEA com outros tipos de modelos de representação de incidentes, como o STAMP (Systems-Theoretic Accidents Model and Processes) proposto por Leveson e colaboradores (LEVESON, 2003).

Para ser possível agrupar várias correntes causais, os efeitos decorrentes do incidente devem ser idênticos. Caso exista uma particularidade de um incidente quando deflagrado por uma condição específica, essa corrente causal deve ser tratada separadamente. Por outro lado, em alguns casos é possível simplificar a rede agrupando alguns elementos da CNEA – por exemplo, no caso do mesmo evento gatilho deflagrar mais de uma condição perigosa.

A nomenclatura explicitada na legenda tem o mesmo significado da utilizada em outras técnicas. A explicitação e discussão sobre a taxonomia aborda o significado exposto na legenda da Figura 11.2.

11.2 MODELAGEM DA CNEA

O processo de modelagem envolve, normalmente, uma consulta a pessoas que podem ser afetadas pelo risco e que têm conhecimento tanto do ponto de vista técnico quanto de segurança. A partir da experiência das pessoas, é possível levantar os cenários; os controles existentes para reduzir o risco; identificar possíveis barreiras a serem implementadas para reduzir o risco etc. Ao longo da aplicação da técnica CNEA, recomenda-se seguir cinco passos principais, conforme apresentado nas próximas seções, a saber: definição do escopo de análise; identificação do modo de falha (incidente); identificação das causas; identificação dos efeitos; identificação das barreiras; identificação do evento gatilho e identificação da condição perigosa.

11.2.1 DEFINIÇÃO DO ESCOPO DE ANÁLISE

É a definição dos limites da análise, tanto no que se refere ao desdobramento das causas quanto dos efeitos. Assim, antes de iniciar a modelagem dos eventos a serem estudados, deve-se ter claro até onde será feita a investigação das causas (qual o nível de detalhamento) e até onde se analisará o impacto da ocorrência deste incidente. É muito importante definir-se quais os resultados que se deseja obter com a análise e qual a forma de explicitar os resultados e também quais outras técnicas serão abordadas para ajudar na organização e versões sobre a análise efetuada.

11.2.2 IDENTIFICAÇÃO DO INCIDENTE

O segundo passo da elaboração da CNEA é a identificação do incidente (IN). Identificar o incidente significa efetuar um detalhamento do mesmo (preferencialmente *a priori*, ou seja antes que o mesmo aconteça) de forma que seja possível definir as barreiras para mitigar os efeitos ou consequências sobre a função, o ambiente ou a segurança humana. O incidente (Figura 11.1) é um modo de falha, ou uma falha generalizada de um sistema técnico. Algumas perguntas ajudam a identificar, caracterizar ou sistematizar um incidente:

- Que funções um dado sistema ou componente deve cumprir?
- Quais as condições de operação do sistema / componente?
- Como se caracteriza o incidente?

Assim, é possível identificar claramente como ocorre o evento que se deseja evitar. O incidente (IN) é, então, representado na posição central do diagrama CNEA (Figura 11.1), sendo caracterizado, por exemplo, como uma não-função ou um funcionamento fora das condições especificadas no projeto. Quando o CNEA está sendo usado para organizar o resultado de uma FMEA o incidente é o modo de falha. Evidentemente, uma análise como essa é feita apenas para os modos de falha principais que evidenciam uma condição perigosa (CP) em relação ao incidente, cuja consequência (CO) traz desdobramento indesejável para o ser humano, ambiente ou, pode levar a indisponibilidade, ou mesmo, a não continuidade da função no próprio sistema técnico.

11.2.3 IDENTIFICAÇÃO DAS CAUSAS

Causa (CA) é o evento onde está a origem do incidente, origem do modo de falha. Em toda análise de risco ou de confiabilidade, procura-se sempre eliminar ou mitigar a causa. As causas são os motivos que levam à ocorrência do evento central e por isso no diagrama de CNEA (Figura 11.1) estão localizadas no lado esquerdo do mesmo. Vale destacar que a ação da equipe de análise é identificar todas as causas que conduzem ao modo de falha. Descrevem-se as causas imediatas (que estão diretamente relacionadas com a percepção do operador do item) e as causas intermediárias (que requerem análise

mais detalhada do modo de falha). Contudo, atenção maior deve-se dar às causas raízes, dado que no estudo das mesmas tem-se a possibilidade de obter maior sucesso do processo de análise. Para tanto, questiona-se quais as possíveis correntes causais levam a ocorrência do incidente (da forma que foi delineado).

11.2.4 IDENTIFICAÇÃO DOS EFEITOS

No diagrama CNEA (Figura 11.1), os efeitos estão dispostos no lado direito do evento central, e podem também ser chamados de conseqüência (CO) (Figura 11.2), quando a abordagem está relacionada a análise de risco. Na abordagem proposta deve-se identificar os possíveis desencadeamentos até se chegar aos efeitos finais dentro do escopo de análise. Para tanto, se delineia todas as condições intermediárias e se estabelece as possíveis ligações entre as mesmas. Para facilitar a análise, a equipe define como será a abordagem do efeito. Por exemplo, se o incidente for modo de falha então é razoável pensar os efeitos como a maneira do modo de falha se manifestar. Tem-se efeitos característicos como vibração, ruído, temperatura, cheiro, mudança de cor, dilatação térmica etc. Se o incidente estiver no nível de uma pane ou de um acidente, então, por decorrência, a abordagem será em nível de consequências. Exemplo de consequências são: incêndio, contaminação, explosão, mortes, descontinuidade etc.

11.2.5 IDENTIFICAÇÃO DAS BARREIRAS

As barreiras são divididas em dois grupos. O primeiro grupo tem **função preventiva**, com objetivo de eliminar, reduzir, acompanhar e controlar as causas que permitem ou promovem o incidente (IN) na corrente causal. O segundo grupo é de **contingência**, definido para eliminar, mitigar, ou preparar-se para atuar sobre o efeito/consequências (CO) (Figura 11.1 e Figura 11.2) dado que ocorreu um incidente. Para identificar os dois tipos de barreiras, as seguintes perguntas são recomendadas:

- Como prevenir a ocorrência do incidente ou de suas causas?
- Quais possíveis formas de monitoramento e de controle?
- Como é possível mitigar os efeitos, caso o evento central ocorra?

- É possível manter a função do sistema, mesmo na ocorrência do incidente?

Nesse ponto, é interessante fazer uma análise mais ampla, supondo inclusive que as barreiras podem falhar. Destaca-se que a análise deve ser feita separadamente, conforme já mencionado.

A partir da identificação das barreiras de prevenção e contingência, pode-se definir um plano de ações para o gerenciamento do risco. Para tanto, outras questões orientam as ações:

- Que tarefas serão executadas para assegurar que as barreiras sejam implementadas?
- Que tarefas serão executadas para assegurar que as barreiras se mantenham ativas?
- Quem é responsável pelas tarefas?
- Como saber quando a tarefa deve ser executada?
- Como saber exatamente o que deve ser feito? Existe um procedimento?
- Qual a capacitação requerida para a execução das tarefas?
- Como verificar se a tarefa foi executada corretamente e se ela é efetiva?

Com o plano de ações definido é possível realimentar a CNEA com as novas informações obtidas.

Dessa forma, recomenda-se avaliar algumas questões:

- Existe controle suficiente sobre o risco? O que mais pode ser feito?
- É possível aumentar a efetividade do controle sobre o risco?
- É viável aumentar o número de barreiras para a ocorrência do evento central?
- Há possibilidade de remover alguma barreira?
- O plano de ações é viável?

11.2.6 IDENTIFICAÇÃO DO EVENTO GATILHO

O evento gatilho (EG) da Figura 11.2 é um evento que deflagra ou potencializa a condição perigosa para a condição de risco, de tal

sorte que resulte num incidente. Incidente, como já comentado, é um modo de falha que proporciona o impedimento da função ou cria restrições para que a função se desenvolva de acordo com o planejado. Em nível de confiabilidade, evento gatilho é um evento externo, como aumento de pressão, poeira, umidade, temperatura, impacto etc., que impulsiona o aparecimento de um modo de falha que, por exemplo, estava oculto durante o ciclo de vida do item (entendendo item como componente, subsistema, sistema etc.). Em análise de risco, o evento gatilho também está relacionado com evento externo advindo do ambiente, do homem ou do próprio sistema técnico. Cita-se tempestades, ciclones, tornados, enchentes, acidentes de trânsito, incêndios, protestos, distúrbios que levam a condição perigosa se transformar num incidente, na forma de descontinuidade da função como não fornecimento de energia elétrica, fuga de corrente, vazamento de produto químico etc.

Eventos gatilhos estão muito presentes na condição humana ao longo do ciclo de vida de trabalho e no seu processo. Por exemplo, no ciclo de vida de uma atividade, os horários iniciais da atividade e o final das mesmas são mais propensos a erros. Em estudos de segurança no trabalho, chama-se atenção de que no início e no final de turnos há maior chance de ocorrer falhas operacionais decorrentes de desatenção ou de fadiga. Nessas situações, as causas são organizacionais, e as barreiras para impedir a ocorrência do evento gatilho estão fortemente relacionadas com a capacitação e trabalho em equipe.

11.2.7 IDENTIFICAÇÃO DA CONDIÇÃO PERIGOSA

A condição perigosa (CP) da Figura 11.2 é própria de todo sistema técnico no ciclo de vida de trabalho, originado a partir de uma causa que precisa ser estudada. É sabido que todo sistema técnico é portador de perigo. Assim, em trabalho extremo ou diante de eventos críticos esse perigo, diante de uma causa potencial, produz um modo de falha que pode gerar uma condição perigosa. Isso acontece, por exemplo, quando os programas de operação ou manutenção não estão devidamente preparados para suportar as dúvidas dos operadores e manutentores diante das circunstâncias normais de funcionamento e de forma mais significativas nos eventos especiais de operação e manutenção. A condição perigosa é mais facilmente identificada a

partir de estudos de cenários. É possível ser definida nos processos de análise de confiabilidade e de risco, utilizando técnicas de *brainstorming*, análise funcional, FMEA com identificação da criticidade (que muitos autores denominam de FMECA). Como exemplo de condição perigosa cita-se a falha oculta.

11.3 RELAÇÃO ENTRE A CNEA E OUTRAS TÉCNICAS

A CNEA é uma técnica para modelar relações causa/efeito e, portanto, pode ser utilizada em substituição ou complementação às técnicas próprias para esse tipo de análise. Nas seções a seguir apresenta-se algumas considerações sobre as relações entre a CNEA e FTA, ETA, BTA e FMEA.

11.3.1 CNEA E FTA

Na CNEA é possível desdobrar as causas do evento central até a resolução desejada (no limite do escopo de análise), mantendo a representação dos eventos intermediários e a forma com que se relacionam. É interessante salientar que a estrutura em rede causal permite representar as ligações sem ter que especificar como as causas interagem, oferecendo um modelo gráfico para facilitar o entendimento dos especialistas quanto às correntes causais do evento central em análise.

Para o desenvolvimento da análise com a técnica, em face de ser amigável com o raciocínio de soluções do cotidiano, não é necessário um nível de conhecimento muito especializado – como ocorre quando se desenvolve uma árvore de falha. Isso porque não é preciso saber as relações lógicas entre os eventos modelados, como é exigido pela FTA.

Por exemplo, na Figura 11.3, a cadeia causal está representada por uma FTA. No entanto, para estabelecer o relacionamento entre os eventos, é necessário saber qual porta lógica será utilizada, "E" ou "OU". Ou seja, é requerido um conhecimento especializado em relação ao domínio das relações causa/efeito, no contexto da função dos sistemas, se as funções têm grau de dependência, se estão operando em série ou têm itens redundantes.

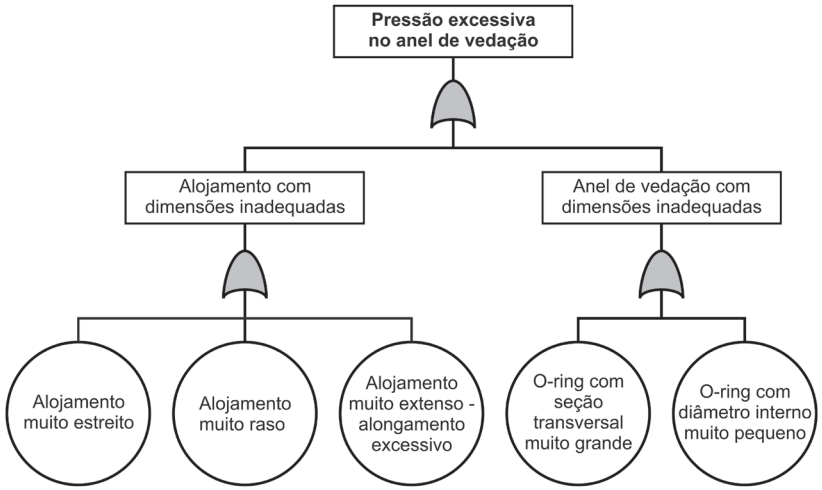


Figura 11.3 Exemplo de FTA

A mesma modelagem apresentada pela Figura 11.3, no contexto da FTA, está representada na Figura 11.4, no contexto da CNEA. Neste caso, porém, não se tem as portas lógicas OU (próprias do FTA definidas no Capítulo 8), mas apenas a nomenclatura dos eventos descritos pela taxonomia, ou seja, o significado de cada elemento que forma a árvore – causa-evento de risco.

Assim, se em um caso específico o conhecimento das relações não contribui consideravelmente para o entendimento do modelo ou o analista não possui conhecimento suficiente para estabelecer as relações, é possível utilizar a CNEA, como está mostrado na Figura 11.4.

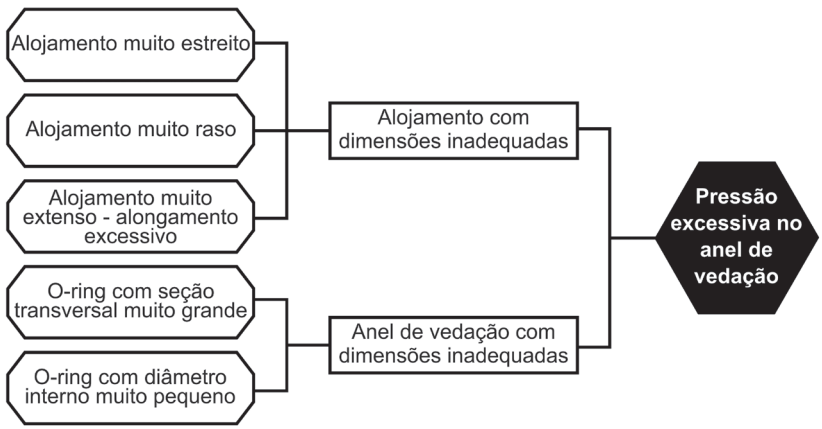


Figura 11.4 Relação entre FTA e CNEA

11.3.2 CNEA E ETA

Com relação à análise dos efeitos, a CNEA permite traçar os cenários delineando os potenciais estados futuros, considerando a ocorrência do evento central. Assim como nas causas, os efeitos também são representado na forma de rede, evidenciando o encadeamento até se alcançar os efeitos finais (delimitado pelo escopo de análise). Note-se que outras técnicas, como a ETA, fazem o delineamento dos eventos pivotais, mas evidenciam apenas os estados finais (resultados dos cenários).

Eventos pivotais são aqueles que alteram o encadeamento da corrente causal. Em uma ETA todos os eventos analisados são pivotais, como apresentada na Figura 11.5. Na CNEA, os efeitos são considerados como estados, e as barreiras como eventos pivotais. Com isso, a CNEA permite destacar os efeitos intermediários a partir dos quais definem-se as barreiras para mitigar os efeitos finais.

Figura 11.5 Representação de um evento pivotal (Barreira 1) em uma ETA

Na CNEA o evento pivotal é modelado considerando que a barreira pode ou não ser bem sucedida. Esta consideração é mais relevante na análise de efeitos, em que o sucesso da barreira resulta em um efeito de menor proporção, mas que não deve ser desprezado. A Figura 11.6 ilustra esta situação. A eficácia da barreira, indicada pela linha espessa abaixo da barreira, na Figura 11.6, implica na ocorrência do efeito 3. O mesmo impede a ocorrência do efeito 1 e seus efeitos seguintes. Ou seja, o efeito 3 na prática pode significar um sinal de alerta, um mecanismo de segurança, um comando automático, ou uma desabilitação de uma função que impede que o incidente caminhe para o efeito 1 e subsequentes. Assim, a barreira atua como um evento pivotal, da mesma forma que no modelo da ETA ilustrado na Figura 11.5.

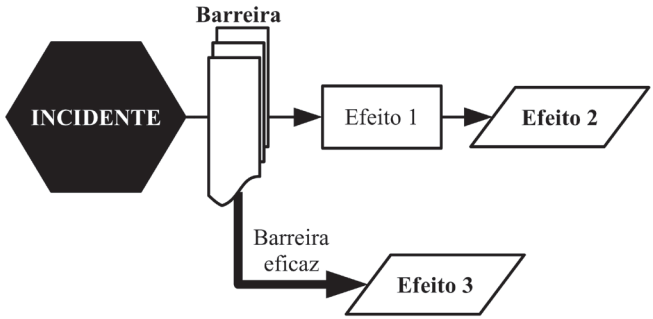


Figura 11.6 Representação de uma barreira eficaz (evento pivotal) em uma CNEA

Note-se que é possível, em apenas um diagrama, visualizar as relações das causas (que também podem ser modeladas em uma árvore de falhas) e dos efeitos (que podem ser modeladas em uma árvore de eventos). Observa-se que a CNEA pode ser modelada sem ter que determinar o tipo de relação existente entre seus elementos – como em uma FTA (*fault tree analysis*) –; e os efeitos podem ser levantados sem a necessidade de compreender todos os eventos que influenciam na corrente causal, como ocorre na ETA (*event tree analysis*).

11.3.3 CNEA E FMEA E BTA

A forma que a CNEA está estruturada é muito conveniente para integrá-la à FMEA, pois é possível delinear os potenciais efeitos e causas dos modos de falha e, posteriormente, identificar as barreiras, que são os controles atuais e os planos de ações. Dessa forma, a integração com a CNEA possibilita minimizar algumas limitações da FMEA – principalmente no que diz respeito à representação do conhecimento no formato de tabelas. A explicitação das barreiras na forma de figuras facilita o entendimento do que deve ou precisa ser feito. Assim, as principais ações explicitadas na última coluna de uma tabela de FMEA ganham evidência se representadas na forma de figuras como explicitadas na Figura 11.6 ou Figura 11.7. Isso porque, as ações da última coluna da tabela de FMEA são em si barreiras para eliminar, diminuir as ações das causas que geram os modos de falha ou para mitigar os efeitos.

Tradicionalmente, se apresenta nas tabelas de FMEA as causas raízes e os efeitos finais decorrentes dessas causas, sem

considerar os eventos intermediários. Para chamar atenção entre a relação FMEA e BTA mostra-se a Figura 11.7. No exemplo tem-se ao centro o evento pivotal (Risco). No lado esquerdo do evento pivotal posiciona-se as ameaças e respectivas barreiras e do direito as consequências com as respectivas medidas de recuperação, segundo Lewis & Hurst (2005). Algumas considerações são feitas em relação à aplicação da técnica BTA, já que a mesma foi reorganizada e redefinida para construir a CNEA.

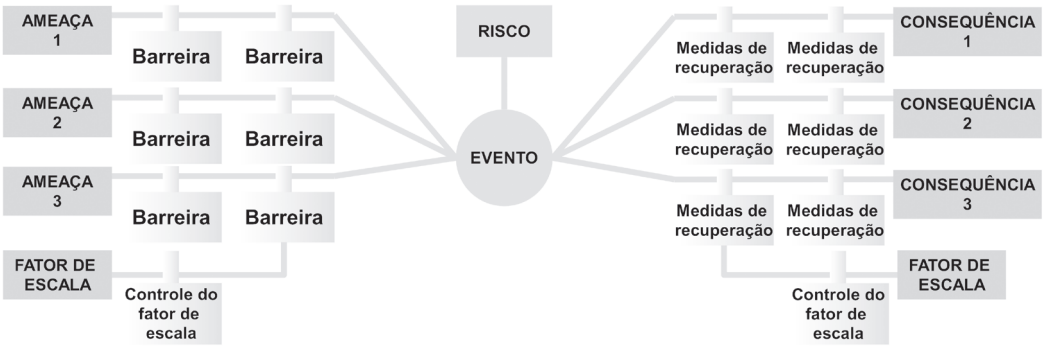


Figura 11.7 Formalismo da BTA (LEWIS & HURST, 2005)

No uso da técnica BTA há que considerar a taxonomia da mesma:

- Ameaça: causa potencial para dar início ao cenário de risco que leva ao evento central.
- Barreira: medidas de proteção para impedir que as ameaças alcancem o cenário de risco.
- Evento central: evento que inicia o cenário de risco, ou seja, o ponto no qual o controle sobre o risco é perdido.
- Consequência: possíveis consequências resultantes da ocorrência do evento central.
- Medidas de recuperação: medidas para mitigar as consequências.
- Fator de escala: possíveis falhas das "barreiras" ou das "medidas de recuperação".
- Controle do fator de escala: medidas para evitar a falha da "barreira" ou da "medida de recuperação".

Note-se que na BTA apresentada não é possível delinear uma corrente causal que leve ao evento central. Outros autores, por sua vez, utilizam o conceito de causas intermediárias para modelar os cenários de acidentes utilizados na análise quantitativa de risco, resultando em um diagrama com a estrutura de uma rede causal.

Chama-se atenção para o fato de que o termo "barreiras", na CNEA, é utilizado tanto para medidas preventivas, com o objetivo de reduzir o risco, quanto para medidas de contingência, que visam mitigar os efeitos do incidente. No caso da BTA, são chamadas de "medidas de recuperação".

É importante salientar que na CNEA não se modela os "fatores de escala" e seus controles (como acontece na Figura 11.7), pois o diagrama se restringe à análise do evento central. Para identificar as possíveis causas de falhas das barreiras – bem como as medidas de proteção – é recomendável fazer uma nova análise.

11.4 CONSIDERAÇÕES FINAIS

A utilização da técnica CNEA (*causal network event analysis*) permite obter modelos detalhados de incidentes e, consequentemente, facilita a compreensão dos sistemas e o diálogo com os participantes da análise. Ademais, com a cadeia causal mais detalhada, pode-se identificar um número maior de pontos para a tomada de ações (barreiras) e, portanto, melhorar os resultados.

Como não há necessidade de conhecer as relações determinísticas entre os elementos da cadeia, como ocorre na FTA por meio de portas lógicas, a inclusão de falhas na cadeia causal tornou-se bastante simplificada.

A CNEA foi inicialmente concebida para se integrar à FMEA e, dessa forma, facilitar seu desenvolvimento, visto que uma das deficiências da FMEA é a representação na forma de tabela. As duas técnicas são bastante complementares, isto é, enquanto o FMEA apresenta conjuntamente todos os modos de falha de um componente, a CNEA facilita a visualização dos modos de falha de interesse, explicitando as relações de causa/efeito.

Sistemas geralmente apresentam muitos modos de falha (incidentes), sendo que cada modo de falha é modelado em um diagrama CNEA próprio. Por essa razão, existe uma limitação no uso da técnica

quando se deseja analisar a influência entre modos de falha e entre sistemas. Esse problema identificado no uso da técnica pode ser diminuído quando se combina a CNEA com a FMEA, pois diversos sistemas podem ser representados em uma mesma tabela.

CNEA é uma técnica de análise de cenário e tem a limitação quanto a atualização dos modelos, no caso de alterações de projeto que influenciam na ocorrência dos eventos dentro da cadeia causal. Manter os modelos atualizados pode-se tornar uma tarefa difícil, principalmente se houver mudanças numerosas e frequentes. Para isso, sugere-se o emprego de ferramentas computacionais que possam dar suporte a utilização da técnica, podendo assim solucionar este problema..

Em aplicação em sistemas reais, foi possível perceber a grande utilidade da CNEA, tanto para modelagem de falhas em equipamentos como em processos. A representação da cadeia causal por meio da técnica é bastante simples o que facilitou a comunicação entre os membros da equipe composta por profissionais de diversas áreas como técnicos de manutenção, engenheiros eletricistas, engenheiros mecânicos, gerentes de manutenção.

Por fim, destaca-se que o conceito de barreira eficaz permite evidenciar situações conflitantes, por exemplo, redução da disponibilidade em detrimento do aumento da segurança, pois os sistemas de proteção executam o desligamento do equipamento para preservá-los de danos maiores, refletindo na indisponibilidade.

Capítulo 12

CARACTERIZAÇÃO DO SF_6

O objetivo deste capítulo é explanar os aspectos físico-químicos do SF_6 (Hexafluoreto de Enxofre) e, particularmente, as propriedades importantes para sua utilização como meio isolante e de extinção do arco em equipamentos elétricos. Os tópicos abordados neste capítulo e no de Disjuntores Isolados a SF_6 (Capítulo 13) auxiliam o entendimento e a aplicação das técnicas de análise de risco apresentadas ao longo do livro.

12.1 HEXAFLUORETO DE ENXOFRE (SF_6) – ASPECTOS GERAIS

O SF_6 é um composto químico inorgânico formado por um átomo central de enxofre ligado a seis átomos de flúor, em uma estrutura octaédrica simétrica. Em condições normais de temperatura e pressão e em seu estado puro, o SF_6 é um gás quimicamente inerte, estável, inodoro, incolor, não tóxico e não inflamável.

O SF_6 é um produto industrializado desenvolvido por síntese direta a partir do flúor e do enxofre fundido (Figura 12.1).

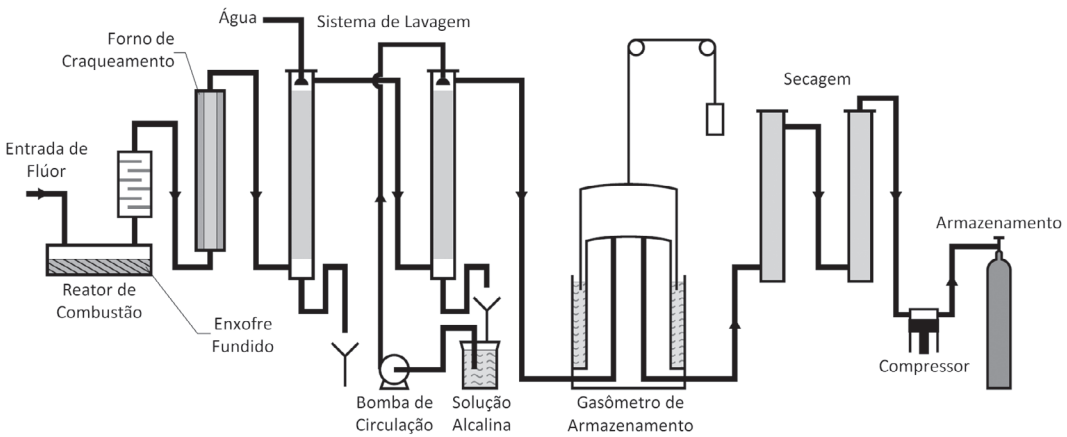


Figura 12.1: Processo de síntese do SF_6 (KOCH, 2003).

O produto resultante do processo de síntese é purificado por craqueamento, lavagem e secagem, sendo posteriormente liquefeito por compressão para eliminar os elementos não condensáveis: oxigênio, nitrogênio e tetrafluoreto de carbono. Finalizado o processo, o SF_6 purificado é estocado na forma comprimida em recipientes de aço (ABNT, 1992b)[1]. O Quadro 12.1 mostra alguns parâmetros relacionados ao armazenamento para comercialização do SF_6 (ELETROSUL, 2008).

Quadro 12.1: Parâmetros para comercialização do SF_6.

Tipo de Cilindro	Conteúdo	Pressão (kgf/cm^2)	Peso Bruto (kg)
K	50.0 kg	21.0	118.0
G	7.7 kg	21.0	19.7

12.2 HISTÓRICO DE DESENVOLVIMENTO DO SF_6

O SF_6 foi sintetizado pela primeira vez nos laboratórios da Faculdade de Farmacologia de Paris, por Henri Moissan e Paul Lebeauem em 1900. Em 1906 Henri Moissan ganhou o prêmio Nobel de química por suas experiências com o flúor (FIHMAN, 1997).

As primeiras pesquisas sobre aplicações industriais de SF_6 foram feitas em 1937, pela *General Electric Company*, que sugeriu sua utilização em equipamentos elétricos por conta da sua grande rigidez dielétrica (intensidade máxima do campo elétrico "tensão elétrica" que um material isolante pode suportar sem conduzir eletricidade). Em 1939, o uso do SF_6 para cabos e capacitores foi patenteado por Thomson-Houston. (GARZON, 2002)

Logo após a II Guerra Mundial, em 1947, apareceram trabalhos sobre a isolação de transformadores e, em 1948, foi desenvolvido um processo industrial nos Estados Unidos para a produção comercial do gás SF_6.

Na década de 60, iniciou-se a comercialização em larga escala do SF_6 na indústria elétrica nos Estados Unidos e na Europa, ao mesmo tempo em que eram lançados os primeiros disjuntores e chaves utilizando este gás.

[1] Norma cancelada em 26/11/2007.

Além do setor elétrico, o SF_6 possui aplicação em janelas anti-ruído misturado com argônio, devido à baixa velocidade de transmissão acústica; na indústria metalúrgica, como atmosfera de proteção na produção de magnésio e suas ligas; na purificação de ligas de alumínio; como gás de limpeza na fabricação de semicondutores; em aplicações médicas como contraste em ultra-som, pneumonectomias, doenças do ouvido médio, correção de descolamento de retina; refrigerante em cirurgias oftalmológicas; e como agente refrigerante e de extinção do fogo, uma vez que não é inflamável. Em algumas dessas aplicações, as normas técnicas e leis estão impondo restrições ao uso a partir do controle de consumo e de descarte.

12.3 APLICAÇÕES DO SF_6 NO SETOR ELÉTRICO

Dentre os principais equipamentos de média, alta e extra-alta tensão que se utilizam dos benefícios do SF_6 destacam-se: disjuntores, secionadores, transformadores para instrumentos, barramentos, linhas de transmissão, subestações blindadas (*Gas Insulated Substation* - GIS), além de aplicações na fabricação de semicondutores.

Das aplicações supracitadas, a que consome a maior quantidade de SF_6 e requer cuidados especiais para garantia da qualidade do SF_6 como elemento dielétrico e de extinção do arco elétrico são as subestações blindadas. A subestação blindada isolada a SF_6 é um conjunto de equipamentos de manobra, medição e proteção encapsulados em invólucro metálico aterrado, incluindo seus dispositivos de operação, comando, controle e proteção, no qual o isolamento é obtido parcialmente pelo SF_6 ao invés do ar à pressão atmosférica (ABNT, 1987).

Uma subestação isolada (GIS) a SF_6 traz como vantagem notória a necessidade de pouco espaço físico para sua implantação, entre 10% e 15% do espaço requerido por uma subestação isolada a ar, vantagem substancial em regiões metropolitanas de alta concentração demográfica.

A grande quantidade de disjuntores isolados a SF_6, instalados no Brasil, torna a massa total de SF_6 utilizada neste equipamento substancial, mesmo que a quantidade de gás por disjuntor seja muito menor em comparação com as subestações blindadas.

12.4 PROPRIEDADES FÍSICO-QUÍMICAS IMPORTANTES PARA A UTILIZAÇÃO DO SF_6 NO SETOR ELÉTRICO

Devido a grande eletronegatividade, alta capacidade de transferência de calor e baixa temperatura de ionização, o SF_6 é utilizado pela indústria elétrica como meio dielétrico e de extinção do arco elétrico. O tempo de extinção é aproximadamente 100 vezes menor no SF_6 do que no ar, sob condições semelhantes.

O SF_6 é um dos gases mais pesados conhecidos, apresentando uma densidade de 6,139g/ℓ a 21ºC e 1bar, ou seja, aproximadamente 5 vezes maior que a densidade do ar. Além disso, pode ser submetido a grandes variações de temperatura sem que isto represente grandes variações de pressão.

Ainda quanto ao comportamento térmico do SF_6, sabe-se que a 500°C tem início sua dissociação; a 3000°C há decomposição do SF_6 em íons de enxofre e flúor; após a extinção do arco a recomposição ocorre em aproximadamente 1000°C. Neste processo parte do SF_6 não se recompõe, dando origem a subprodutos. A Figura 12.2(a) ilustra o comportamento do SF_6 sob a influência do arco elétrico comparado ao Nitrogênio (N_2) e a Figura 12.2(b) sua condutividade térmica.

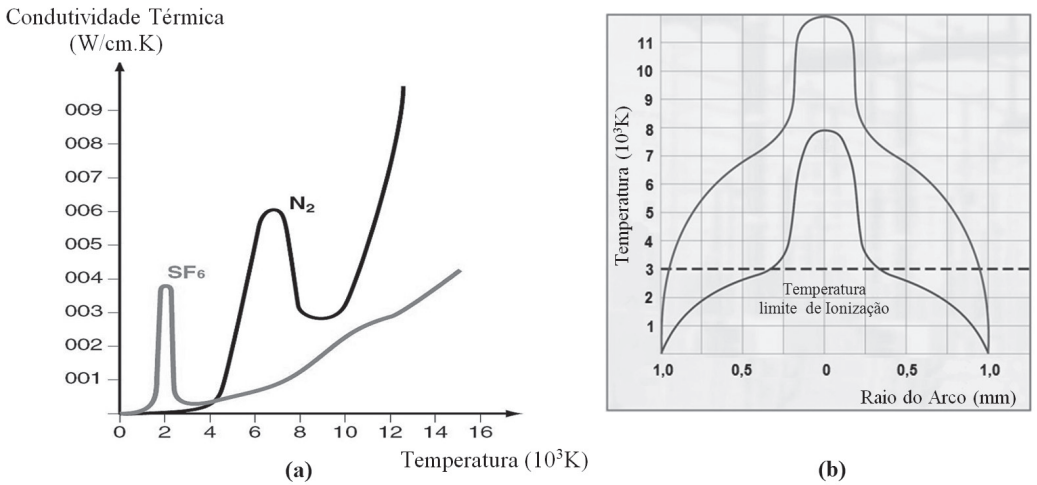


Figura 12.2: Comportamento térmico do SF_6 (KOCH, 2003 e THEOLEYRE, 1999).

Da Figura 12.2 (b) é possível ver que na região próxima do eixo do arco, onde a temperatura é muito elevada, a condutibilidade térmica do SF_6 é baixa, e a dissipação do calor se fará a um gradiente acentuado de temperatura. Na região pouco afastada do eixo do arco, a temperatura pode estar abaixo da temperatura de ionização do SF_6. Como consequência, a sua condutibilidade elétrica se torna praticamente inexistente, uma vez que o SF_6, por ser eletronegativo, tem grande facilidade em absorver elétrons livres. Por outro lado, em temperaturas baixas, a sua condutibilidade térmica é muito alta. Quando o valor instantâneo da corrente elétrica estiver bem próximo do seu zero natural, o arco fica reduzido a uma fina coluna cilíndrica com elevada temperatura, ao redor da qual há uma massa gasosa não condutora de eletricidade e cuja temperatura é relativamente baixa. Neste ponto, a rigidez dielétrica do SF_6, no espaço entre contatos, se recupera rapidamente, o arco se extingue e as tensões de restabelecimento com taxas elevadas de crescimento que venham a surgir não terão possibilidade de ocasionar a reiginição ou reacendimento do arco. Essas propriedades elétricas e térmicas do SF_6 tornam possível a interrupção de correntes acompanhadas de tensões de restabelecimento com taxas elevadas de crescimento dispensando, em alguns casos, a necessidade de resistores de pré-inserção.

A característica mais marcante do SF_6 frente a outros meios dielétricos atualmente em uso é a sua rigidez dielétrica. A 60 Hz e 1 bar em campo homogêneo, a rigidez dielétrica do SF_6, é da ordem de 2,3 a 2,5 vezes mais elevada do que os valores correspondentes para ar ou nitrogênio. A Figura 12.3 (a) mostra a rigidez dielétrica do SF_6 comparado ao óleo isolante e ao ar, onde se verifica que, para qualquer valor de pressão, a rigidez dielétrica do SF_6 é maior do que a do ar, e para uma pressão maior do que, aproximadamente, 2,75 bar o SF_6 supera também o óleo isolante. A Figura 12.3 (b) mostra a tensão elétrica isolada pelo SF_6 em uma comparação com o N_2 em função da pressão para diferentes distâncias de eletrodos (13mm, 25mm e 51mm).

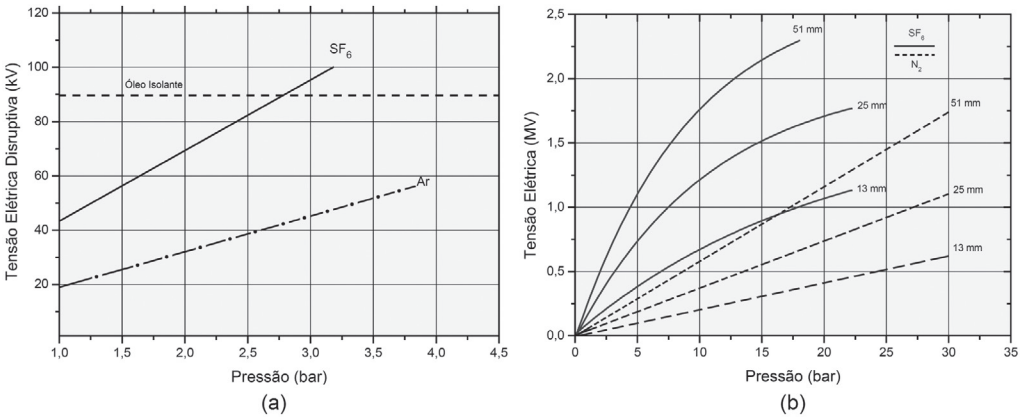


Figura 12.3: Característica dielétrica do SF_6 (SIHVENGER & TRINDADE, 2008).

Sob a influência de um arco elétrico, parte do SF_6 pode ser dissociada, conforme a fórmula 12.1:

$$SF_6 \rightarrow SF_5^- + F^- \qquad 12.1$$

Esta reação é reversível e, portanto, após a descarga, os produtos da dissociação se recombinam desde que não ocorra nenhuma reação secundária com moléculas de água, metais vaporizados, paredes do recipiente ou outros componentes em contato com o SF_6. Das reações secundárias podem resultar produtos sólidos e gasosos. Os produtos sólidos da decomposição, resultantes das descargas de alta energia, também são dielétricos, de modo que, quando depositados na forma de pó na superfície dos isoladores, de uma forma geral não prejudicam a eficácia operacional do equipamento. No entanto, este princípio aplica apenas se a umidade do gás no interior do equipamento for extremamente baixa. Se expostos à umidade, os produtos resultantes da decomposição do SF_6 se decompõem por hidrólise, formando produtos secundários que podem reagir com os materiais em contato com o SF_6.

Se a formação de produtos de decomposição não pode ser evitada por meio da utilização de métodos de construção adequados, a corrosão pode ser em grande parte evitada pela eliminação de umidade ou pelo emprego de materiais adequados. Metais e ligas comumente utilizados como o alumínio, aço, cobre e latão, permane-

cem praticamente livres de ataque corrosivo. Por outro lado, materiais como vidro, porcelana, papel isolante e materiais similares podem ser gravemente danificados proporcionalmente à concentração das substâncias corrosivas. Materiais isolantes, tais como resina epóxi, PTFE, polietileno, cloreto de polivinila e poliésteres, são apenas ligeiramente afetados.

12.5 DESVANTAGENS DA UTILIZAÇÃO DO SF_6 NO SETOR ELÉTRICO

A grande desvantagem associada ao uso do SF_6 em equipamentos elétricos está relacionada com o processo de formação de subprodutos, por decomposição do gás nas condições de operação de alguns equipamentos elétricos (por exemplo: disjuntores). Este processo de degradação é favorecido pelas altas temperaturas desenvolvidas durante o arco e pela presença de algumas impurezas: ar, CF_4, água, carbono, hidrogênio e sílica (base de muitos materiais isolantes), tungstênio, cobre e níquel (constituintes de ligas de aço). Nesse processo, a quebra de ligações S-F leva à formação de um grande número de subprodutos, muitos dos quais com características tóxicas e corrosivas.

Em termos ambientais, o SF_6 é aproximadamente 23.000 vezes mais nocivo para o efeito estufa que o dióxido de carbono. Portanto, sua emissão para a atmosfera é altamente danosa. Em face disso, legislações específicas e ações deliberadas por parte das empresas que utilizam o SF_6 buscam mitigar ao máximo a emissão deste gás para a atmosfera.

Quanto à segurança, apesar de não ser um gás tóxico, por ser mais denso que o ar, em ambientes fechados e de pouco espaço, expulsa o oxigênio causando asfixia e, em sua forma líquida, o vazamento do SF_6 pode causar congelamento.

12.6 REFERÊNCIAS REGULAMENTADORAS DA UTILIZAÇÃO DO SF_6 NO SETOR ELÉTRICO

Constatou-se, após o protocolo de Kyoto, uma preocupação crescente, das concessionárias de energia e órgãos regulamentadores

do setor elétrico, com as questões relacionadas com o meio ambiente em especial o efeito estufa. A bibliografia técnica-científica relacionada ao SF_6 reflete estas preocupações acompanhando a evolução dos conceitos e modernizando suas exigências e regulamentações.

Uma das instituições pioneiras no empenho para redução das emissões de SF_6 é a EPA - *Environmental Protection Agency* (Agência de Proteção Ambiental dos Estados Unidos). A EPA possui um programa voluntário que congregam concessionárias e fabricantes de equipamentos elétricos que utilizam SF_6 com o objetivo de reduzir emissões e propor boas práticas para manuseio e reciclagem do gás. Em seu repositório bibliográfico a instituição conta com diversos manuais e estudos de caso relacionados com o SF_6.

Outra instituição de referência em recomendações para o uso do SF_6 é o CIGRÉ - *Comité International des Grands Réseaux Electriques* (Comitê Internacional de Grandes Consumidores de Energia Elétrica). O CIGRÉ possui, além de pesquisas de âmbito mundial sobre o uso e a emissão de SF_6, diversas publicações que orientam a utilização do SF_6 para fins de isolação e extinção do arco elétrico. Estas publicações fundamentaram as exigências das normas IEC (*International Electrotechnical Commission*) quanto aos níveis de pureza do SF_6 reciclado e outras relacionadas aos disjuntores isolados a SF_6. As principais contribuições bibliográficas do CIGRÉ para os estudos relacionados ao uso do SF_6 em disjuntores são as seguintes: relatório da 2ª pesquisa mundial sobre defeitos e falhas em disjuntores, incluindo dados sobre o vazamento de SF_6; guia para entendimento do desempenho ambiental e funcional do SF_6 quando misturado a outros gases, principalmente N_2 e CF_4; guia de reciclagem do SF_6 no qual são abordadas as exigências de pureza e os procedimentos para manuseio e reciclagem do SF_6; guia para preparação de instruções para manuseio do SF_6 visando redução das perdas em campo; e, no Brasil, o guia para manuseio, segurança e manutenção de hexafluoreto de enxofre (SF_6) em equipamentos elétricos.

Os fabricantes de equipamentos elétricos que utilizam o SF_6 para fins de isolação e extinção do arco elétrico também estão sensibilizados quanto aos problemas gerados pela sua emissão ao meio ambiente. Prova disto são as publicações do CAPIEL (*Coordinating Committee for the Associations of Manufacturers of Industrial Electrical*

Switchgear and Control Gear in the European Union) um comitê de coordenação das associações de fabricantes de equipamentos elétricos da União Europeia. O CAPIEL possui diversas publicações relacionadas ao uso do SF_6 em equipamentos elétricos envolvendo questões técnicas e ambientais, incluindo um relatório que mostra a diminuição das emissões de SF_6 entre 1995 e 2005, proporcionadas por ações voluntárias dos fabricantes de equipamentos elétricos.

A preocupação com as emissões de SF_6 se reflete também entre os órgãos normativos que nos últimos anos fizeram atualizações profundas em suas normas para adequá-las às restrições clamadas pelos órgãos ambientais. Entre os exemplos deste fato estão: atualização das normas da IEC que tratam do controle e tratamento do SF_6 retirado de equipamentos elétricos incluindo especificações para sua reutilização; especificação da qualidade técnica do SF_6 para uso em equipamentos elétricos; utilização e manipulação do SF_6 em equipamentos de alta tensão; e, atualização das normas da ABNT (Associação Brasileira de Normas Técnicas) que tratam dos disjuntores de alta tensão (NBR/IEC 62271) e especificação do SF_6 (NBR/IEC 11902). Da ABNT, resta atualizar as normas que tratam da verificação das propriedades (NBR/IEC 12160) e procedimentos, relacionados ao SF_6 (NBR/IEC 12318) as quais seguramente serão atualizadas seguindo recomendações da IEC.

12.7 ASPECTOS DE SEGURANÇA QUE DEVEM SER OBSERVADOS NO MANUSEIO DO SF_6

Quando presente em concentrações superiores a 35% em volume no ar ambiente, o SF_6 pode provocar a asfixia devido à redução do teor de oxigênio do ar para valores inferiores ao mínimo necessário para a respiração (17% em volume). O risco de concentrações elevadas do SF_6 é maior em instalações localizadas ao nível do solo, ambientes não ventilados e/ou que possuam porões e dutos. Para manter e/ou garantir a concentração do SF_6 abaixo do limite de tolerância é necessário a utilização de métodos adequados de exaustão. Nos locais onde a exaustão geral não é adequada utiliza-se respiradores com suprimento de ar. Em espaços confinados ou quando houver deficiência de oxigênio na atmosfera, deve-se utilizar equipamento autônomo de respiração com proteção facial total na pressão positiva.

Pelo fato do SF_6 estar pressurizado tanto durante seu armazenamento quanto na utilização há que se prever os riscos de explosões inerentes e o congelamento durante sua expansão que, em contato com a pele ou os olhos, podem trazer riscos à saúde.

Além dos equipamentos e cuidados supracitados os seguintes EPI's são recomendados: óculos de segurança com lente incolor e proteção lateral; luvas protetoras de raspa para manusear cilindros e prevenir contra a exposição ao SF_6 liquefeito; e sapatos de segurança.

12.8 REUTILIZAÇÃO DO SF_6 EM EQUIPAMENTOS ELÉTRICOS

O SF_6 deve ser continuamente reutilizado ao longo de todo o ciclo de vida do equipamento, ou seja, desde seu desenvolvimento e testes até o seu decomissionamento, incluindo a fase de comissionamento, manutenção e reparo. Ele pode também ser transferido do equipamento que está sendo substituído para o equipamento sendo instalado. Assim, o gás percorre um ciclo contínuo de reutilização. Essa reutilização sistemática do SF_6 exige que o gás seja mantido num nível de qualidade tal que ele possa realizar suas funções. Isso é conseguido por meio do manuseio correto e da reciclagem em campo.

O termo reciclagem abrange a recuperação e reutilização do SF_6. Para o caso do gás que não pode ser imediatamente recuperado em campo, deve-se prever purificação adicional em laboratório ou companhia de reprocessamento especializada para posterior remoção do eco-ciclo de forma compatível com o ambiente. A recuperação eficiente e a reutilização do SF_6 em campo exigem (CIGRÉ, 2003):

- Equipamentos elétricos projetados para facilitar a reciclagem, permitindo a reutilização do SF_6;
- Equipamentos de reciclagem adequados associados a procedimentos para reciclagem e manuseio;
- Padrão de pureza para a reutilização do gás reciclado, o que inclui: conhecimento das origens e quantidades dos contaminantes que resultam do uso do SF_6 em equipamentos elétricos;

- Métodos para verificar a qualidade do SF_6 reciclado;
- Também, e dentro de uma perspectiva de longo prazo, um conceito para o descarte final do SF_6, para que se possa removê-lo do eco-ciclo transformando-o em substâncias compatíveis com o meio ambiente.

Como o SF_6 é contido e não consumido ou liberado, a reciclagem pode ser facilmente introduzida como uma parte natural do seu manuseio. Por esta razão, os usuários do SF_6 devem estabelecer políticas de reciclagem sistemática e mitigação das emissões para a atmosfera, diminuindo perdas por vazamentos nos equipamentos, quer seja durante a vida útil do equipamento que contém o SF_6 ou durante ações de reparo e/ou atualização tecnológica. Esta política deve ser sustentada com padronizações, procedimentos, equipamentos apropriados e programas sistemáticos de capacitação de pessoal.

12.9 FUNCIONAMENTO DE UM EQUIPAMENTO DE RECICLAGEM DE SF_6

O funcionamento básico de um equipamento de reciclagem (reciclador) de SF_6 é mostrado na Figura 12.4. Seus principais componentes são: filtros; compressor(es); bomba de vácuo; e cilindro de armazenamento. As principais etapas do processo de reciclagem são:

- Remoção do gás: depois de extraído do equipamento o SF_6 é filtrado para então ser comprimido dentro de um cilindro de armazenamento.
- Reutilização / reabastecimento: a reutilização do SF_6 reciclado (purificado) só ocorre depois da remoção do ar do equipamento de reciclagem, com o auxílio de uma bomba de vácuo (tubulações de remoção). O equipamento é, então, reabastecido com o SF_6 do cilindro utilizando-se um compressor de pistão para SF_6 (tubulação de reabastecimento). É aconselhável utilizar tubulações distintas para remoção e reabastecimento do SF_6 evitando, assim, a sua contaminação por partículas.

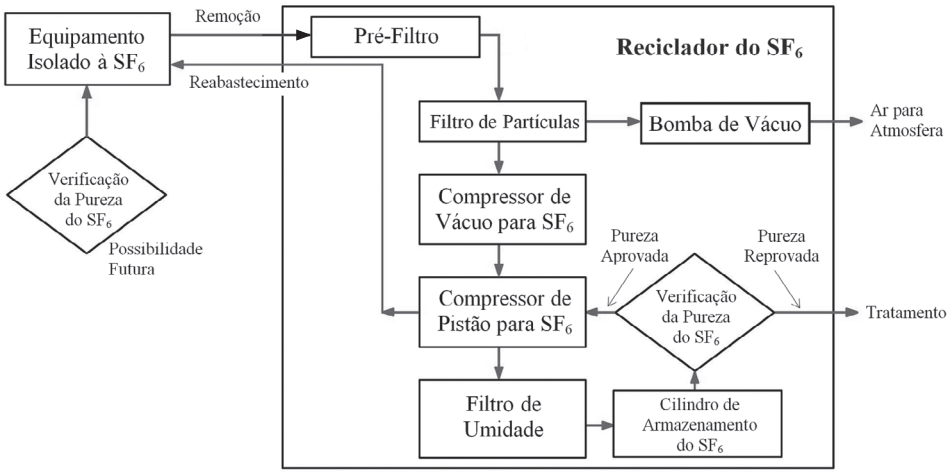


Figura 12.4: Esquema funcional básico de um reciclador de SF_6 (CIGRÉ, 2003)

12.10 FONTES E EFEITOS DA CONTAMINAÇÃO DO SF_6 EM EQUIPAMENTOS ELÉTRICOS

As substâncias contaminantes do SF_6 geradas em equipamentos elétricos têm como fontes principais: manuseio do SF_6; vazamentos; dessorção de superfícies, partes componentes e adsorvedores; decomposição por descargas parciais; reações secundárias da descarga de produtos de decomposição; e geração mecânica de partículas de poeira. Os níveis em que estes agentes contaminantes se apresentam dependem, principalmente, do projeto, fabricação e montagem do equipamento; do processo de manuseio do gás; do projeto do adsorverdor; e da atividade de descarga acumulada (CIGRÉ, 2003).

Uma deterioração funcional do equipamento pelos agentes contaminantes do SF_6 pode, de um modo geral, apresentar riscos cujos efeitos levam às seguintes consequências: riscos para a saúde dos operadores e manutentores; corrosão do equipamento; emissão de SF_6 para a atmosfera; perda de desempenho de isolamento; perda da capacidade de chaveamento (somente para subestações blindadas); e diminuição da taxa de transferência de calor.

12.11 CLASSIFICAÇÃO E EXIGÊNCIAS DE QUALIDADE DO SF_6

Classes de classificação do SF_6:

- SF_6 novo: gás adquirido em cilindros, conforme fornecido pelos fabricantes originais do SF_6 e obedecendo ao padrão do SF_6 novo, conforme o estabelecido pelo IEC 60376, ou um padrão nacional, como, por exemplo, a NBR 11902. Uma vez que o gás tenha sido retirado dos cilindros nos quais foi colocado pelo fabricante ele deve ser considerado gás usado.
- SF_6 sem arco: gás que foi de alguma maneira, manuseado, porém, que não sofreu arco. Os maiores agentes contaminantes do gás sem arco podem ser o ar (introduzido, principalmente, quando do manuseio) e a umidade (dessorvida das superfícies). Pequenas quantidades de produtos de decomposição do SF_6 (variando normalmente entre 100ppmv) podem também estar presentes quando as descargas parciais já ocorreram no gás.
- SF_6 com arco normal: gás recuperado após operação normal de chaveamento. O SF_6 com arco normal pode conter, além do ar e da umidade, produtos da decomposição e subprodutos gerados pela ação do arco elétrico.
- SF_6 com arco intenso: gás reciclado do equipamento no qual ocorreu arco devido a uma falha. Nesse caso, esperam-se níveis altos de agentes contaminantes sólidos e gasosos em grande porcentagem de volume.

As verificações da qualidade do SF_6 reciclado são feitas para que os níveis de impureza residual não excedam os valores normalizados. São verificados: o total de agentes contaminantes gasosos e não-reagentes (principalmente o Ar e o CF_4); o total de produtos de decomposição gasosos e reagentes; agentes contaminantes líquidos e sólidos tais como óleo, poeira, partículas e a umidade. A Tabela 12.1 mostra os contaminantes do SF_6, suas principais origens e seus efeitos deteriorantes.

Tabela 12.1: Contaminantes do SF_6 (CIGRE, 2003).

Contaminante	Principal Origem	Efeito Deteriorante
Ar | CF_4	Manuseio | chaveamento | arcos internos	Chaveamento | isolação do SF_6
Umidade	Dessorção das superfícies e dos polímeros	Isolação superficial por condensação de líquido e assim as outras células
SF_4 | WF_6 | HF | SO_2 SOF_2 | SOF_4 | SO_2F_2	Arco interno | Descargas parciais | Reações Secundárias	Isolação superficial | Toxicidade
CuF_2 | WO_3 | WO_2F_2 WOF_4 | AlF_3	Erosão de contato | Arco interno	Toxicidade
Carbono Partículas metálicas	Carbonização de polímeros | Desgaste Mecânico	Isolação superficial | Isolação do SF_6
Óleo	Bombas e lubrificações	Isolação superficial

A Figura 12.5 ilustra o procedimento padrão de decisão para a verificação da qualidade do SF_6 reciclado. O SF_6 novo pode conter contaminantes provenientes de seus processos de fabricação e purificação ou do seu manuseio, transporte e transvazamento. Os provenientes dos processos de fabricação e purificação são, principalmente, o tetrafluoreto de carbono (CF_4), o fluoreto de hidrogênio (HF) e os fluoretos solúveis, enquanto que os provenientes da manipulação são, principalmente, o ar, a umidade e o óleo mineral. Esses contaminantes podem alterar as características do SF_6 de três formas distintas: quanto à sua toxidez, corrosividade e rigidez dielétrica.

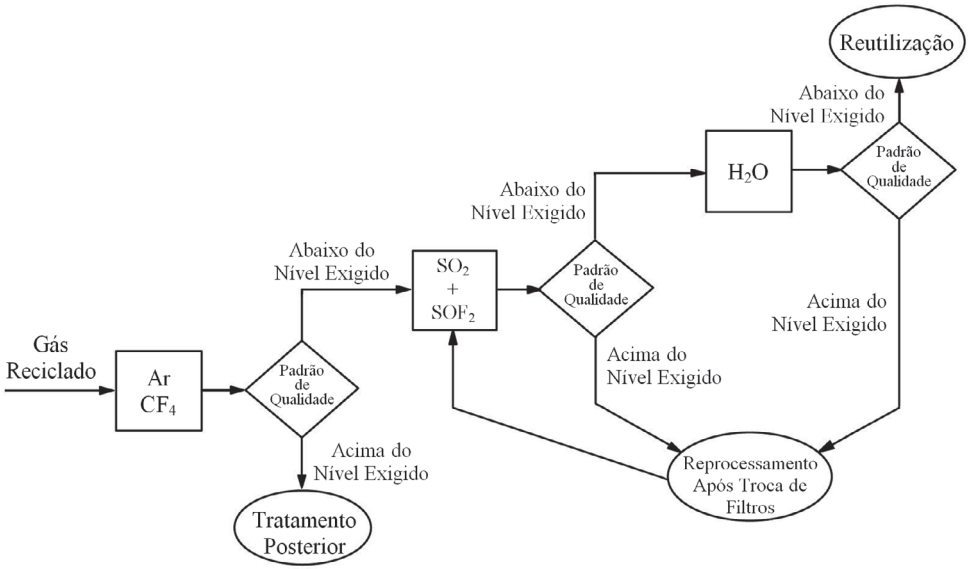


Figura 12.5: Procedimento para a verificação da qualidade do SF_6 reciclado (CIGRE, 2003).

A maioria das impurezas presentes no SF_6 novo está em concentração tão baixa, que praticamente não afeta a rigidez dielétrica do produto. Os teores máximos aceitáveis dessas impurezas no SF_6 novo, segundo a IEC 60376 (IEC, 2005) e a NBR 11902 (ABNT, 1992a) são mostrados na Tabela 12.2.

Tabela 12.2: Níveis máximos de impurezas para o SF_6 novo (IEC, 2005; ABNT, 1992a).

Conteúdo	**Especificação** (NBR 11092/2010)	IEC 60376/2005		
		Especificação	**Método analítico (somente para indicação)**	**Incerteza**
Ar (O_2 + N_2)	500 mg/kg [6]	2000 mg/kg [1]	Absorção infra-vermelho	35 mg/kg
			Cromatografia gasosa	3 – 10 mg/kg
			Densidade	10 mg/kg
CF_4	500 mg/kg [6]	2400 mg/kg [2]	Cromatografia gasosa	9 mg/kg

H_2O	15 mg/kg [6]	25 mg/kg [3]	Gravimétrico	9 mg/kg
			Eletrolítico	2 – 15 mg/kg
			Ponto de orvalho	1 °C
Óleo mineral	10 mg/kg [6]	10 mg/kg	Fotométrico	< 2 mg/kg
			Gravimétrico	0,5 mg/kg [5]
Acidez Total (expressa em HF)	1 mg/kg [6]	1 mg/kg [4]	Titulação	0,2 mg/kg

1) 2 g/kg é equivalente a 1% vol. sob condições ambientes (100 kPa e 20ºC).
2) 2400 mg/kg é equivalente a 4000 ml/l sob condições ambientes (100 kPa e 20ºC).
3) 25 mg/kg é equivalente a 200 ml/l e para um ponto de orvalho de –36ºC, medido em condições ambientes (100 kPa e 20ºC).
4) 1 mg/kg é equivalente a 7,3 ml/l sob condições ambientes (100 kPa e 20ºC).
5) Dependendo da quantidade da amostra.
6) Método de ensaio definido pela ABNT NBR 12160.

12.12 RECOMENDAÇÕES PARA ARMAZENAMENTO E TRANSPORTE DO SF_6

Os contêineres de armazenamento e transporte do SF_6 novo devem adequar-se às legislações nacionais para contêineres de pressão. No Brasil, os critérios de identificação para o transporte terrestre, manuseio, movimentação e armazenamento de produtos são definidos pela ABNT NBR 7500/2009. O SF_6 novo pertence à classe dos gases não inflamáveis, não corrosivos e com baixa toxidez e, neste caso, a simbologia de identificação para o transporte é a mostrada na Figura 12.6.

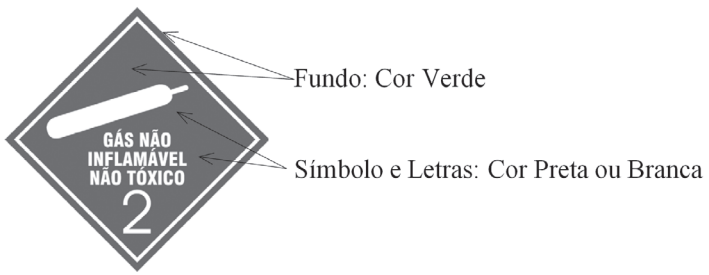


Figura 12.6: Simbologia para identificação e transporte do SF_6 (ABNT, 2009)

O SF_6 reciclado pode necessitar um armazenamento temporário em campo, e ser transportado para outros locais para sua reutilização ou posterior purificação. Isto exige regulamentações para um armazenamento adequado em nível internacional. Nenhuma das regulamentações atuais menciona explicitamente "Hexafluoreto de Enxofre (SF_6) usado". Em razão disso, e até o momento, acaba sendo classificado dependendo das características e quantidades dos seus agentes contaminantes. Os critérios principais para a classificação do transporte do SF_6 usado e contaminado são as características tóxicas e de corrosão dos agentes contaminantes e suas concentrações.

12.13 PROCEDIMENTO PARA DESCARTE FINAL DO SF_6

Nos casos em que o SF_6 não é reciclável ou quando o mesmo não é mais necessário, pode ser eliminado de um modo ambientalmente adequado submetendo-o a um processo térmico.

Quando aquecido acima de 1000°C, o SF_6 começa a se dissociar em fragmentos (espécies reativas) que reagem com outras substâncias, principalmente o hidrogênio (H) e o oxigênio (O) para formar óxido de enxofre (SO) e ácido fluorídrico (HF). O SF_6 pode, assim, ser destruído com uma eficiência de remoção maior que 99% quando o processo térmico opera a 1200ºC. Os produtos da reação SO e HF são removidos passando-se os produtos da reação através de um filtro contendo hidróxido de cálcio umedecido ($Ca(OH)_2$). Durante este processo, se formam sulfatos sólidos e fluoretos, como: sulfato de cálcio ($CaSO_4$ - Gesso) e fluoreto de cálcio (CaF_2) (CIGRÉ, 2003).

12.14 CONSIDERAÇÕES FINAIS

Devido a suas excelentes características como meio isolante e de extinção do arco elétrico, o SF_6 ainda será o dielétrico preferencial em equipamentos elétricos por alguns anos. Esta longevidade seguramente está atrelada ao desenvolvimento de disjuntores de estado sólido (semicondutores) ou de outras técnicas de extinção mais eficientes, principalmente para os níveis de tensão da rede básica (≥ 230kV).

Quanto à manutenção do SF_6, a principal preocupação é com a umidade. As principais fontes de umidade são os invólucros e

condutores de alumínio e os isoladores de resina epóxi. Atenção especial, também, deve ser dada a logística do SF_6, tanto para evitar sua contaminação quanto seu lançamento para a atmosfera.

Por questões ambientais, as normas que regulamentam a utilização do SF_6 em disjuntores estão cada vez mais restritivas quanto ao lançamento deliberado do SF_6 para a atmosfera. Tal procedimento deve ser evitado e técnicas de reciclagem implementadas para reaproveitamento do gás ou, caso isso não seja mais possível, proceder-se com o descarte de forma ambientalmente correta.

Capítulo 13

DISJUNTORES ISOLADOS A SF_6

Este capítulo aborda os aspectos gerais e as partes constituintes dos disjuntores isolados a Hexafluoreto de Enxofre (SF_6). O objetivo é apresentar de forma mais detalhada o disjuntor para auxiliar o entendimento e a aplicação das técnicas de análise apresentadas nos capítulos anteriores.

13.1 ASPECTOS GERAIS

A excelente qualidade de extinção e de isolamento do arco elétrico proporcionadas pelo SF_6 permitiu um considerável avanço na tecnologia de fabricação dos disjuntores. Tal avanço resultou na diminuição no tamanho dos disjuntores e consequentemente no uso de menor quantidade de SF_6 para uma mesma capacidade de interrupção. Associado a isso, as técnicas de interrupção avançaram, exigindo cada vez menos energia para operação dos disjuntores, ao mesmo tempo em que permitem incrementos na capacidade de interrupção.

Embora o SF_6 tenha sido sintetizado pela primeira vez em 1900, somente 30 anos depois foi utilizado em transformadores, e, no final dos anos de 1940, teve início o desenvolvimento de disjuntores e chaves para abertura em carga, isolados a SF_6.

O disjuntor é definido, segunda a IEC 60050/2009, como sendo um dispositivo mecânico de manobra, capaz de estabelecer, conduzir e interromper correntes nas condições normais do circuito, assim como estabelecer, conduzir durante um tempo especificado e interromper correntes sob condições anormais especificadas do circuito, tais como as de curto circuito. O Quadro 13.1 sintetiza as principais funções do disjuntor.

	Condição Operacional		
Função	**Corrente Nominal**	**Sobrecarga**	**Curto-Circuito**
Conduzir	X	X	X
Interromper	X	X	X
Estabelecer	X	X	X
Isolar	Não		

Quadro 13.1: Síntese das funções do disjuntor.

Os aspectos normativos dos disjuntores para uso interno ou externo em tensão acima de 1.000V em corrente alternada de 50 ou 60 Hz (objeto deste capítulo) são tratados pela norma ABNT NBR/IEC 62271/2006 Parte 100 – Disjuntores de alta tensão de corrente alternada.

13.2 HISTÓRICO DO DESENVOLVIMENTO DOS DISJUNTORES ISOLADOS A SF_6

Segundo Vorpe et al. (1996), os disjuntores com contatos de interrupção envoltos pelo ar são os mais simples e, historicamente, foram os primeiros a serem utilizados. Para atender ao crescimento da potência de interrupção e à elevação dos níveis de tensão no sistema elétrico, surgiram os disjuntores isolados a óleo mineral isolante. Na década de 30, os disjuntores a ar comprimido apareceram como a melhor técnica de extinção do arco elétrico na alta tensão, contrapondo-se aos disjuntores isolados a óleo, responsáveis por acidentes graves provocados por explosão e incêndio. Em 1953 foi construído nos Estados Unidos o primeiro protótipo do disjuntor a isolado à SF_6 para aplicação em alta tensão. Já os disjuntores a vácuo foram fabricados no início dos anos 70, com boa aceitação para utilização em média tensão. A nova linha de evolução aponta para o uso de disjuntores a semicondutores, cujo futuro é promissor, pois são os que mais se aproximam do disjuntor ideal.

Os primeiros disjuntores de SF_6 eram do tipo dupla pressão, com funcionamento similar aos disjuntores a ar comprimido. O SF_6 era armazenado em um recipiente de alta pressão (aproximadamente 16 kgf/cm^2) e liberado sobre a região entre os contatos do disjuntor. A principal diferença com relação aos disjuntores a ar comprimido consistia no fato do SF_6 não ser descarregado para a atmosfera após atravessar as câmaras de interrupção, e sim para um tanque com SF_6 a baixa pressão (aproximadamente 3 kgf/cm^2). Assim, o gás a alta pressão era utilizado

para interrupção do arco e o SF_6, a baixa pressão, servia à manutenção do isolamento entre as partes energizadas e a terra. Após a interrupção, o gás descarregado no tanque de baixa pressão era bombeado novamente para o reservatório de alta pressão, passando por um filtro de alumina ativada para remoção de produtos da decomposição.

As principais desvantagens dos disjuntores a SF_6 de dupla pressão eram a baixa confiabilidade dos compressores de gás e a tendência do SF_6 liquefazer-se à temperatura ambiente quando comprimido (a temperatura de liquefação do SF_6 a 16 kgf/cm^2 é 10°C), o que obrigava a instalação de aquecedores no reservatório de alta pressão com consequente aumento da complexidade e redução da confiabilidade. Essas desvantagens resultaram na descontinuidade da fabricação destes disjuntores e no desenvolvimento do disjuntor de pressão única.

Os disjuntores de pressão única, também chamados do tipo "impulso" ou *puffer*" são assim denominados porque o SF_6 permanece no disjuntor, durante a maior parte do tempo, a uma pressão constante de 3 a 6 kgf/cm^2. A pressão necessária à extinção do arco é produzida individualmente nas câmaras de extinção por um dispositivo (*puffer*) formado por um pistão e um cilindro soprador. Ao se movimentarem, estes elementos deslocam consigo o contato móvel e comprimem o gás existente no interior do cilindro (Figuras 13.1).

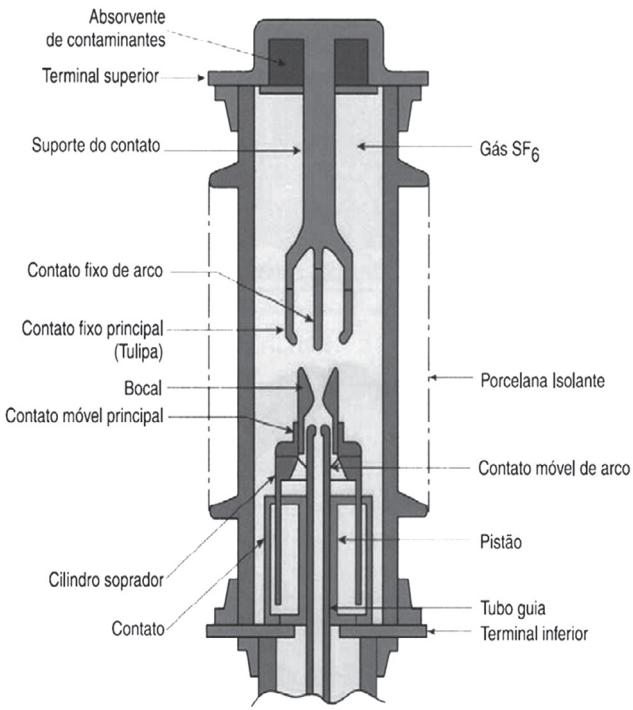
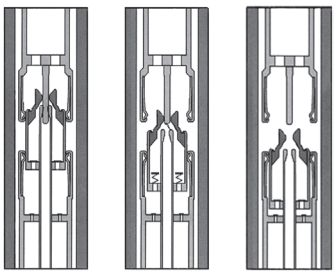


Figura 13.1: Contatos do disjuntor isolado a SF_6 de pressão única (TRAFO, 2009).

A compressão do SF_6 por esse processo produz pressões da ordem de 2 a 6 vezes a pressão original. No intervalo entre a separação dos contatos e o fim do movimento o gás comprimido é forçado a fluir entre os contatos e através de uma ou duas passagens (*nozzles*), extinguindo o arco de forma semelhante ao dos disjuntores de dupla pressão (Figuras 13.2).



a) Contatos fechados

b) Contatos em processo de abertura

c) Contatos abertos (isolados)

Figura 13.2: Processo de abertura dos contatos - disjuntor isolado a SF_6 de pressão única (AREVA, 2006).

O desenvolvimento e a disseminação dos disjuntores a SF_6 estão ligados ao aprimoramento das técnicas de selagem dos recipientes e detecção de vazamentos de gás. Estes aprimoramentos permitem reduzir os vazamentos de SF_6 nos disjuntores em níveis inferiores a 1% por ano.

13.3 CLASSIFICAÇÃO DOS DISJUNTORES

Os disjuntores podem ser classificados segundo diversos critérios, os próximos itens esclarecem alguns destes critérios.

13.3.1 CLASSE DE TENSÃO

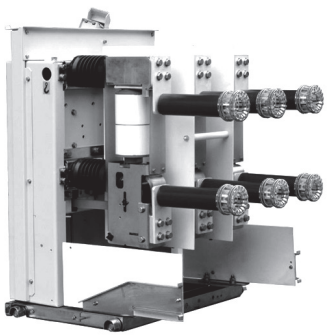
Quanto à classe de tensão, ou seja, o nível de tensão para o qual o disjuntor está dimensionado e apto a ser aplicado tem-se:

- Baixa Tensão (BT), onde: BT < 1 kV;
- Média Tensão (MT), onde: 1 kV ≤ MT < 69 kV;
- Alta Tensão (AT), onde: 69 kV ≤ AT ≤ 230 kV;
- Extra Alta Tensão (EAT), onde: 230 kV < EAT < 800 kV;
- Ultra Alta Tensão (UAT) onde: UAT ≥ 800 kV.

13.3.2 TIPO DE INSTALAÇÃO

Quanto à instalação e ,consequentemente, o grau de impacto das influências externas, tem-se:

- Instalação Interna: o disjuntor está dimensionado para instalação abrigada em cabines ou compartimentos protegidos das intempéries (Figura 13.3a);
- Instalação Externa: o disjuntor está dimensionado para instalação ao tempo e, portanto sujeito às intempéries (Figura 13.3b).



a) Instalação Interna

b) Instalação Externa

13.3.3 ISOLAÇÃO DA CÂMARA DE EXTINÇÃO

Segundo a ABNT NBR/IEC 62271-100/2006 quanto à isolação da câmara de extinção tem-se:

- Disjuntor de tanque vivo: neste caso, as partes ativas de interrupção são inseridas em um invólucro, o qual está no potencial da linha e isolado da terra. Suas principais características são o baixo custo (quando desprovido de transformador de corrente), o menor espaço para montagem e a menor quantidade de fluído isolante (Figura 13.4a);
- Disjuntor de tanque morto: as partes ativas de interrupção são inseridas em um invólucro metálico aterrado. Suas

principais características são: facilidade para instalação de transformadores de corrente em ambos os lados do disjuntor, maior resistência a abalos sísmicos e ajuste e montagem feitos na fábrica (Figura 13.4b).

a) Disjuntor de Tanque Vivo

b) Disjuntor de Tanque Morto

13.3.4 DIELÉTRICO QUE ENVOLVE OS CONTATOS

O processo evolutivo da tecnologia dos disjuntores esteve sempre atrelado ao meio dielétrico que envolve os contatos. O meio dielétrico também determinou o ritmo e a necessidade de modernização dos mecanismos de extinção do arco elétrico. Entre os principais meios dielétricos tem-se: ar comprimido, óleo, vácuo, SF_6 e semicondutores. A Figura 13.5 mostra os níveis de tensão em que estes meios isolantes são ou foram utilizados ao longo do processo de desenvolvimento dos disjuntores e seu predomínio ao longo dos anos para o nível de média tensão.

Na Figura 13.5(a) percebe-se que o ar comprimido e o SF_6 são adequados para os níveis de tensão mais altos, o óleo e o vácuo para os níveis intermediários de tensão e o ar para níveis de tensão mais baixos. Esta constatação está fortemente atrelada ao desenvolvimento tecnológico dos mecanismos de extinção, o que faz com que atualmente o vácuo e o SF_6 sejam os meios dielétricos predominantes para quase todos os níveis tensão, conforme mostra a Figura 13.5(b).

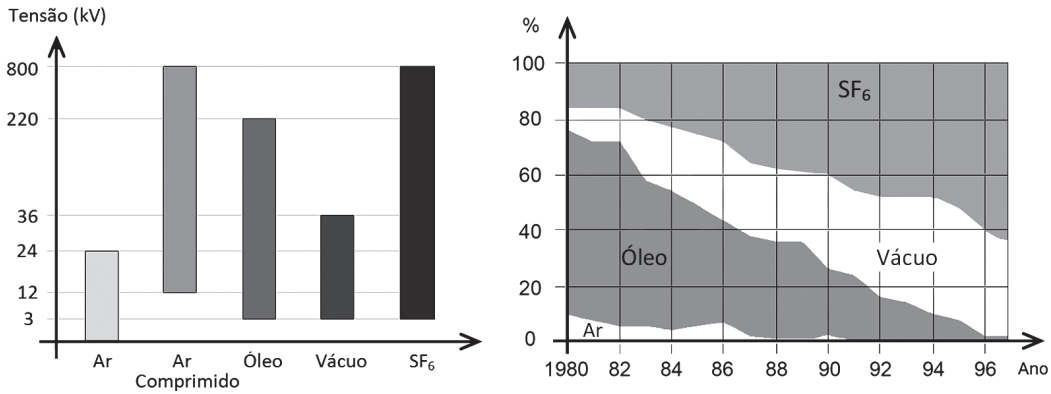


Figura 13.5: Meio isolante em função do nível de tensão (THEOLEYRE, 1999).

13.4 PARTES CONSTITUINTES DO DISJUNTOR

A Figura 13.6 mostra um disjuntor de tanque vivo, isolado a SF_6, para instalação externa e cujas partes principais indicadas são descritas na sequência.

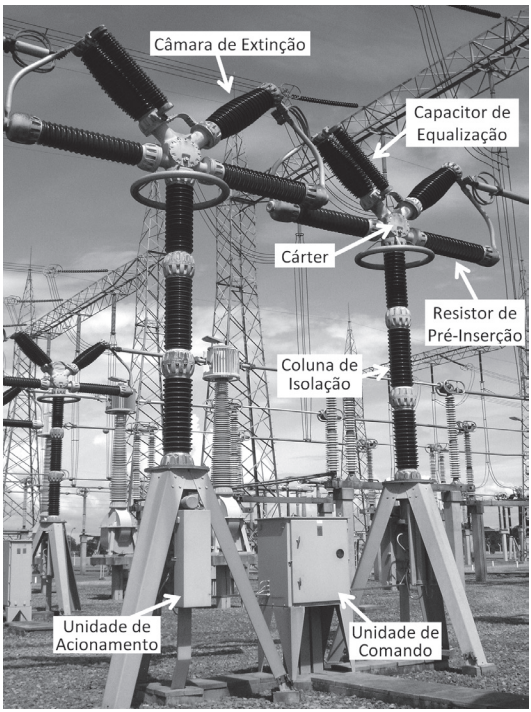


Figura 13.6: Partes constituintes de um disjuntor (ELETROSUL, 2008)

13.4.1 CÂMARA DE EXTINÇÃO

A câmara de extinção é o compartimento que envolve os contatos do circuito principal do disjuntor. Suas funções, além da contenção do SF_6, são: confinar o arco elétrico, favorecer a sua extinção, resistir às solicitações térmicas e mecânicas do processo de extinção e suportar estruturalmente os terminais, os contatos principais e seus mecanismos de atuação.

13.4.2 CAPACITOR DE EQUALIZAÇÃO

O capacitor de equalização de potencial é utilizado em disjuntores com múltiplas câmaras de extinção. A finalidade é garantir que durante o processo de abertura e com o disjuntor aberto a tensão sobre as câmaras de extinção seja a mais uniforme possível.

13.4.3 RESISTOR DE PRÉ-INSERÇÃO

O resistor de pré-inserção é instalado, em câmara auxiliar, em paralelo com o contato principal do disjuntor, entrando em operação durante o processo de abertura e/ou fechamento do disjuntor. Durante o processo de abertura do disjuntor, suas funções principais são: equalizar as tensões nas câmaras de extinção; reduzir as sobretensões devidas à abertura de cargas indutivas; reduzir a taxa de crescimento e o pico da TTR (Tensão Transitória de Restabelecimento) em faltas terminais e quilométricas; e reduzir a TTR durante a abertura de correntes capacitivas. Durante o processo de fechamento do disjuntor, suas funções principais são: limitar a corrente durante o fechamento de cargas capacitivas; reduzir as sobretensões que ocorrem durante o fechamento de linhas longas.

13.4.4 CÁRTER OU MECANISMO DE ACIONAMENTO

O cárter é a parte do disjuntor responsável pela transferência do movimento proveniente da haste de manobra para as câmaras de extinção e resistores de pré-inserção, com o auxílio dos mecanismos nele contidos. O cárter também contém SF_6 como meio dielétrico, porém, o gás está hermeticamente isolado daquele que circula entre

as câmaras de extinção, resistores e coluna de isoladores. Isso permite a substituição de qualquer câmara ou resistor sem afetar a pressurização das outras partes do disjuntor.

13.4.5 COLUNA DE ISOLAÇÃO/SUPORTE

A coluna de isolação acomoda a haste de manobra que transmite o movimento da unidade de acionamento (hidráulica ou mola) para o cárter. A coluna de isolação também contém SF_6, cuja função é isolar a coluna, além de circular pelas câmaras e resistores para auxiliar na refrigeração. Além disso, a coluna de isolação mantém a distância de isolamento entre o solo e os componentes da câmara de extinção, no caso de disjuntores de tanque vivo e serve de suporte para a estrutura, composta pela câmara de extinção, resistor, capacitor e cárter. Os isoladores da coluna de isolação são unidos por flanges e as vedações são críticas por evitar que o SF_6 entre em contato com a umidade.

13.4.6 UNIDADE DE COMANDO

Trata-se do subconjunto que abrange os elementos de comando, controle e supervisão do disjuntor. Seus componentes e suas características funcionais dependem do tipo de acionamento e do meio extintor. Por exemplo: um disjuntor a SF_6 com acionamento eletro-hidráulico deverá ter sistemas de supervisão da densidade do gás e pressão do óleo, incorporados a unidade/painel de comando, enquanto que um disjuntor a óleo com acionamento à mola dispensa este tipo de supervisão. A unidade de comando poderá também incorporar detalhes funcionais e dispositivos para contemplar requisitos específicos do usuário.

13.4.7 UNIDADE DE ACIONAMENTO

É o subconjunto que possibilita o armazenamento da energia necessária à operação mecânica do disjuntor, bem como a liberação desta energia pela ação de mecanismos apropriados, quando do comando de abertura ou fechamento do disjuntor. A Tabela 13.2 mostra as principais combinações de mecanismos de armazenamento de energia para abertura e fechamento do disjuntor.

Tabela 13.2: Métodos de acumulação de energia para abertura e fechamento do disjuntor.

Fechamento	Abertura
Mola	Mola
Mola	Ar comprimido
Ar comprimido	Ar comprimido
Solenóide (Bateria)	Mola
Óleo - Pneumático	Mola
Óleo - Pneumático	Óleo - Pneumático

A unidade de acionamento deve satisfazer às seguintes necessidades: acelerar as massas das partes móveis; vencer as forças de atrito; o esforço oposto do amortecedor; a resistência do injetor de SF_6 (*puffer*); as forças eletromagnéticas; e acumular energia na mola de abertura. Atualmente, o mecanismo mais utilizado, tanto para fechamento quanto para abertura do disjuntor, é a mola com carregamento motorizado alimentado por bateria.

13.5 FORMAÇÃO E EXTINÇÃO DO ARCO ELÉTRICO EM DISJUNTORES SF_6

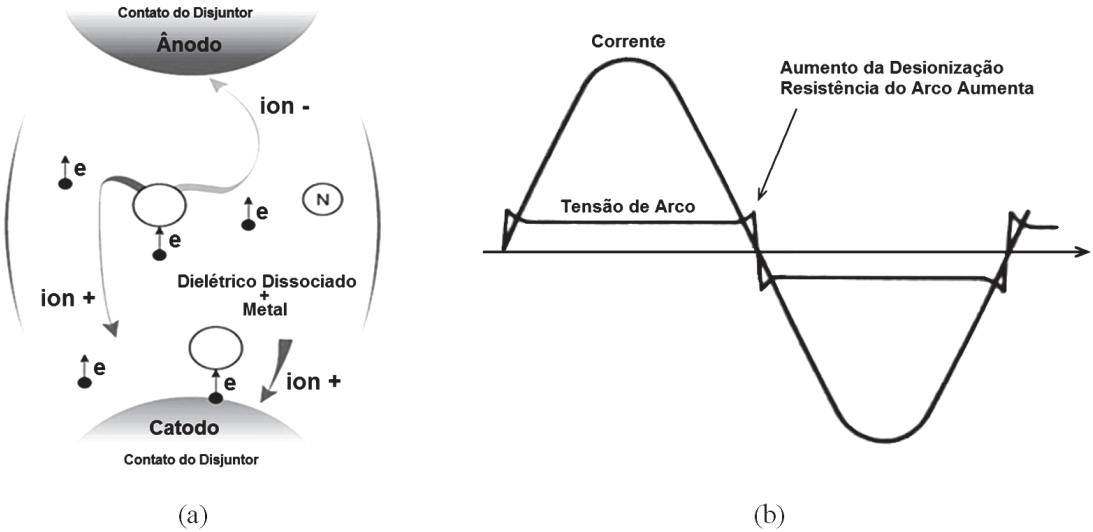
O arco elétrico é um fenômeno que ocorre quando se separam dois terminais de um circuito que conduz determinada corrente de carga, sobrecarga ou de defeito. Em função disso, em um meio fortemente ionizado cria-se um canal condutor com brilho intenso, o qual eleva significativamente a temperatura do entorno no qual o arco se desenvolve.

13.5.1 INTERRUPÇÃO DO ARCO ELÉTRICO

O processo de interrupção da corrente elétrica por um disjuntor a SF_6 inicia-se com a formação do arco entre os contatos principais, assim que tiver início a sua separação. A elevada temperatura do arco, estimada entre 10.000 a 30.000 ^oK, causa a decomposição do gás, havendo a formação de SF_2 e SF_4, principalmente, e em pequenas quantidades de S_2, F_2, S e F, além de outras substâncias. Ao mesmo tempo, há a vaporização do metal dos contatos que reage com parte

dos produtos da decomposição do SF_6, formando-se um pó esbranquiçado com boas propriedades isolantes e que se deposita nas paredes e contatos da câmara de extinção, sendo também, em parte, absorvido pela alumina ativada existente no interior da câmara. Uma parte dos produtos da decomposição do SF_6 pode reagir com a água, eventualmente presente, e formar substâncias que são corrosivas para a porcelana e o vidro. No entanto, grande parte dos produtos da decomposição do SF_6 se recombina em tempo muito curto (10^{-6} a 10^{-7} segundos) após a extinção do arco. Devido à ausência de ar no SF_6, a oxidação e a abrasão dos contatos praticamente não se verifica e, por isso, o seu desgaste é muito pequeno.

As fases do arco elétrico podem ser divididas em: propagação e sustentação; extinção; e pós-arco. A fase de propagação e sustentação ocorre antes da corrente zerar. Nesta etapa, o arco se forma em uma coluna de plasma formada pelos íons e elétrons do dielétrico e do metal vaporizado dos contatos (Figura 13.7a). O arco se mantém pelo plasma, enquanto este estiver aquecido devido ao efeito Joule. A tensão entre os terminais, durante o processo de separação, é devida à resistência de arco. Tal tensão depende da natureza do arco (CA / CC) e é influenciada pela intensidade da corrente, pela capacidade do meio de extinção em trocar calor e pelo material do dielétrico e dos contatos (Figura 13.7b).



(a) (b)

Figura 13.7: Propagação e sustentação do arco elétrico ((a)THEOLEYRE, 1999 (b) COLOMBO, 1986).

A fase de extinção depende da rapidez do processo de desionização do meio extintor, o que ocorre quando o valor da corrente está próximo de zero. Neste momento, a resistência de arco (R) aumenta e, caso a desionização se processe rapidamente, de forma a recompor o dielétrico, a tensão entre os contatos (U) não será suficiente para rompê-lo. Neste caso, o processo de extinção tem sucesso e a corrente (I) é zerada. Caso contrário, o processo de extinção falha, com a corrente aumentando e a resistência de arco diminuindo (Figura 13.8).

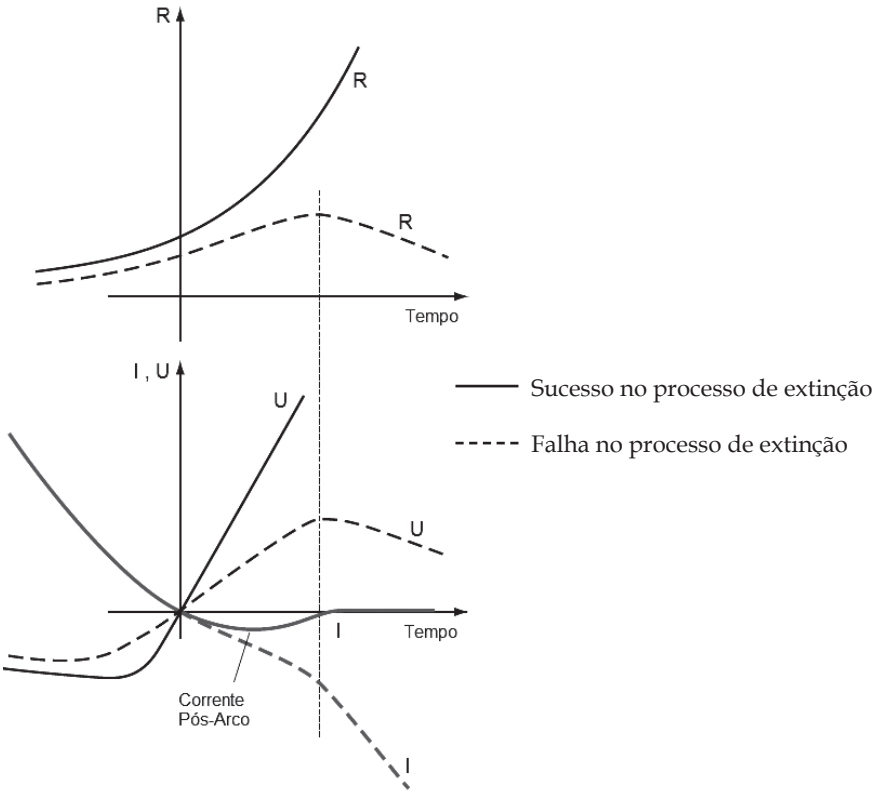


Figura 13.8: Extinção do arco elétrico (THEOLEYRE, 1999).

Para o sucesso da extinção do arco elétrico, na fase de pós-arco o dielétrico, deve se recompor em uma taxa superior ao crescimento da TTR (Figura 13.9). Caso contrário, pode ocorrer a reignição do arco (se o tempo de retorno do arco ocorrer em menos de ¼ de período) ou o reacendimento do arco (se o tempo de retorno do arco for maior que ¼ de período).

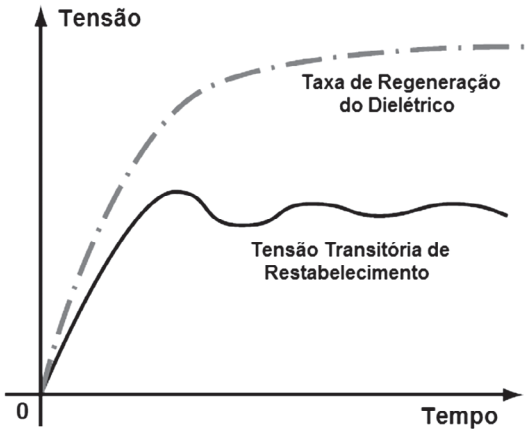


Figura 13.9: Fase de pós-arco (THEOLEYRE, 1999)

13.5.2 ESTRATÉGIAS PARA EXTINÇÃO DO ARCO ELÉTRICO

Nos últimos anos, os mecanismos e estratégias para extinção do arco elétrico em SF_6 evoluíram de técnicas mecânicas para forçar o fluxo do gás sobre o arco (dupla pressão e pistões) para técnicas que se utilizam da própria corrente a ser extinta para auxiliar a extinção (arco rotativo e expansão térmica). Na maioria das vezes, os disjuntores isolados a SF_6 se utilizam de técnicas combinadas de extinção do arco cujos objetivos são resfriar o arco, isolar os contatos do disjuntor e interromper o mais rápido possível a passagem da corrente no circuito, reduzindo ao máximo os danos aos contatos e a geração de subprodutos que possam contaminar o SF_6. A Figura 13.10 ilustra as principais técnicas de extinção do arco elétrico, resumidas a seguir:

- Dupla pressão: durante a abertura do disjuntor, o SF_6 previamente comprimido no tanque de "alta pressão" é liberado por uma válvula sobre o arco (câmara de extinção), contribuindo para sua extinção e refrigeração dos contatos. Finalizado o processo de abertura, o SF_6 é bombeado para o tanque de alta pressão.
- *Puffer*, sopro, impulso ou autocompressão: o SF_6 comprimido pelo movimento do contato móvel do disjuntor é "soprado" transversalmente sobre o arco auxiliando sua refrigeração e extinção.

- Expansão térmica: a energia térmica do arco é utilizada para aumentar a velocidade do processo de abertura e o fluxo de SF_6 sobre o arco.
- *Puffer* + expansão térmica: combinação dos 2 processos anteriores.
- Arco rotativo: o arco é resfriado e extinto a partir da sua rotação sobre os contatos do disjuntor originado pelo campo magnético radial produzido pela própria corrente a ser extinta. Esta técnica reduz o desgaste dos contatos e acelera o resfriamento do arco.
- Auto-expansão: é uma combinação de expansão térmica e arco rotativo.

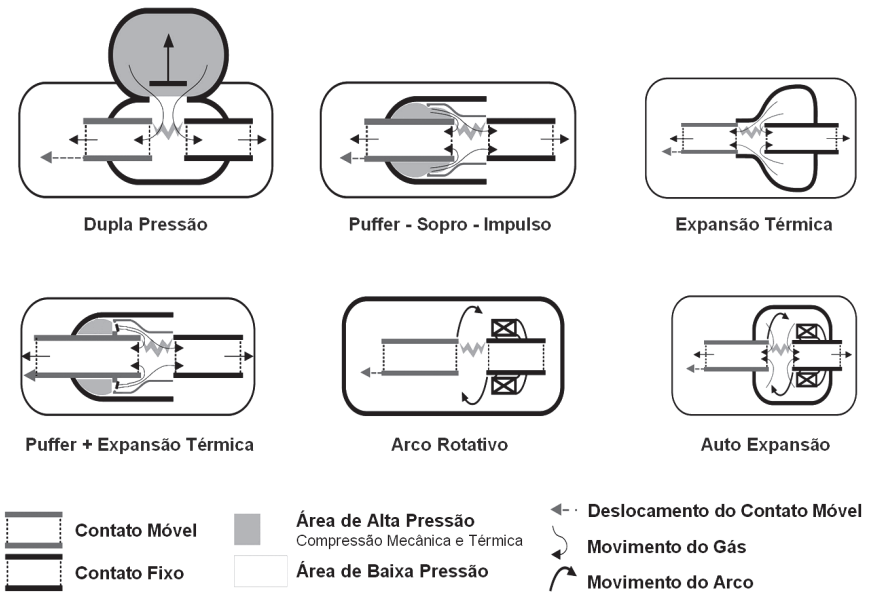


Figura 13.10: Estratégias para extinção do arco elétrico (BERNARD, 1995)

13.6 COMENTÁRIOS FINAIS

Apesar do tamanho reduzido dos disjuntores isolados a SF_6, principalmente devido à excelente qualidade de extinção e de isolamento deste gás, associado a técnicas eficientes de interrupção do arco elétrico, existe uma tendência, atualmente, da utilização

de subestações blindadas (*Gas Insulated Substation* - GIS), ao invés de subestações isoladas a ar. Tal tendência ocorre em função da necessidade de instalar subestações nos centros urbanos. Devido à densidade demográfica e o custo do terreno para construção de grandes subestações torna-se mais conveniente as GIS, em face do pequeno espaço a ser ocupado comparativamente ao requerido pela subestação isolada a ar. A tendência pela GIS justifica-se também em face da mesma ser construída em prédio fechado, o que melhora a inserção com o meio urbano.

Outra tendência promissora é a utilização de disjuntores de estado sólido ou disjuntores a semicondutor, uma vez que esses se aproximam muito do disjuntor ideal. Entretanto, o que se tem no momento, nesse sentido, são estudos laboratoriais e algumas aplicações de campo. Devido ao custo e a estabilidade requerida para o setor elétrico, ainda demandará um bom tempo até que novas tecnologias venham substituir o uso dos disjuntores isolados a SF_6.

Quer seja por necessidades operacionais ou penalização por desligamentos intempestivos, é dada uma importância cada vez maior à disponibilidade dos equipamentos das subestações de transmissão e distribuição de energia elétrica. No caso específico dos disjuntores, outra tendência são as técnicas de monitoramento do estado e de controle eletrônico, que permitem aumentar a disponibilidade do disjuntor e otimizar as intervenções de manutenção permitindo, além disso, o registro mais eficiente das informações operacionais e de mantenabilidade.

Capítulo 14

APLICAÇÃO DA METODOLOGIA DE ANÁLISE DE RISCO

A metodologia de análise de risco é uma parte muito importante da metodologia de gestão de risco. Enquanto a gestão ou gerenciamento de risco ocorre durante todo o ciclo de vida, a análise acontece em momentos específicos. É normalmente demandada quando ocorre uma mudança das metas estratégicas das organizações, diante da definição de novos padrões de segurança, quando da mudança de tecnologia, quando incidentes acontecem etc.

Este capítulo aborda o tema central do livro, a análise de risco. Para levar o leitor a inteirar-se deste tema, tomou-se por base fazer algumas perguntas que pretendem chamar atenção para a maneira dos autores pensarem em relação ao desenvolvimento de uma metodologia para análise de risco. As perguntas têm o objetivo de estabelecer um diálogo com o leitor referente aos temas abordados.

- Qual é o objetivo da análise de risco?
  O objetivo da análise de risco é dominar o conhecimento sobre "todas" as causas que contribuem para a ocorrência de um incidente (ou risco da ocorrência de um incidente) e "todos" os efeitos resultantes do incidente. É importante destacar que dominar o conhecimento sobre o sistema técnico e suas interrelações é fundamental para a gestão do risco ao longo do ciclo de vida. Diz-se que "um problema bem definido é um problema resolvido". E um problema só é bem definido se for bem conhecido, bem analisado. Por isso que o domínio do conhecimento sobre o sistema técnico é o objetivo da análise de risco.
- Como se faz a análise de risco?
  A análise de risco se faz por meio de uma metodologia de análise de risco, que é um conjunto de procedimentos e ações

empreendidas por meio de técnicas que são aplicadas de forma sistematizada para cumprir um objetivo bem definido. Observa-se que grande parte das técnicas para fazer análise de risco foi apresentada ao longo do livro.

- Qual o resultado esperado de uma análise de risco?
  Ao final da análise se tem definida as barreiras preventivas para eliminar ou diminuir as causas que contribuem para o incidente, e as barreiras para mitigar os efeitos, caso o incidente ocorra. As barreiras serão tão mais efetivas quanto maior for o domínio do conhecimento relativamente ao sistema técnico, principalmente no que se refere à função de todos os "itens" que constituem o sistema, ao ambiente que está inserido, a importância para a continuidade, a quantidade de energia que está presente, ao tipo de material, entre outros. Observa-se que item é um termo genérico, que varia de acordo com o escopo da análise, por exemplo: sistema, subsistema, componente, parte do componente, parte da matéria etc. A análise de risco é feita para o delineamento da gestão de risco ao longo do ciclo de vida do sistema em estudo.

14.1 ESTRUTURAÇÃO DA METODOLOGIA DE ANÁLISE DE RISCO

Metodologia de análise de risco é um conjunto de procedimentos e de ações empreendida por meio das técnicas de análise, para estudar um determinando sistema técnico. Neste capítulo serão apresentados os passos e as ações efetuadas num processo de análise de risco. Apresenta-se também exemplos de aplicação para mitigar a emissão para atmosfera do gás SF_6 presente em disjuntores isolados a SF_6.

A organização do capítulo está sintetizada na Figura 14.1. Como já salientado, o processo de análise é uma parte da metodologia de gestão. Desenvolve-se na etapa de delineamento que gera as informações para o tratamento e aceitação do risco. Para tanto, alguns conceitos são emitidos a partir de um conjunto de passos desenvolvidos no processo de análise de risco, como será exposto neste capítulo, tendo por referência a Figura 14.1, que foi desenvolvida a partir das figuras 4.1 e 4.2 da metodologia para gestão de risco.

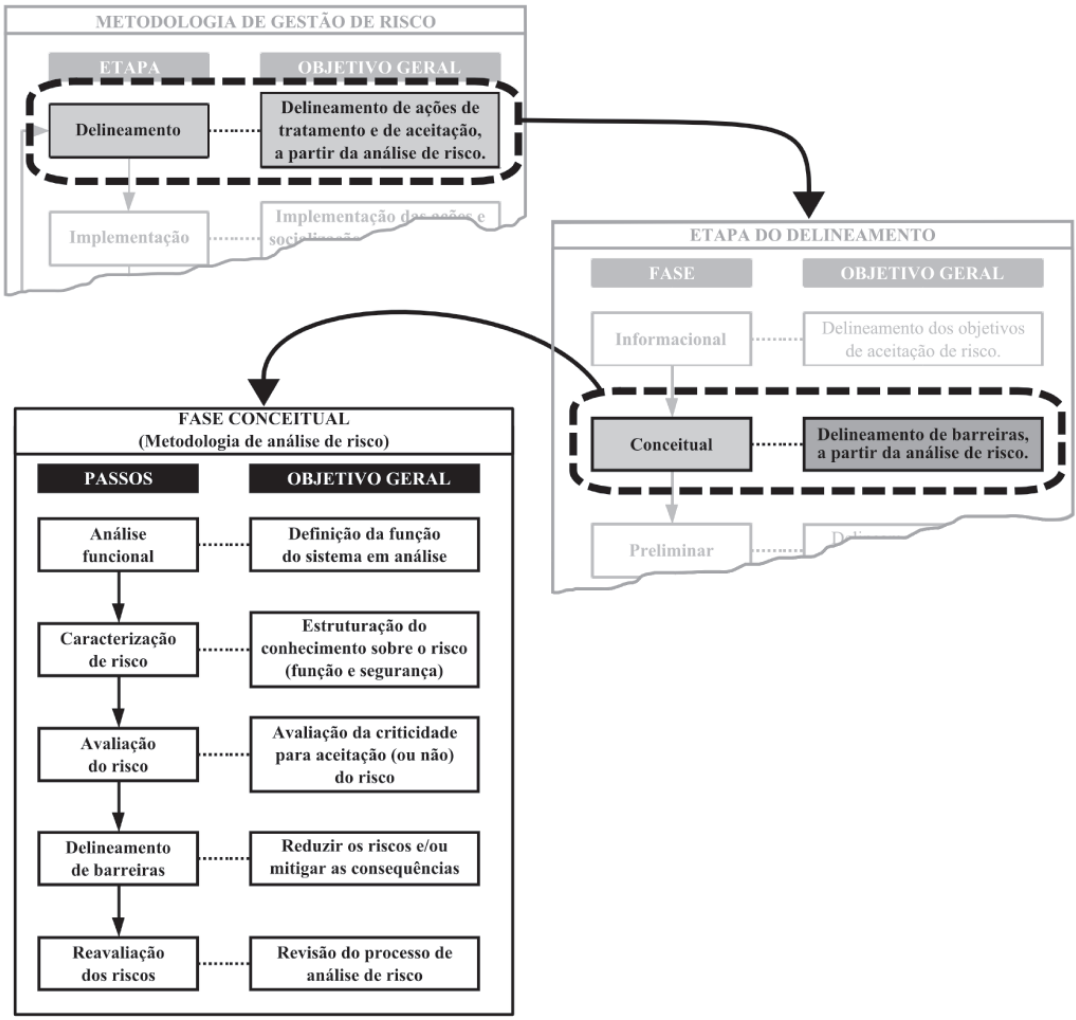


Figura 14.1 Sistematização da metodologia de análise de risco no contexto da Gestão de Risco

Na fase conceitual da Figura 14.1 estão definidos os passos e os objetivos a serem alcançados em cada passo. Evidentemente, para cada um dos passos técnicas devem ser utilizadas para ajudar o processo de análise por parte da equipe que está estudando os riscos dos sistemas técnicos.

A Figura 14.2 apresenta algumas das técnicas de análise a serem apresentadas. O ideal é que haja uma capacitação mínima

sobre cada uma das técnicas para que todos os participantes da análise tenham domínio do que fazer e o que sintetizar. Por mais simples que seja o sistema técnico, alguma complexidade sempre estará presente. Por isso é importante que os membros da equipe tenham bom conhecimento sobre o sistema técnico em análise e sobre a técnica que está sendo utilizada.

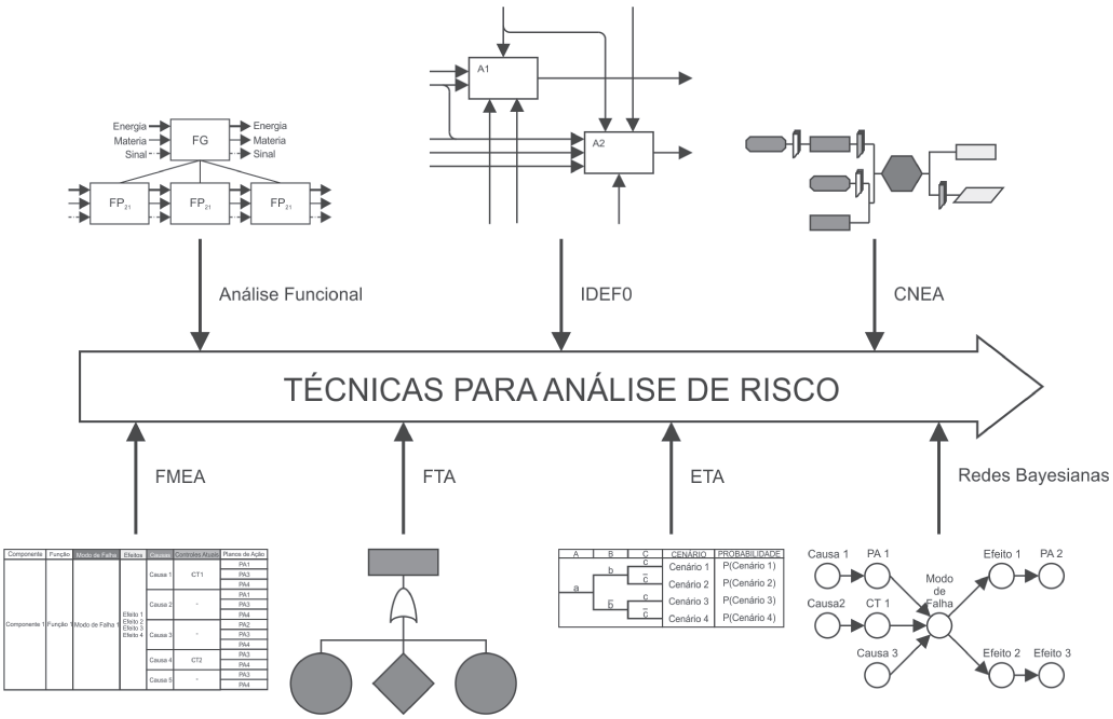


Figura 14.2 Exemplos de técnicas utilizadas para análise de risco em sistemas técnicos

A análise de risco é feita em instantes específicos, mas é importante que exista uma continuidade na assimilação do conhecimento e nos processos de análise. Ou seja, cada análise deve ser sintetizada na forma de relatório, e as ações devem ser registradas para que na nova análise que doravante ocorrerá se aproveite o conhecimento adquirido nos processos anteriores. É essa ação continuada de conhecimento que dará estabilidade à segurança e à continuidade dos sistemas técnicos simples ou complexos, como do setor elétrico, químico, petrolífero, aeronáutico, espacial etc.

14.2 PASSOS PARA ANÁLISE DE RISCO

Os passos para a fase conceitual da etapa de delineamento da Figura 14.1 são cinco. Ao descrevê-los, apresenta-se exemplos para ilustrar as técnicas de análise e a aplicação no MitiSF_6. Como já comentado, o processo de análise de risco torna-se mais efetivo quanto mais e melhor definido for o problema. Assim, dado a complexidade da empresa e a diversidade de equipamentos existentes foi necessário estabelecer alguns condicionantes para a abordagem da análise. A decisão primeira e geral é focar a análise somente em disjuntores isolados a SF_6. Isso porque há na empresa outros equipamentos que utilizam este gás como dielétrico.

São diversos os modelos de disjuntores que utilizam o gás SF_6 como dielétrico. A diversidade de modelos vem da obrigatoriedade da empresa em firmar contratos de compra via licitação, da aplicação nas diferentes linhas de transmissão, na atualização de modelos definidos por empresa fabricante, na alteração de modelos em face dos processos de fusões das empresas, na longevidade dos disjuntores e consequentes atualizações tecnológicas e na especificidade de função que o disjuntor deve operar na linha de transmissão.

Os seguintes critérios foram utilizados para a seleção do modelo de disjuntor para estudo piloto:

- Modelo e/ou fabricante com a maior massa de SF_6 e cujo disjuntor está em operação.
- Modelo e/ou fabricante no nível de tensão de maior concentração de disjuntores.
- Modelo e/ou fabricante mais antigo no sistema da ELETROSUL.
- Modelo e/ou fabricante com menor Índice de Eficiência de Extinção com relação à tensão de isolação e massa de SF_6 necessária (IEEMassa)[1].
- Modelo e/ou fabricante com menor Índice de Eficiência de Extinção calculado a partir da potência manobrada pelo disjuntor e densidade de SF_6 (IEEDensidade).
- Modelo e/ou fabricante com estudo consolidado na literatura nacional e/ou internacional.

[1] IEEMassa e IEEDensidade são índices elaborados ao longo do projeto MitiSF_6 com a intenção de avaliar a tecnologia dos disjuntores. Equipamentos com maior índice precisam de menor massa de SF_6 para operar uma mesma potência nominal de manobra.

- Modelo e/ou fabricante utilizado em outras concessionárias.
- Modelo e/ou fabricante com maior potência manobrada pelo disjuntor.
- Modelo e/ou fabricante com posição operacional estratégica dentro do sistema ELETROSUL.
- Modelo e/ou fabricante com maior dificuldade de manutenção em função de sua localização em campo.
- Modelo e/ou fabricante que tenha manutenção programada dentro do tempo do projeto.

A partir dos critérios definidos, optou-se por estudar, primeiramente, os disjuntores da família Merlin Gerin, e – como caso piloto – optou-se pelo disjuntor Merlin Gerin FA4.

Observa-se que nem o projeto MitiSF_6 e nem a metodologia de análise de risco que está sendo apresentada têm como objetivo fazer alterações de projeto nos equipamentos (disjuntor). O foco está em estudar os possíveis cenários associados à perda de SF_6 para a atmosfera a partir do disjuntor ou durante o processo de manipulação do gás.

A seguir apresenta-se os passos recomendados para a análise de risco que podem ser delineados tanto do ponto de vista qualitativo quanto do quantitativo.

14.2.1 ANÁLISE FUNCIONAL

A análise funcional é utilizada para a caracterização das funções do sistema em análise, tanto do ponto de vista do processo quanto das funções dos itens que compõem o sistema técnico. Observa-se, porém, que há perigos que não estão associados a nenhuma função do sistema, mas é possível que alguns deles sejam identificados ao longo do processo de análise funcional. Isto porque, durante a análise, aumenta-se o conhecimento sobre o sistema, o que facilita a identificação de outros fatores (inclusive que não estão relacionados com a análise de risco, como o desempenho de sistema, por exemplo). Esses perigos externos, não associados às funções devem, tanto quanto possível, serem eliminados, pois não trazem benefício para o desempenho do sistema.

Duas técnicas foram utilizadas para a análise funcional: a IDEFØ para a definição da função global do processo de manipulação do gás, e a análise funcional de produtos para desdobrar as funções

do disjuntor, para identificar aquelas que poderia implicar na perda do gás para atmosfera.

14.2.1.1 APLICAÇÃO DA ANÁLISE FUNCIONAL DE PROCESSO

A técnica IDEFØ foi utilizada para a análise funcional de processo para se obter melhor comunicação e visualização dos sistemas. Veja que o objetivo desse passo é definir a função do sistema em análise, como exposto na Figura 14.1.

A aplicação da técnica aconteceu dentro do Departamento de Manutenção do Sistema da ELETROSUL (DMS), cuja função global é fazer manutenção dos equipamentos e linhas da empresa (Figura 14.3). A função global do DMS é muito mais ampla do que aqui foi destacado. Por conta da objetividade da análise, apenas as funções que tinham relação com a manipulação do SF_6 foram desdobradas e estudadas.

A partir da função global foram identificados os recursos (mecanismos e controles) críticos para que o sistema cumpra seus objetivos e as saídas possíveis dos processos relacionados que são: ter um equipamento sempre "tão bom quanto novo" e resíduos controlados de SF_6, N_2, entre outros.

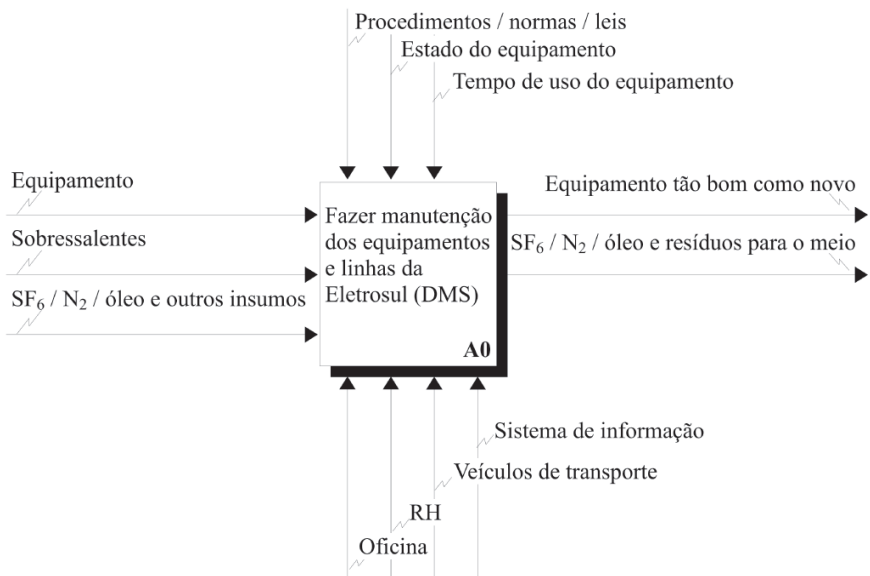


Figura 14.3: Diagrama raiz da IDEFØ dos processos relacionados à manipulação do SF_6 e definição da função global

Em relação ao controle "procedimentos / normas / leis", foi feito um estudo de organizações de referência em normatização, no manuseio e no tratamento de SF_6 – além das normas e regulamentações que se referem ao gás. Também foram feitas visitas técnicas e reuniões para captar a percepção da empresa quanto ao que ela considera tolerável nos riscos referentes à perda de SF_6 no DMS. Destaca-se, ainda, que o número ONU (Organização das Nações Unidas) do SF_6 é o 1080, que traz a indicação dos seguintes riscos: explosão do reservatório em caso de aquecimento; queimaduras pelo frio no contato com o líquido ao vaporizar-se; e asfixia por falta de oxigênio em caso de fuga importante (IGEO, 2000). Tratou-se de estudar em detalhe os relatórios do EMS em relação ao estado e tempo de uso dos equipamentos, não somente os disjuntores, mas todas as máquinas que eram utilizadas para operar com o SF_6: recarga dos disjuntores, retirada do gás dos disjuntores quando a manutenção era requerida, recolocação dos disjuntores em campo, processo de recuperação do gás, processos de controle do gás, descarte dos resíduos, estado das garrafas, padronização das máquinas, bicos e mangueiras para manipular o gás etc.

Uma vez definida a função global no diagrama IDEFØ, fez-se o desdobramento das funções pertinentes ao projeto até a resolução desejada. Por exemplo, a função "A0: Fazer manutenção dos equipamentos e linhas da ELETROSUL (DMS)" foi subdividida em cinco outras funções: "A1: Gerenciar insumos" (Quadro 14.1); "A2: Fazer manutenção de equipamentos isolados a SF_6"; "A3: Fazer manutenção de equipamentos isolados a óleo"; "A4: Fazer manutenção de equipamentos isolados a ar"; e "A5: Fazer manutenção de equipamentos isolados a vácuo". As funções A1 e A2 por estarem relacionadas com o gás foram novamente desdobradas (Quadros 14.2 e 14.3).

No Quadro 14.1 ilustra-se a descrição da função do nódulo A1 "Gerenciar insumos". Apresenta-se apenas a descrição do que é gerenciar insumos. Este quadro tem o objetivo de detalhar o modelo de análise e manter registradas todas as decisões da equipe de análise.

Quadro 14.1: Descrição da função "A1: gerenciar insumos"

A1: Gerenciar insumos O processo para gerenciar insumos é o que garante o fornecimento de recursos necessários para manter o bom funcionamento dos equipamentos, e depende da boa interação entres diversos setores da empresa, como manutenção e compras. No presente projeto, apenas o gerenciamento de SF_6 será tratado.

Para aprofundar a análise faz-se novo detalhamento do nódulo "A1: Gerenciar insumos" como mostrado na Figura 14.4. A função foi desdobrada em 5 novas funções, sendo A11 relacionada com gerenciar consumo de SF_6. As outras funções tratam do gerenciamento de cada um dos outros insumos operados na empresa, e por isso não são detalhadas no texto.

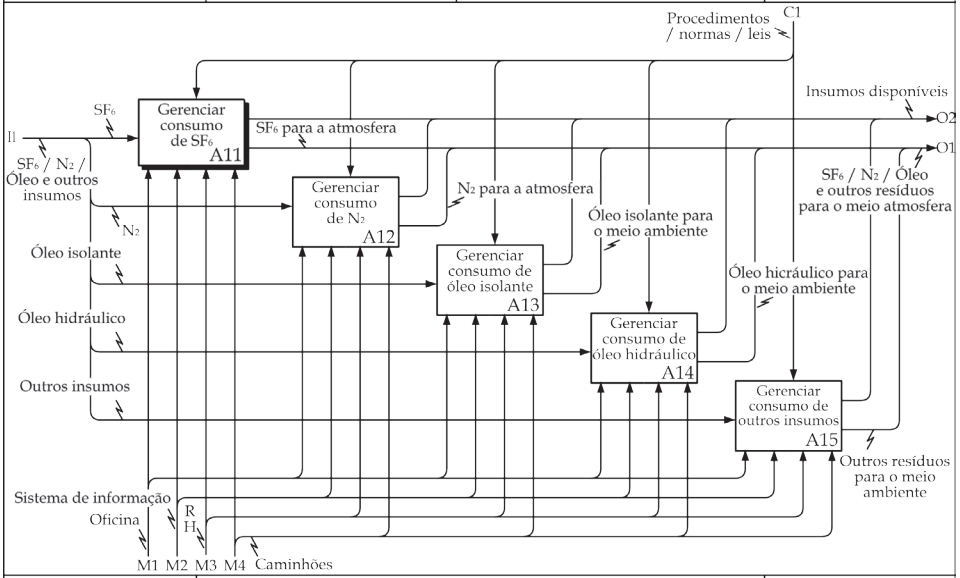
No Quadro 14.2 evidencia-se a análise efetuada para o nódulo A11. Apresenta-se a análise do nó sobre a função, os mecanismos, controles e saídas do nó.

O uso da técnica IDEFØ exige um nível de detalhamento muito intenso. A representação na forma de nódulos com todas as definições chegando e saindo da caixa de controle leva a razoável intensificação de informações em cada uma das análises. Devido a isso, foi estruturado um processo de representação da técnica na forma de planilha, como está no Quadro 14.3[2].

Apresenta-se, então, no Quadro 14.3, o desdobramento das funções A11 e A21 até o terceiro nível de detalhamento. Neste nível, o quadro apresenta o detalhamento em nível dos modos de falha (MF) e dos efeitos (EF). O mesmo foi feito para o nódulo A211: Comissionar disjuntor. Essa função de comissionar ocorre no caso de instalação de disjuntor novo ou disjuntor reformado. Foram identificados para esta função dois modos de falha: disjuntor aceito com SF_6 inadequado e perda de gás durante o enchimento. Por efeitos identificou-se: perda de SF_6 para a atmosfera, inalação de subprodutos tóxicos e comprometimento à saúde dos colaboradores.

[2] No projeto mitiSF6 foi desenvolvido uma versão inicial do software, chamado de Pharos, para auxiliar o desenvolvimento de FMEA.

Projeto: MitiSF6	Documento: MT-DE-NE-04	Elaborado: Heito Azuma Kagueiama Aprovado: Acires Dias	Revisão: 0 Data: 12/07/2007



Nódulo: A1	Título: Gerenciar insumos	Página: 07

Figura 14.4 Diagrama IDEFØ do nó A1 da função gerenciar insumos.

Quadro 14.2: Detalhamento da função "A1:gerenciar insumos"

Projeto: MitiSF6	Documento: MT-DE-NE-04	Elaborado: Heito Azuma Kagueiama Aprovado: Acires Dias	Revisão: 0 Data: 12/07/2007

[A11] Gerenciar consumo de SF_6

O processo de gerenciar o consumo de SF_6 é fundamental para a organização da manutenção, pois é um insumo excencial para que os equipamentos isolados a gás cumpram suas funções. Pode-se caracterizar o processo da seguinte forma:

Entradas

SF_6 : insumo necessário para o funcionamento dos equipamentos.

Mecanismos

Sistema de informação: controla as informações como tempo de operação do equipamento, ordens de serviço, estoques de insumos etc.

RH: são os recursos humanos envolvidos no processo

Caminhões: veículos empregados no transporte de equipamentos, equipes de manutenção e insumos.

Oficina: a Eletrosul dispõem de 5 oficinas que atendem as respectivas regionais, são elas: Sertão do Maruim, Curitiba, Xanxerê, Campo Grande e Gravataí

Controles

Procedimentos / normas / leis: padrões estabelecidos pela empresa e entidades reguladoras para o tipo de serviço exercido pela empresa.

Saídas

SF_6 para atmosfera: perdas ocorridas durante o processo.

SF_6 disponível: quantidade real de SF_6 disponível (gás novo, tratado e usado).

[A12] Gerenciar consumo de óleo N_2

Por estar fora do escopo do projeto, o gerenciamento do consumo de N_2 não será tratado.

[A13] Gerenciar consumo de óleo isolante

Por estar fora do escopo do projeto, o gerenciamento do consumo de óleo isolante não será tratado.

[A14] Gerenciar consumo de óleo hidráulico

Por estar fora do escopo do projeto, o gerenciamento do consumo de óleo hidráulico não será tratado.

[A15] Gerenciar consumo de outros insumos

Por estar fora do escopo do projeto, o gerenciamento do consumo de outros insumos não será tratado.

Nódulo: A1	Título: Gerenciar insumos	Página: 08

Quadro 14.3 Detalhamento da A11: Gerenciar insumo e A21: Fazer manutenção de disjuntores isolados a SF_6

OpenFMECA — Bugtracker | Ajuda | Contato | 2007 NeDIP | Luís Fernando Peres Calil | Fechar

- [-] [ST] DMS
  - [-] [SS] A1: Gerenciar insumos
    - [-] [SS] A11: Gerenciar consumo de SF_6
      - [+] [SS] A111: Dimensionar e verificar estoque de SF_6
      - [+] [SS] A112: Avaliar necessidade de compra
      - [+] [SS] A113: Comprar SF_6
      - [+] [SS] A114: Recebimento de SF_6
      - [+] [SS] A115: Tratar, avaliar, consolidar e estocar SF6 tratado
  - [-] [SS] A2: Fazer manutenção de equipamentos isolados a SF_6
    - [-] [SS] A21: Fazer manuten,ão de.ntores isolados a SF_6
      - [+] **[SS] A211: Comissionar disjuntor**
        - [+] [MF] Disjuntor aceito com SF_6 inadequado
        - [-] [MF] Perda de gás durante o enchimento
          - [-] Efeitos:
            - [-] [EF] Perda de SF_6 para a atmosfera
            - [-] [EF] Inalação de subprodutos tóxicos
            - [-] [EF] Comprometimento à saúde de colaboradores
          - [-] Causas:
            - [+] [CA] Purga na linha de SF_6
            - [+] [CA] Linha de gás em mau estado de conservação
            - [+] [CA] Impacto na válvula
            - [+] [CA] Falta de procedimentos padronizados
            - [+] [CA] Corpo técnico sem capacitação para executar a operação
        - [+] [MF] Disjuntor aceito com problemas de estanqueidade

Home

Opções
Novo modo de falha
Editar
Deletar

Relatórios
Relatório STD
Relatório descrição

Cadastro
Efeitos
Controles atuais
Plano de ações

A211: Comissionar disjuntor
O processo de comissionamento consiste em uma série de testes para avaliar a condição do equipamento na primeira instalação do disjuntor. Normalmente o comissionamento é feito pelo fabricante do disjuntor com supervisão da ELETROSUL, no entanto, pode-se contratar uma terceira empresa para fazê-lo. O fornecedor do disjuntor faz a carga inicial de SF_6 e eventualmente existe um excedente de gás. Estes cilindros, quando cheios, são adicionados ao estoque (tem entrada no sistema de informação) e, quando já utilizado parte do SF_6, permanecem na subestação em que foi

Siglas:
[ST] Sistema
[SS] Subsistema
[MF] Modo de falha
[EF] Efeito
[CA] Causa
[CT] Controle atual
[PA] Plano de ação

A técnica IDEFØ permitiu analisar as funções de todo o processo de manipulação do gás SF_6 no contexto da manutenção. Para o último nível da análise foram identificados modos de falha e efeitos. Os modos de falha são os núcleos da análise. Portanto, todas as ações devem estar voltadas para a efetividade de barreiras que mitiguem ou eliminem as causas que geram os modos de falha. Os efeitos são a forma como os modos de falha se manifestam em nível do ambiente e da segurança humana. Podem também serem chamados de consequências. E também para os efeitos barreiras devem ser desenvolvidas para mitigar os efeitos para o ambiente e para a segurança.

14.2.1.2 APLICAÇÃO DA ANÁLISE FUNCIONAL DE PRODUTO

A análise funcional de produtos é uma técnica apropriada para estudar, compreender e definir as funções de sistemas técnicos (*hardware*). Recomenda-se desdobrar as funções dos sistemas em

subsistemas e componentes ou partes do mesmo, até a resolução que permite identificar os perigos contidos em cada um das funções, como mostrado na Figura 6.1. Assim, a técnica é mais indicada quando se tem desdobramento estrutural (não funcional).

Para melhor exemplificar a aplicação da técnica toma-se, por exemplo, o disjuntor.

- Qual é a função do disjuntor para o sistema elétrico? É estabelecer, conduzir e interromper correntes nas condições normais do circuito, assim como estabelecer, conduzir durante um tempo especificado e interromper correntes sob condições anormais especificadas do circuito, tais como as de curto-circuito (IEC, 2009).
- Que tipo de disjuntor vai ser analisado? Disjuntores isolados a SF_6.
- Que tipo de risco deseja-se analisar por meio da técnica de análise funcional? É o risco de emissão de SF_6 para a atmosfera.
- Qual é a função do disjuntor isolado a SF_6? Conter SF_6.

Assim, o trabalho de análise tem foco na função do disjuntor de "conter SF_6". Neste caso, as restrições são as normas e regulamentos para conter a perda de gás nos equipamentos. Os recursos críticos, por sua vez, estão relacionados à integridade dos invólucros e das vedações.

Para desenvolver a análise funcional toma-se por referência o disjuntor Merlin Gerin FA4, ilustrado na Figura 14.5. Os disjuntores são montados em fases nas subestações, e cada fase é composta por dois módulos. Em cada módulo, a câmara de extinção, o cárter, o resistor de pré-inserção e a coluna de isoladores de porcelana são preenchidos com SF_6. No caso do disjuntor Merlin Gerin FA4, esses subsistemas estão interligados, ou seja, o gás circula em todo o módulo, exceto no cárter, que fica isolado. Há outros modelos de disjuntores onde, inclusive, o cárter está interligado. No capítulo 13 detalhou-se a constituição dos disjuntores.

Entre os subsistemas que contém SF_6 como dielétrico tem-se: câmara de extinção, cárter, coluna de isoladores. Cada um desses subsistemas tem função específica a ser desenvolvida e é constituído

por grande número de componentes. Esses componentes são demandados a cada operação do disjuntor e desempenham papel importante para a função do disjuntor e para a função "conter gás" no disjuntor. Por meio da técnica, identificam-se todas as vedações do equipamento, apresentando a localização no desenho, o detalhamento da função, o número de peças por disjuntor, as características construtivas, o material, as dimensões e o fluido que esta vedação isola.

Figura 14.5 Subestação com destaque para disjuntores Merlin Gerin FA4 (550kV)

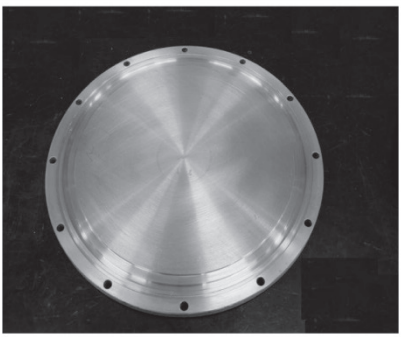
Por exemplo, ao aplicar-se a análise funcional para o cárter fez-se os seguinte procedimentos:

- Definiu-se o cárter: é a parte do disjuntor responsável pela transferência do movimento proveniente da haste de manobra para as câmaras de extinção e resistores de pré-inserção, com o auxílio de mecanismos contidos nele. Contém SF_6 como meio

dielétrico. Para esse modelo, o gás está hermeticamente isolado daquele que circula entre as câmaras de extinção, os resistores e a coluna de isoladores.

- Desdobrou-se o cárter em componentes: para isso, fez-se a seleção do modelo de disjuntor, estudou-se os desenhos do disjuntor e fotografou-se cada um dos componentes. A fotografia foi importante para o estudo da função, envolvendo especialistas que não têm o hábito de fazer leitura de desenho. Facilita a capacitação e análise da função de cada componente.
- Desenvolveu-se a análise dos componentes: definiu-se o nome de cada componente e as funções dos mesmos. Na Figura 14.6 apresenta-se um exemplo desse estudo, onde o componente foi denominado de item. O item 5 – placa de fechamento - tem três funções importantes para conter o gás SF_6, como ilustrado na Figura 14.6.

Figura 14.6 Análise funcional da placa de fechamento do cárter



ITEM 5 – Placas de fechamento

Função:

- Vedar o SF_6.
- Impedir a entrada de umidade.
- Alojar os anéis de vedação (*O-rings*)

A análise funcional, então, serviu de base para todas as outras técnicas de análise a serem utilizadas na fase de caracterização de risco e nas seguintes. Tem importância especial para a FMEA do disjuntor, dado que é fundamental ter bem definido a função para o bom desenvolvimento da técnica. Por exemplo: se a função do disjuntor é conter SF_6,, então, o modo de falha principal é não conter SF_6. Do ponto de vista funcional, uma vez que a função esteja bem definida, o modo de falha poderá ser obtido pela não execução da função. Para detalhar esse modo de falha, uma análise estrutural também deve ser feita, apontando problemas relacionados com o material, fabricação, tempo de uso, ação do meio ambiente entre outros.

14.2.2 CARACTERIZAÇÃO DE RISCO

Uma vez que o estado inicial do sistema em análise foi caracterizado pela análise funcional em nível de processo ou de produto, o passo seguinte é caracterizar o risco advindo dos perigos presentes no sistema, subsistema e componentes. Os perigos, em termos gerais, se relacionam com o modo de falha, ou seja, com o não cumprimento da função de um ou de mais itens presentes no sistema. Claro que há situações cujo perigo vem do meio externo e não tem relação direta com a função do item.

Usualmente, esse processo de caracterização compreende a combinação de técnicas de criatividade e analíticas, objetivando identificar as situações de perigo existentes, e de riscos que já ocorreram no sistema ou em sistemas similares e as de que não se tem conhecimento de ter ocorrido. Utiliza-se listas pré-elaboradas, base de dados de risco e técnicas de criatividade – como tempestade de idéias (*brainstorming*). Outra solução é levantar e classificar os perigos relacionados ao sistema em análise e identificar os incidentes que cada perigo pode desencadear. Para organizar as reuniões recomendam-se fazer atas, filmagens, gravações e sintetizar o *brainstorming* em diagramas como o de Ishikawa (espinha de peixe), planilhas, listas etc.

Caso seja necessário fazer a análise de um incidente já ocorrido, recomenda-se utilizar o histórico de operação do sistema, trazer a experiência de especialistas e desenvolver diagnóstico do incidente. Para tanto, recomenda-se o uso de modelos próprios para investigação científica de análise de acidentes, como os utilizados em acidentes aeronáuticos (MAURINO et al, 1995, REASON 1997).

Na identificação do incidente é necessário caracterizar a forma da ocorrência, a caracterização da ocorrência, o nível de criticidade, as ações recomendadas e os custos envolvidos. Nem sempre há somente uma técnica para evidenciar a caracterização do risco. Por isso, a seguir, apresenta-se exemplos do uso de técnicas consorciadas para ajudar no processo de caracterização.

A saída final do processo de caracterização do risco é evidenciar conhecimento sobre sua ocorrência para nos passos seguintes definir barreiras eficientes de garantia da segurança. Por isso é que se deve esmerar no estudo do risco envolvendo mais de uma técnica. Com as técnicas, desenvolvem-se diferentes ponto de vista, que devem

inspirar as equipes de análise para exercícios de criatividade em soluções para aumentar a segurança dos sistemas técnicos.

14.2.2.1 RELAÇÃO FMEA E CNEA

A técnica FMEA, como apresentada no Capítulo 7, estrutura o conhecimento desenvolvido para análise de um sistema relacionando nome do item, função, modos de falha, causas, efeitos, prioridades de análise e ações para mitigar ou eliminar falhas. A técnica traz complexidades em relação ao tempo demandado para análise, custo da análise, quantidade de informação, atualização da informação, repetição de abordagem, problemas de continuidade e dificuldade de visualizar as falhas principais.

A técnica CNEA, como apresentada no Capítulo 11, visa analisar incidentes no contexto da análise de risco. A técnica mostrou-se adequada para representar os eventos do FMEA na forma gráfica, com destaque para a implementação das ações e barreiras para as falhas. Para os eventos mais críticos, a representação na forma de figura facilita a comunicação com todo aquele que atua ou interage com o sistema técnico em análise. Contudo, perde-se em amplitude com a CNEA se for utilizada como única técnica de análise de um sistema complexo.

A Figura 14.7 exemplifica a adaptação do diagrama da técnica CNEA para análise de modos de falha do FMEA. Para tanto, identificou-se o evento central, normalmente definido como incidente, por um modo de falha. Ao modo de falha associou-se um grau de severidade (“S”). Note-se que o grau de severidade “S” refere-se a todos os efeitos. Está representado no modo de falha, que representa o nódulo de origem desses efeitos. Nessa forma de análise, o modo de falha é modelado numa corrente causal e diagramado entre as causas que levam à ocorrência do incidente e seus efeitos.

Do lado esquerdo do modo de falha definem-se as causas. As mesmas são desdobradas em causas raízes, intermediárias, ou imediatas, definidas de acordo com a profundidade da análise feita no FMEA. Associou-se a cada causa o Número de Prioridade de Risco (NPR) com os respectivos índices de ocorrência “O” e de dificuldade de detecção “D”. A dificuldade de detecção, por exemplo, se refere a todos os controles existentes ao longo da corrente causal, desde as causas até os efeitos.

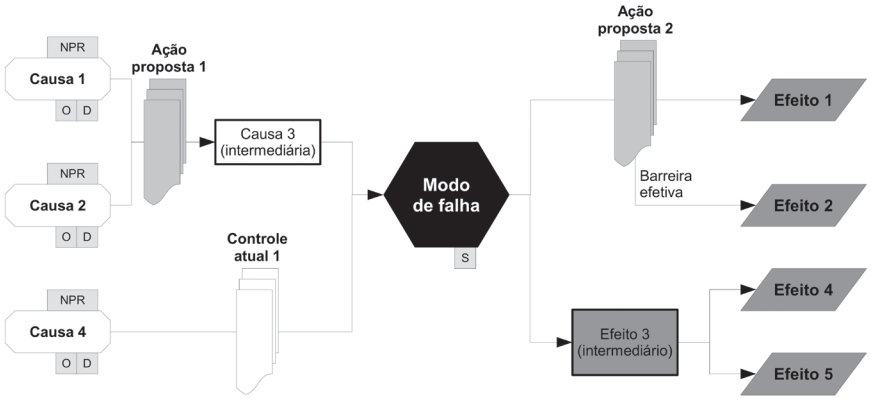


Figura 14.7 Diagrama CNEA adaptado para representar FMEA

Adicionalmente, para a adequação do diagrama CNEA, às informações presentes na planilha da FMEA, foram feitas algumas adaptações. Como está indicado na Figura 14.7 fez-se diferenciação entre as barreiras para as seguintes condições: barreiras brancas significam "controle atual", ou seja, já existem no sistema. Barreiras preenchidas com cor definem "ação proposta", ou seja, serão definidas a partir da análise efetuada. Além disso, inclui-se na análise de CNEA os índices que definem o Número de Prioridade de Risco (NPR) indicando a Severidade (S), a Ocorrência (O) e Detecção (D). Os mesmos são utilizados para ajudar a equipe de análise a definir prioridades para o detalhamento da análise, implementação das barreiras e aporte de recursos financeiros para melhoria do sistema técnico.

A representação gráfica permite uma melhor contextualização que a planilha e se mostra mais adequada, tanto por proporcionar uma análise mais eficaz quanto por gerenciar melhor o conhecimento gerado, facilitando a visualização das ações a partir do modo de falha.

Destacam-se os seguintes benefícios na utilização do diagrama da CNEA:

- melhora a comunicação entre o analista e outros colaboradores, auxiliando no envolvimento dos especialistas e na busca de consenso para tomadas de decisões;
- melhora a explicitação e disseminação do conhecimento, sendo indicado como ferramenta para capacitação;
- possibilita a representação de eventos imediatos e intermediários, e não apenas causas-raiz e efeitos-finais;

- permite identificar onde um controle atual está atuando na corrente causal e onde será implementado controles futuros;
- apresenta, de forma mais evidente a relação entre as causas e entre os efeitos; e
- melhora a formalização do conhecimento e, consequentemente, o reaproveitamento das informações da análise.

Destaca-se ainda que a modelagem do incidente no diagrama da CNEA facilita a tarefa da identificação dos eventos e estados envolvido, pois permite visualizar a corrente causal para cada modo de falha. Assim, o diagrama também facilita a elicitação do conhecimento do especialista, pois atua como uma ferramenta de comunicação.

A experiência obtida durante os processos de análise indicou que a CNEA se mostra aderente à FMEA, pois a permite modelar o cenário resultante do incidente utilizando estados, que são os efeitos da FMEA.

Contudo, a CNEA não é a única técnica que pode ser utilizada para representar na forma gráfica a análise de FMEA. A FTA (*fault tree analysis*) (Capítulo 8) modela tanto as causas quanto as consequências. Porém, a opção por modelar a corrente causal utilizando a CNEA torna o trabalho mais simples, pois a modelagem das causas em uma FTA requer um conhecimento maior do sistema, uma vez que é necessário identificar as portas lógicas que indicam a relação entre as causas, sendo que na CNEA isto não é necessário. Os efeitos e as consequências podem também serem representados por uma ETA (*event tree analysis*) (Capítulo 8). Nessa técnica, a modelagem é feita em relação aos eventos pivotais e somente avalia-se o estado final após cada combinação de eventos.

No entanto, a CNEA tem uma desvantagem em relação à estrutura FTA/ETA, que é o tratamento estatístico. O uso de estatísticas na estrutura FTA/ETA é bastante consolidado; no entanto, na CNEA, não existe um formalismo para isso. Para contornar este inconveniente, propõe-se que o tratamento estatístico para a CNEA seja feito utilizando-se a teoria de redes bayesianas.

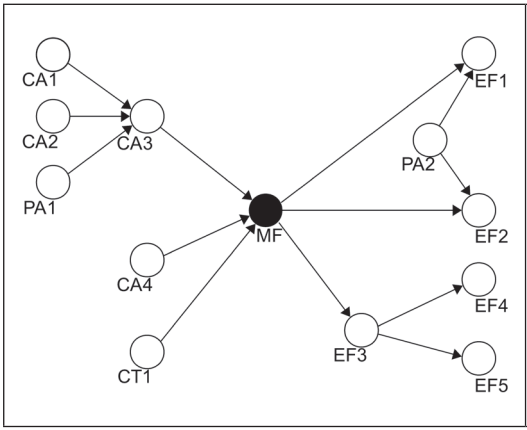
14.2.2.2 RELAÇÃO CNEA E REDES BAYESIANAS

Assim como a CNEA, as redes bayesianas (Capítulo 10) também são redes causais, o que torna a utilização conjunta das técnicas

bastante apropriada. A Figura 14.8 apresenta a rede bayesiana equivalente ao diagrama CNEA ilustrado na Figura 14.5, considerando todos os eventos independentes.

É interessante destacar que se pode verificar a aderência do modelo à realidade, por meio de análise de d-separadores, ou seja, a análise de variáveis independentes.

Tanto as barreiras que já são controles atuais quanto as barreiras a serem propostas nesta modelagem entram como nódulos de mesmo nível dos eventos que se pretendem salvaguardar, exemplificado no Quadro 14.4, que ilustra uma tabela de relações para o nódulo "CA3".



Legenda:
MF – Modo de falha.
CA1 – Causa 1.
CA2 – Causa 2.
CA3 – Causa 3 (intermediária).
CA4 – Causa 4.
CT1 – Controle atual 1.
PA1 – Ação proposta 1.
PA2 – Ação proposta 2.
EF1 – Efeito 1.
EF2 – Efeito 2.
EF3 – Efeito 3 (intermediário).
EF4 – Efeito 4.
EF5 – Efeito 5.

Figura 14.8 Rede bayesiana para o diagrama da Figura 14.7

Quadro 14.4 Tabela de relações do nódulo "CA3" da rede bayesiana da Figura 14.7

CA1	CA2	PA1	CA3 (causa intermediária)
Ocorrer	Ocorrer	Eficaz	Não ocorrer
Ocorrer	Ocorrer	Não eficaz	Ocorrer
Ocorrer	Não ocorrer	Eficaz	Não ocorrer
Ocorrer	Não ocorrer	Não eficaz	Ocorrer
Não ocorrer	Ocorrer	Eficaz	Não ocorrer
Não ocorrer	Ocorrer	Não eficaz	Ocorrer
Não ocorrer	Não ocorrer	Eficaz	Não ocorrer
Não ocorrer	Não ocorrer	Não eficaz	Não ocorrer

Também é possível modelar – em rede bayesiana – barreiras que têm um evento derivado (caso ela seja bem sucedida) por meio de uma ligação na forma de ponte, como ilustrado na Figura 14.9, contemplando, assim, os tipos de relações possíveis em uma CNEA. Assim, podem-se verificar as consequências da efetividade, ou não, de uma barreira para o comportamento do sistema. Estas regras definem como um modelo elaborado utilizando CNEA pode ser transposto para um modelo em redes bayesianas. Isto permite que o usuário possa delinear a rede bayesiana, sem ter que se preocupar em fazer análise de d-separadores. De fato, uma ferramenta computacional poderia fazer essa transposição automaticamente e a modelagem da rede bayesiana seria transparente para o usuário. Para facilitar esses relacionamentos a utilização de *software* torna-se recomendável.

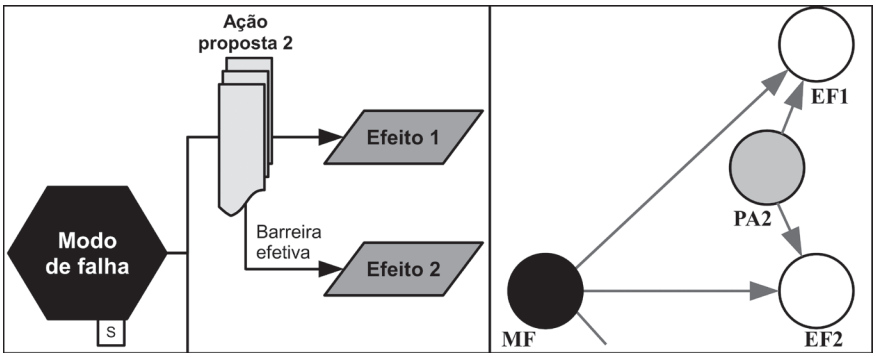


Figura 14.9 Detalhe da análise da Figura 14.7 do diagrama CNEA para modelagem em rede bayesiana

As redes bayesianas permitem também tratar incertezas nas relações. Mas a utilização combinada entre a CNEA e redes bayesianas são adequadas à análise determinística, exemplificado no Quadro 14.4. No exemplo, não ocorrendo o nódulo "CA1", ocorrendo o nódulo "CA2" e se o "PA1" não for eficaz, então, por certo ocorrerá a causa intermediária "CA3".

Além disso, as redes bayesianas permitem introduzir incerteza na relação, e, com isso, é possível modelar a probabilidade de ocorrência da causa intermediária "CA3", dada a combinação como: 80% de probabilidade de ocorrer e 20% de não ocorrer, por exemplo.

Da mesma forma que para a causa, a relação entre as técnicas é útil na modelagem dos efeitos. Isto porque a ocorrência do efeito EF3, por exemplo, não implica necessariamente na ocorrência do EF4. Nesse caso, a modelagem da cadeia causal desenvolve-se de maneira probabilística, desde que se tenham condições de atribuir ou considerar probabilidades de ocorrência dos eventos constituintes da cadeia causal.

Destaca-se, ainda, que a principal dificuldade de se implementar a rede bayesiana, como também qualquer outra técnica de análise quantitativa, está na disponibilidade de dados estatísticos. Uma forma de contornar essa limitação é lançar mão de base de dados, fazer simulações, levantar dados a partir do conhecimento dos especialistas. A partir dos especialistas pode-se definir algumas probabilidades que vão sendo corrigidas a partir de atualizações estatísticas definidas pela variável aleatória mais apropriada para a análise da corrente causal.

14.2.2.3 RELAÇÃO ENTRE CNEA E FTA

A representação da corrente causal por meio da técnica CNEA evidencia a posição das barreiras entre as causas e o modo de falha, e entre este e os efeitos. Assim, se existe um modo de falha então também existe falha nas barreiras, sem o que o modo de falha não aconteceria. Do lado esquerdo, a análise é um pouco diferente. Existindo um modo de falha também existirá efeito. As barreiras têm a função apenas de mitigar o efeito, ou, no caso de risco, as consequências.

Na Figura 14.10, o modo de falha é simplesmente chamado de incidente. Como houve falha na barreira de controle atual 1, utilizou-se a técnica FTA para identificar as causas das falhas nas barreiras, ou seja, os "furos" presentes nas barreiras. Observa-se que as causas que são apresentadas na Figura 14.10 se referem ao incidente. Essa mesma análise também poderia ser feita na CNEA, dando continuidade ao diagrama. Entretanto, o diagrama tende a se tornar confuso, sendo preferível fazer a CNEA a cada um dos incidentes (modo de falha) do item em análise e utilizar a técnica FTA para detalhar as causas que tiverem maior importância para análise dentro da corrente causal da CNEA.

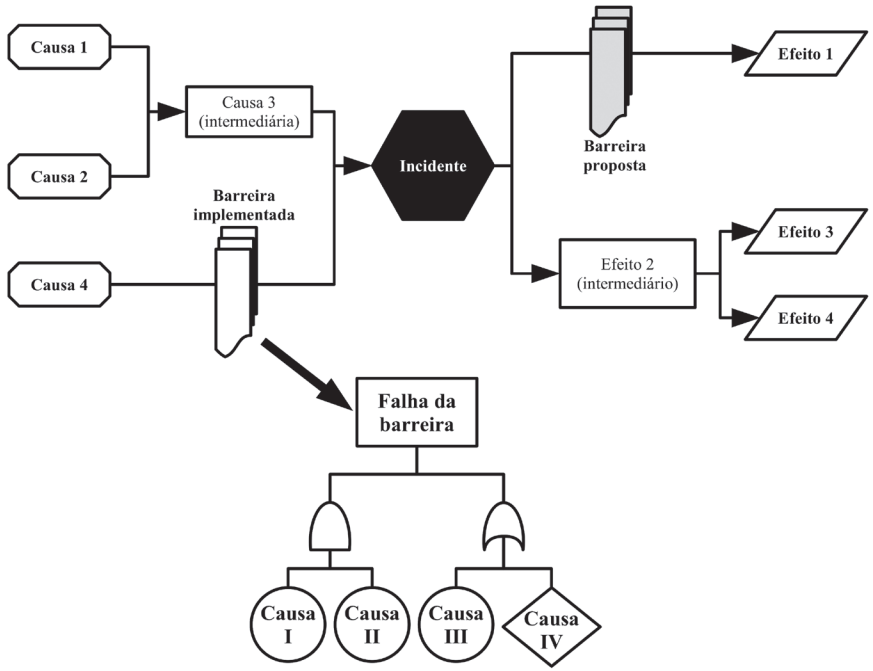


Figura 14.10 Ilustração de uma análise de falha de barreira por FTA

Como já observado no Capítulo 8, é possível fazer análise probabilística em uma FTA. Assim, utiliza-se a FTA para determinar a probabilidade de falha de uma barreira, de uma causa "furar" a barreira atual, ou se tiver dados, a barreira futura a ser instalada. Para tanto, há que se ter dados de probabilidade de ocorrência desse evento. A forma de obter as informações estatísticas ou de especialistas para estabelecer a probabilidade segue as mesmas recomendações anteriormente comentadas.

A modelagem da técnica FTA é feita a partir das regras, que já estão bem definidas para a técnica. Dado diversas aplicações e uso generalizado da FTA já existem software disponíveis para processos de automatização da construção dos diagramas da técnica FTA. Assim facilita a passagem da CNEA para a FTA, ou, de forma mais direta, quando for o caso, da técnica FMEA para a FTA.

A modelagem da FTA da Figura 14.10 foi definida para o evento topo que ocorreu. A partir dele, se identificou as causas que mais contribuíram para isso. Quando se está analisando barreiras a

serem implantadas numa corrente causal, pode-se ainda, a partir de algumas causas prováveis, indicar que evento de topo virá ocorrer. Essa flexibilidade de análise valoriza muito a técnica e é um bom exercício de racionalizar o conhecimento da equipe de análise de sistemas, subsistemas ou componentes ainda na fase de projeto conceitual e preliminar.

14.2.2.4 EXEMPLO DE APLICAÇÃO DA CARACTERIZAÇÃO DO RISCO

A seguir apresenta-se uma aplicação de caracterização de risco nos processos que envolvem o gás SF_6. Primeiramente, explicita-se os exemplos de aplicação envolvendo as técnicas para o processo de manipulação do gás. Depois utiliza-se a técnica FTA em um componente do disjuntor. Em ambos os casos caracterizam-se os modos de falha que contribuem para o risco de vazamento do gás.

Para tanto, foram levantados os modos de falha (MF) para cada função. Como foi apresentado no Quadro 14.4, destacaram-se os modos de falha para a função A211 de comissionar disjuntor, presente no último nível de desdobramento do IDEFØ. Os modos de falhas identificados são: disjuntor aceito com SF_6 inadequado e perda de gás durante o enchimento.

Claro que para levantar os modos de falha, foram utilizadas técnicas de criatividade (como *brainstorming* e *brainwriting*) e listas de modos de falhas de outras FMEAs, utilizadas como referência. Isso que dizer que não se deve desperdiçar conhecimento já existente nos relatórios técnicos e bibliografia.

No exemplo que será apresentado deu-se destaque para o modo de falha: perda de gás durante o enchimento, dado que este modo de falha tem reflexo direto na equipe que atua na manutenção. Portanto, a perda do gás neste processo depende dos equipamentos utilizados, da capacitação dos manutentores e uniformização das ações de todas as equipes e dos itens utilizados para a ação de enchimento. A perda do gás, além de contribuir fortemente para o efeito estufa, poderá ter reflexos diretos na saúde do trabalhador.

Ao analisar o modo de falha pela técnica FMEA tem-se o relatório da análise transcrito no Quadro 14.5. Observa-se que o quadro 14.5 está incompleto, pois não apresenta o item e a função do item descritos no Quadro 14.3. Dependendo da aplicação e quando outras

técnicas não foram utilizadas, é importante que se indique todas as colunas da planilha da FMEA. Para o modo de falha – perda de gás durante o enchimento – definiu-se cinco causas e três efeitos. Para controlar as causas e efeitos postularam-se barreiras para as causas e efeitos. Para se ter efetividade da análise propôs-se ações que devem ser implementadas.

Observa-se que o Quadro 14.5 foi desenvolvido para um único modo de falha. Ao fazer isso para todos os modos de falha gera-se um conjunto muito grande de planilhas.

Uma forma de racionalizar o processo, principalmente quanto à implementação das ações propostas, é associar às colunas da FMEA o Número de Prioridade de Risco (NPR) que vai indicar a partir das opiniões dos especialistas que causas e que efeitos devem ser priorizados pelas ações. Ou seja, que barreiras devem ser priorizadas para eliminar ou mitigar as causas que deflagram os modos de falha? A resposta a esta pergunta é obtida de reunião com especialista. A representação das barreiras é muito bem indicada na técnica CNEA.

Quadro 14.5 FMEA do modo de falha potencial "Perda de SF_6 durante o enchimento", em [A211]

Modo de falha	Efeitos	Causas	Controles atuais	Ações propostas
Perda de gás durante o enchimento	- Perda de SF_6 para atmosfera - Inalação de subprodutos tóxicos - Comprometimento à saúde dos colaboradores	Falta de procedimento padronizado	- Capacitação do corpo técnico - Cuidados quanto à fonte de calor próximo ao recebimento (ex. cigarro)	Procedimentos documentados para a operação de enchimento
		Corpo técnico sem capacitação para executar a operação	- Capacitação do corpo técnico - Cuidados quanto à fonte de calor próximo ao recebimento (ex. cigarro)	Procedimentos documentados para a operação de enchimento
		Impacto na válvula	- Verificação da condição da válvula e conexões - Cuidados quanto à fonte de calor próximo ao recebimento (ex. cigarro)	
		Linha de gás em mau estado de conservação	- Verificação da condição da válvula e conexões - Cuidados quanto à fonte de calor próximo ao recebimento (ex. cigarro)	
		Purga na linha de SF_6	- Cuidados quanto à fonte de calor próximo ao recebimento (ex. cigarro)	Fazer vácuo na linha de SF_6

A Figura 14.10 ilustra a CNEA que representa o modo de falha "perda de SF_6 durante o enchimento", nódulo A211 do diagrama IDEFØ do Quadro 14.3 e também apresentado no Quadro 14.5.

O modo de falha assume o evento central chamado de incidente. As causas descritas no Quadro 14.5 ficam à direita do evento central, e os efeitos, à esquerda. Observa-se que há dois padrões de barreiras, as ações propostas na última coluna da FMEA e as que são consideradas já existentes, como a – verificação da condição da válvula e conexão e capacitação do corpo técnico, do lado das causas e a barreira – cuidado quanto à fonte de calor próximo ao recebimento – do lado dos efeitos.

Destaca-se a presença de causas imediatas, ou seja, causas que podem ser percebidas pelos manutentores. Essas causas imediatas já são decorrentes de falhas nas barreiras, tais como: processo para enchimento de SF_6 inadequado e vazamento na válvula ou nas conexões.

Do lado esquerdo da Figura 14.11 estão os efeitos já apresentados no quadro 14.5.

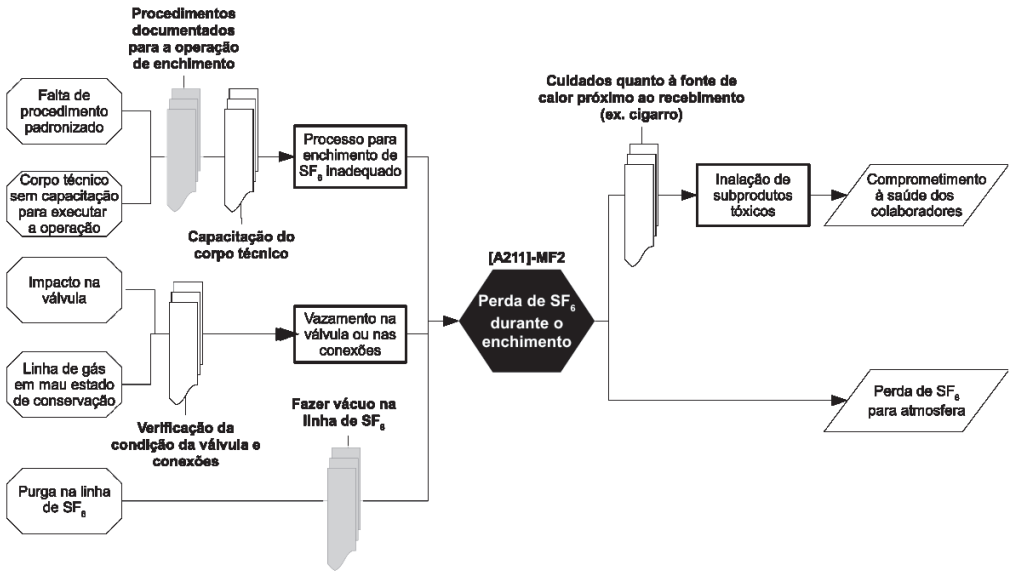


Figura 14.11 CNEA do modo de falha "Perda de SF_6 durante o enchimento", em [A211]

Após esta apresentação do uso das técnicas para análise da Perda de SF_6 durante o enchimento, vale destacar algumas observações:

- As análises foram submetidas aos especialistas da empresa – em reuniões e visitas técnicas – para serem validadas.
- Não foi feita análise de criticidade dos cenários. Assim, foram levantadas barreiras para todas as correntes causais. A seleção das barreiras a serem implementadas e a priorização delas ficou a critério da empresa, que fará essa análise posteriormente. Dessa forma, não foi realizada a avaliação custo/risco/benefício para justificar as barreiras. Além disso, não foi avaliada a possibilidade de contratação de seguro, estratégia já considerada pela empresa.
- Não foi desenvolvido árvore de falha (FTA) para as falhas das barreiras (furos) do processo de manipulação de SF_6 na empresa.

No exemplo de aplicação da técnica FTA, apresenta-se a análise da relação causa/efeito para parte do disjuntor, mais especificamente para um anel de vedação, como o utilizado na ranhura da placa de fechamento do cárter, apresentado no Quadro 14.3.

A função do anel é vedar, e o modo de falha funcional é não vedar. Aprofundando um pouco mais a análise, agora do ponto de vista estrutural, identificou-se que o modo de falha funcional – não vedar – tem origem em diferentes modos de falhas estruturais, entre os quais a deformação permanente do anel de vedação. Esse modo de falha é potencializado por um conjunto de causas raízes e intermediárias, como pode ser visto na árvore de falha (FTA) da Figura 14.12. Na árvore de falha da Figura 14.12, o modo de falha está representado como efeito de um conjunto de causas, que, por sua vez, têm diferentes origens: no ambiente, por decorrência da temperatura ou umidade; na montagem da placa de vedação, proporcionada por pressão excessiva; que por sua vez, é resultado da geometria do alojamento; da variação dimensional da ranhura para alojar o anel; ou de material inadequado para o anel de vedação.

Sabe-se que o modo de falha – deformação permanente do anel de vedação – é proporcionado pela perda da elasticidade do

anel, cujo efeito sobre a junção da placa e cárter é a diminuição da pressão na junta de vedação. Essa perda de pressão é uma das causas de fuga de SF_6, como também facilita a entrada de umidade na câmara que contém o SF_6.

O estudo da deformação permanente do anel de vedação pela técnica da análise de árvore de falha (FTA), exemplificada na Figura 14.12, permite identificar e organizar as causas intermediárias e causas raízes do modo de falha. A atividade de análise é feita com especialistas, normalmente num *brainstorming*. Esse processo de análise é sempre complexo. Neste caso, foi facilitado pelo fato de na coordenação da atividade se dispor de especialista que dominava a taxonomia da técnica e a equipe dispor de especialistas com domínio do conhecimento sobre o sistema técnico analisado.

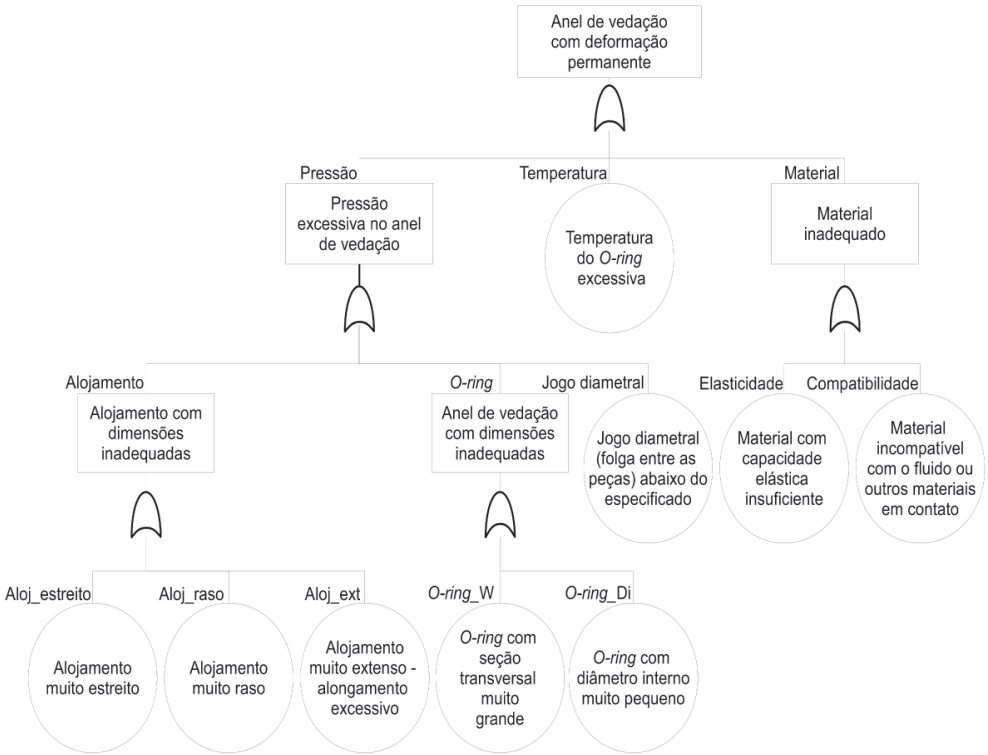


Figura 14.12 Diagrama FTA da falha "Anel de vedação com deformação permanente"

É importante ressaltar que a ideia principal do projeto MitiSF_6 foi fazer uma análise qualitativa para mitigar a perda de gás SF_6. Tal ocorreu devido ao fato de não existir dados para alimentar os cálculos probabilísticos. Diante disso, não foi utilizada a técnica de redes bayesianas. Conclui-se que, pela inexistência de dados estatísticos, a aplicação de redes bayesianas seria bastante complexa e não traria benefícios consideráveis para os resultados da análise e, por esta razão, foi descartada.

Uma vez que se caracterizaram os modos de falha, causas, efeitos e ações para eliminar ou mitigar os efeitos, é possível e recomendável construir alguns cenários para as condições mais críticas. Para a elaboração dos cenários, recomenda-se a metodologia da corrente causal, semelhante ao apresentado na Figura 3.3. Antes, porém, de se estruturar todo o cenário para análise por meio da corrente causal faz-se a avaliação do risco, para melhor priorizar as ações.

14.2.3 AVALIAÇÃO DO RISCO

A avaliação do risco é premida por ações ou motivações com diferentes origens: exigência de leis e normas, exigência de cláusulas de seguro ou contratuais, recomendação de especialistas, relatórios de incidentes ocorridos, semelhança entre sistemas, entre outras. De uma forma ou de outra há sempre a preocupação em evidenciar um cenário crítico, que merece uma atuação diferenciada no trato dos modos de falhas, suas causas, seus efeitos e consequências.

Em qualquer das situações de avaliação há que dispor de algum processo técnico que racionalize as decisões. Ou seja, há que se dispor de critério que possa ser repetido em outras avaliações de evento de risco. A grande dificuldade de se avaliar o risco está na pouca disponibilidade de dados quantitativos, até por que é pouco desejável que se tenha ocorrência de risco. Assim, em grande parte, há que se fazer a avaliação a partir de informações qualitativas.

A avaliação é efetuada em toda a corrente causal (Figura 3.3), desde as causas da condição perigosa e do evento gatilho até as consequências do incidente, incluindo os resultados de cada incidente. As consequências (ou efeitos) são então classificadas quanto à segurança, continuidade, disponibilidade, economia e finança. Cada cenário é avaliado quanto à chance de ocorrer (O), quanto à dificuldade de detecção (D) e a severidade associada (S).

Para tanto, o uso de normas técnicas, como a SAE-J1739 ajuda na avaliação do número de prioridade de risco (NPR) que, nesse caso, é obtido pela multiplicação dos índices de severidade (S), ocorrência (O) e dificuldade de detecção (D). Essa abordagem, embora bem importante e muito utilizada, apresenta alguns inconvenientes, tais como:

- A escala não é homogênea – é idêntica no seu todo e não permite números primos. Por esta escala não existe uma combinação de índices que resulte no NPR igual a 113. De outro modo, fica pouco definido fazer comparações, dado que um NPR igual a 200 não é necessariamente duas vezes mais crítico que um de valor 100.
- Pode-se obter um mesmo valor para o NPR com diferentes combinações de índices, por exemplo, S=9, O=4 e D=3 resulta em um NPR de 108, e S=3, O=4 e D=9 dá o mesmo resultado. No entanto, a primeira combinação se mostra mais crítica, pois a severidade é significante.
- É possível obter NPR relativamente baixo com índices de severidade altos, como, por exemplo, na combinação S=10, O=3 e D=1, tem NPR de 30. Isso pode passar despercebido num processo de avaliação, principalmente quando se utiliza *software* para ajudar na primeira classificação de risco.

Para minimizar essas limitações do NPR, quando se requer uma análise mais elaborada, opta-se por atribuir, além do NPR, um valor especial ao índice de severidade (S). Em grande parte, essa análise normalmente é feita de forma subjetiva, sem uma regra clara. Assim, o resultado dependerá da aversão ou da propensão em aceitar o risco pelo analista.

Com o intuito de contribuir para a avaliação do risco de forma mais racional, desenvolveu –se uma abordagem para categorização da criticidade baseada em relações determinísticas, de forma atributiva em substituição a que, simplesmente, quantifica o NPR pela multiplicação entre a severidade, ocorrência e detecção.

A categorização da criticidade é feita a partir de uma matriz de ocorrência versus severidade, a partir de cada um dos índices de detecção. A Figura 14.13 associada com o Quadro 14.6 exemplificam a aplicação da avaliação de risco a partir de quatro níveis de detecção:

- Detecção fácil (D=1) - A combinação entre ocorrência (O) e severidade (S) proporciona níveis inaceitáveis de risco (IV) quando a ocorrência for ocasional com índice a partir de 5, e a severidade for catastrófica com índice a partir de 9. Também terá níveis inaceitáveis de risco quando a severidade for maior com índice a partir de 5 e a ocorrência for frequente com índice a partir de 9.

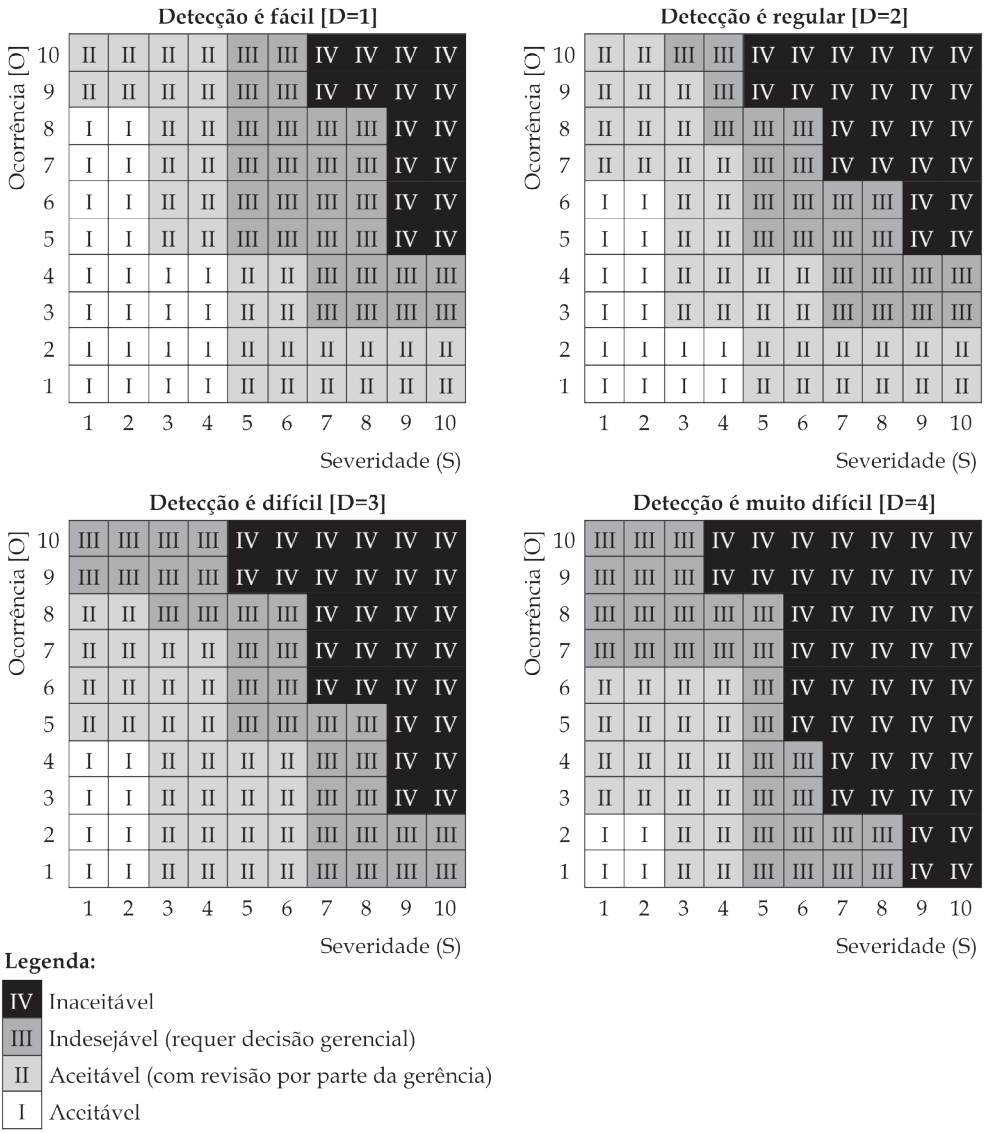


Figura 14.13 Relações determinísticas (regras) para definição do tratamento de cada combinação de índices

- Detecção muito difícil (D=4) – Nesse caso, a combinação entre ocorrência (O) e severidade (S) proporciona níveis inaceitáveis de risco (IV) com muito maior probabilidade. Torna-se risco inaceitável para: ocorrência com índice 1 e 2 com severidade a partir de 9; ocorrência 3 e 4 com severidade a partir de 7; ocorrência de 5 a 8 com severidade a partir de 6; e ocorrência 9 e 10 com severidade a partir de 4.
- Para a detecção regular e difícil a avaliação de risco inaceitável a partir da ocorrência e severidade. Neste caso o nível de criminalidade intermediário fica adequado.

Quadro 14.6 Escala dos índices de severidade, ocorrência e dificuldade de detecção

Severidade (S)	
Categoria	Descrição
1 – 2	Insignificante
3 – 4	Menor
5 – 6	Maior
7 – 8	Perigosa
9 – 10	Catastrófica

Ocorrência (O)	
Categoria	Descrição
1 – 2	Improvável
3 – 4	Remota
5 – 6	Ocasional
7 – 8	Provável
9 – 10	Frequente

Dificuldade de detecção (D)	
Categoria	Descrição
1	Fácil
2	Regular
3	Difícil
4	Muito difícil

Observa-se que tanto as escalas de valores dos índices quanto as regras podem ser adaptadas para cada caso, adequando-se às necessidades de cada análise. Raramente é possível fazer a prevenção de todos os riscos a que o sistema está sujeito. Assim, deve-se fazer a avaliação e priorização dos riscos pela análise da criticidade, a fim de identificar quais riscos podem ser aceitos, confrontando com os objetivos estipulados na fase informacional.

A aplicação da análise de criticidade e avaliação dos riscos são importantes para auxiliar a organização na priorização das ações a serem tomadas com o objetivo de reduzir os riscos. Porém, assim como os demais passos da metodologia, a sua aplicação depende do escopo da análise, influenciadas por decisões gerenciais da organização. Por essa razão, esta análise não foi executada dentro do projeto.

A Figura 14.13 apresenta quatro cenários de risco: aceitável, aceitável com revisão por parte da gerência, indesejável, requerendo revisão pela gerência e inaceitável. A atividade da gerência é deslocar os riscos da condição de inaceitável para aceitável. Uma vez que se tenha o risco

classificado segundo um processo de avaliação como esse, desenvolvem-se as ações para deslocá-los para a condição de aceitável.

Um processo como esse é mais completo que a utilização simples do valor do NPR. Contudo, a partir do uso do NPR é possível identificar aquelas condições que requerem avaliação mais detalhada. É recomendável estruturar um processo de avaliação que proporcione à equipe de análise mais flexibilidade de julgamento dos índices. Por exemplo, estabelecer uma cota crítica igual a 9 para o índice de severidade. Assim, em qualquer processo de avaliação da criticidade, sempre que se atribuir S = 9 há que demandar ações para eliminar ou mitigar a severidade para índices com menores.

14.2.4 DELINEAMENTO DE BARREIRAS

Uma vez modelados e priorizados os potenciais riscos delineiam-se as barreiras para reduzir ou, se possível, eliminar os riscos e mitigar as consequências. Em outras palavras, as barreiras são ações para impedir que os perigos, inerentes aos sistemas técnicos, evoluam para a condição de incidente. Porém, há diferentes estratégias para implementar as barreiras: (a) barreiras para evitar o risco; (b) para transferir o risco; e (c) para reduzir o risco, conforme apresentado no Capítulo 3. É possível e, às vezes, recomendável que se adote mais de uma estratégia.

A ideia de se evitar o risco, apesar de bastante atraente, implica eliminar o perigo, pois somente assim não se correria risco, uma vez que não é possível eliminar totalmente a incerteza do perigo se tornar um incidente. Todo sistema técnico é portador de perigo, que pode evoluir para um incidente. Isso implica que a organização, de alguma forma, está sujeita a algum nível de risco de que o incidente ocorra. Delinear barreiras para evitar o risco pode se tornar muito oneroso, chegando, inclusive, a inviabilizar o negócio.

A transferência do risco está associada à contratação de seguro ou à "terceirização" do sistema técnico exposto ao risco. Isso significa dizer, transferir para outros a responsabilidade pelo incidente, o que, por si só, não exclui o risco do ciclo de vida do sistema técnico. A barreira nesse caso está na existência de suporte financeiro para compensar incidentes que viessem a acontecer. Contudo, em grande parte das vezes, a seguradora exige a existência de procedimentos de

análise e de gestão do risco. O delineamento de barreiras e de gestão do risco, muitas vezes, proporciona descontos significativos no seguro, proporcionando um diferencial competitivo para empresa.

A opção de reduzir o risco, por sua vez, é sempre bem vinda e visa diminuir a probabilidade de ocorrência do incidente e/ou seus efeitos. A atuação para a redução está no delineamento de barreiras para as causas. As barreiras para os efeitos também são recomendáveis. Nesse caso, a barreira visa reduzir as consequências, principalmente para a segurança humana e ambiental.

Aceitar um risco mesmo quando esteja acima dos limites estabelecidos – chamados de riscos retidos ou relutantemente aceitos – pode não parecer prudente, mas, em alguns casos, é a melhor opção. A decisão passa, então, por uma avaliação de custo/risco/benefício. É interessante salientar que o processo de retenção do risco também inclui os riscos ocultos – que a organização não sabe que existem – chamados de involuntariamente retidos.

Como explicitado pela metodologia de gestão de risco sintetizada na Figura 14.1, as barreiras são definidas no passo de delineamento de barreiras, da metodologia de análise de risco, que é a fase conceitual da etapa de delineamento da gestão de risco. A Figura 14.14 exemplifica algumas barreiras definidas na fase de análise de risco. Para melhor esclarecer o leitor quanto às barreiras, serão apresentados alguns exemplos de ações, associadas à nomenclatura da Figura 14.14, que foram construídas ao longo do desenvolvimento do projeto MitiSF_6. As barreiras aqui apresentadas têm uma descrição genérica, mas representam o esforço desenvolvido no projeto MitiSF_6, formalizadas no relatório técnico final [ELETROSUL, 2008]. A seguir exemplifica-se ações para cada uma das barreiras sugeridas. O formato de apresentação visa suscitar desdobramentos que podem ser adaptados para outras aplicações não utilizadas no projeto. De outro modo, também visa preservar informações de cunho exclusivo da empresa onde o projeto foi desenvolvido. Ressalta-se ainda, que cada uma dessas barreiras é desdobrada para atuações específicas, e podem estar associadas às causas como também aos efeitos.

Na Figura 14.14 estão evidenciadas algumas fraquezas das barreiras, que, metaforicamente, são identificadas por "furos". Os furos representam as causas que potencializam os modos de falha que pro-

duzem os incidentes. Os incidentes geram as consequências. Devido a isso, as barreiras precisam ser constantemente revisadas, dado que existe a dinâmica dos processos de falha durante o ciclo de vida.

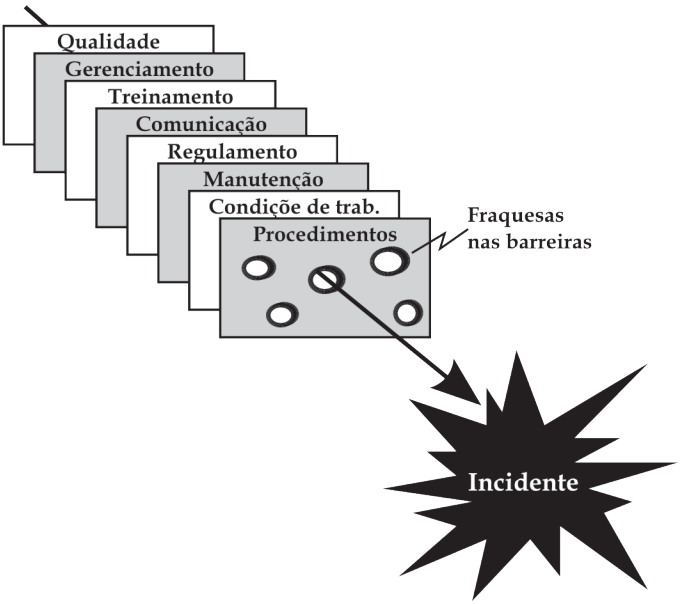


Figura 14.14 Exemplo de delineamento de barreiras definidas na fase de análise de risco

PROCEDIMENTO

- Cada empresa deve estabelecer manuais de atuação tanto no processo de manipulação do SF_6 quanto na atuação sobre os equipamentos. Os manuais serão a base da capacitação do pessoal de manutenção e operação. Também são os instrumentos de consulta sobre os riscos inerentes da utilização do SF_6.
- Sugere-se que a Agência Nacional de Energia Elétrica – ANEEL – desenvolva recomendação na forma de procedimentos, para toda cadeia de transporte do gás SF_6 no território nacional.
- Deve-se dispor de procedimentos para compra, uso e descarte do gás, com o objetivo de ter informações da quantidade de gás existente na empresa e o que foi consumido ao longo do ano.
- Instituir procedimento de limpeza dos disjuntores e descarte do material tóxico retirado de formas a não afetar a segurança humana e ambiental.

CONDIÇÃO DE TRABALHO

- Prover as condições de trabalho de segurança apropriada para os riscos existentes na manipulação do disjuntor, principalmente na abertura do disjuntor, limpeza e manutenção dos itens que tinham contato com o gás.
- Disponibilizar todos os EPIs recomendados pelo setor de segurança, seguindo normas e padrões internacionais de trabalho com gás.
- Dispor de ambiente especial para abertura e limpeza dos disjuntores: roupas, acessórios, itens de proteção para evitar a inalação dos gás ou resíduos do mesmo durante processo de manutenção.
- Dispor de dispositivos especiais para acumular o rejeito resultante do processo de limpeza dos disjuntores.

MANUTENÇÃO

- Efetuar a manutenção com conhecimento das funções para manipular o gás SF_6, como transportar, tratar, armazenar, comprar, descartar e delinear todos os procedimentos para mitigar perdas de gás.
- Estabelecer regras para interferir o mínimo possível no equipamento (realizar enchimento dos disjuntores apenas quando ocorrer alarme).
- Desenvolver programa de manutenção baseado na condição, e não no tempo, para a manutenção geral do equipamento.
- Estabelecer padrões de fazer vácuo na linha em substituição à purga, ou – preferencialmente – manter as mangueiras pressurizadas.
- Centralizar o tratamento de SF_6, e todo SF_6 usado e não aproveitável deve ser segregado e enviado para um descarte especificado.

REGULAMENTO

- Definir regulamentação para manipulação, transporte e armazenagem do gás.

- Adotar regulamentação aderente às normas nacionais e internacionais para que o padrão de análise de consumo seja comparável a outros usuários de SF_6, em nível nacional e internacional.
- Adotar uma regulamentação de política nacional para uso de SF_6 em nível da agência reguladora a exemplo em alguns países da Europa. Controlar consumo (compra, transporte, uso e descarte) de gás em nível nacional, solicitando aos fornecedores de SF_6 que reportem anualmente a quantidade de SF_6 vendida para cada empresa. Solicitar que todas as empresas do setor elétrico reportem, anualmente, a quantidade de SF_6 comprada (para confrontar com a informação do item anterior), vendida e perdida.
- Desenvolver em nível da ANEEL e Ministério de Meio Ambiente um censo de todos os usuários do gás SF_6 no Brasil para avaliar sua quantidade no território nacional.

COMUNICAÇÃO

- Uniformizar o leiaute da comunicação nos equipamentos que operam com SF_6 indicado nos rótulos de garrafas, cilindros e máquinas, todas as informações para controle do gás.
- Desenvolver processos de comunicação para orientar e atualizar informação sobre os cursos de capacitação quanto às normas, procedimentos de operação e manutenção.
- Estabelecer roteiros e regras de compra, recuperação e descarte do gás.
- Estabelecer padrão de comunicação para controle de armazenagem do gás, nos processos de manipulação e de manutenção, e nos controles relativos ao SF_6.

TREINAMENTO/CAPACITAÇÃO

- Estruturar política de capacitação corporativa.
- Desenvolver programas de capacitação com visão ambiental para que os trabalhadores que lidam com o gás SF_6 se conscientizem de quão importante é mitigar a perda do gás, tendo por referência a perda zero de gás.
- Desenvolver programas de visitas a outras empresas para aprender e ensinar as experiências vivenciadas.

- Efetuar treinamento sistemático, com simulação, no uso de itens padronizados de manipulação do gás e para identificar os pontos de vazamento durante a manipulação.
- Refletir sobre a importância do uso de tecnologias atualizadas, como luvas, chaves, conexões, mangueiras, sistema de transporte, sistema de armazenamento etc.
- Desenvolver treinamento para uso do banco de dados e de comunicação de risco.

GERENCIAMENTO

- Dispor de uma metodologia de gestão de risco para vazamento de SF_6.
- Dispor de banco de dados (BD) de pedidos de serviço padronizado com o fim de automatizar a busca de informação quanto as informações sobre falhas do disjuntor (pontos críticos, frequência de ocorrência por modelos, localização, ano de fabricação etc.); gráficos de manutenções relativas ao SF_6 distribuídas por ano; capacitação dos colaboradores com informações para o correto registro no BD; e estrutura de busca apropriada para a gestão das informações.
- Automatizar o cálculo de massa de SF_6 com indicação de complementação ou não de gás, pressão do SF_6 encontrado antes do enchimento, pressão do gás deixado após o enchimento, data do enchimento, temperatura do ambiente, modelo do disjuntor (volume do disjuntor), identificação de fase, módulo e subestação.
- Implementar sistema (informática) para rastreamento do uso e do estoque de SF_6 na empresa.
- Levantar o consumo médio e da capacidade instalada de SF_6 por subestação e regional para estimar o estoque mínimo de cada setor de manutenção e, adicionalmente, indicar ações para reduzir a perda de SF_6.

QUALIDADE

- Desenvolver política de atualização tecnológica específica para os sistemas técnicos que utilizam o SF_6.

- Estabelecer programas de garantia da qualidade a partir da atualização da documentação de procedimentos internos da empresa para apropriar-se dos estudos elaborados.
- Definir o tempo até a medição da qualidade do gás instalada nos disjuntores (ex.: na manutenção de 6 anos) partir das novas políticas, equipamentos e normas.
- Padronizar campos da base de dados de manutenção para complementação de pressão.
- Padronização de todos os cilindros, adequando às normas da ABNT.
- Padronizar procedimentos.

Após a definição das barreiras, é importante verificar se houve alterações nas instalações e indicar como *modus operandi* influencia nos riscos analisados (positiva ou negativamente) ou, ainda, se deflagram novos riscos. Caso isto ocorra, deve-se retornar à analise dos riscos, a partir da existência das barreiras.

Uma vez que os cenários dos riscos estão delineados (incluindo as barreiras), identifica-se ou destaca-se as barreiras mais interessantes, para acompanhar o desempenho das mesmas.

Usualmente, as organizações não têm disponibilidade de recursos suficientes para implementar simultaneamente todas as barreiras levantadas. Assim, estas devem ser priorizadas, e o tratamento dos riscos deve ser feito de acordo com um planejamento.

O passo seguinte ao delineamento de barreiras é a reavaliação da criticidade dos cenários considerados com a implementação das barreiras, para que se possa verificar se os riscos tornaram-se aceitáveis. Caso contrário, deve-se retornar à proposição de novas barreiras ou simplesmente reter o risco mesmo que esteja em um nível acima do considerado aceitável. Caso os custos envolvidos na implementação de barreiras sejam muito elevados em comparação com os custos resultantes da ocorrência do evento indesejado, há que se desenvolver um processo de reavaliação dos riscos.

14.2.5 REAVALIAÇÃO DOS RISCOS

A reavaliação dos riscos é o último passo da fase conceitual da gestão de risco, onde se desenvolve a metodologia de análise de

risco. É de se supor que quando da re-avaliação muito já se conheça do sistema técnico e de todos os incidentes que aconteceram no sistema. Assim, a organização já dispõe de conhecimento e banco de informações que pode ajudar nesse passo de reavaliação.

A partir do conhecimento organizacional (informação, experiência, banco de dados etc.) desenvolve-se a re-avaliação e incorporação de novas experiências e informações.

Para melhor ilustrar esse passo, toma-se por referência a espiral do conhecimento apresentada na Figura 14.15. Nela, o conhecimento está dividido em dois níveis: tácito e explícito, que, ao longo do ciclo de vida, são convertidos em quatro formas: externalização, combinação, internalização e socialização.

CONHECIMENTO TÁCITO

É conhecimento inerente ao indivíduo, normalmente difícil de ser compartilhado. É um conhecimento muito sensível, e normalmente é desenvolvido ao longo do tempo, a partir de muitas ações relacionadas com a atividade técnica, programas de capacitação e treinamento, leitura de literatura técnica, manuais e normas. A outra fonte de evidenciação do conhecimento tácito se dá no convívio com outros técnicos, nos programas de visitação, seminários e cursos.

O projeto MitiSF_6 desenvolveu diferentes atividades para aproximar-se desse conhecimento tácito, a partir dos profissionais das instituições que operam com o SF_6. Para tanto, estruturou-se um programa de visitas às oficinas da ELETROSUL, cujas conversas com os profissionais foram orientadas por questionários estruturados e não estruturados. Também fez-se visitas a empresas importantes para o setor elétrico em nível nacional e internacional. Em nível nacional, foram visitadas as empresas Itaipú Bi-Nacional, Furnas e o Instituto de Pesquisa Cepel no Rio de Janeiro. Em nível internacional, visitou-se a empresa Eliá e DILO, na Bélgica, Areva, na França, e Iberdrola, na Espanha.

Outra forma eficiente de elicitar o conhecimento tácito é nas atividades de seminários, congressos, *workshop* etc. Nesse sentido, cita-se duas experiências bem sucedidas: o seminário sobre gás SF_6: aspectos técnicos, ambientais e de segurança, realizado em

2007, sob a coordenação da ELETROSUL e da CELESC (AZEVEDO & DIAS, 2007) e o *workshop* realizado no departamento de meio ambiente da região de Flandres (LNE – Departement Leefmilieu, Natuur en Energie), na Bélgica, para discutir implementação de normas para regulamentar o processo de controle, transporte e manipulação de SF_6 na Europa, com o representante da empresa DILO (Eltec BVDA) para conhecer as atualizações tecnológicas em máquinas de recuperação de gás.

CONHECIMENTO EXPLÍCITO

Consiste no conhecimento adquirido pela informação registrada e disponibilizada em diferentes formas (livros, artigos, normas, catálogos, entre outros). O conhecimento explícito na literatura especializada fornece as experiências técnicas necessárias e imprescindíveis para a formalidade técnica e científica.

O rigor necessário para atuar na gestão de risco e análise de risco, dada a importância para o ambiente e para a segurança humana, é tal, que nenhuma das ações nesse campo de conhecimento deve ser executada se não tiver explicitado na forma de procedimentos, normas, regulamentos, instrução, entre outros. Ou seja, se não estiver escrito, não existe gestão de risco. O conhecimento tácito é do indivíduo, mas na organização o conhecimento deve estar na forma explícita.

Observa-se que o processo de conhecimento é dinâmico. Então, por meio de diferentes processos de elicitação, obtém-se o conhecimento tácito. Contudo, a permanência desse conhecimento nos dias atuais, e principalmente em nível organizacional, ocorre se ele for escrito, ou seja, transformado em conhecimento explícito.

Ao longo do ciclo de vida dos sistemas técnicos, esse conhecimento é crescente e se transforma de tácito para explícito e vice-versa, sob diferentes formas de conversão caracterizada na Figura 14.15 como expiral do conhecimento, que apresenta as seguintes formas de conversão; externalização, combinação, internalização e socialização.

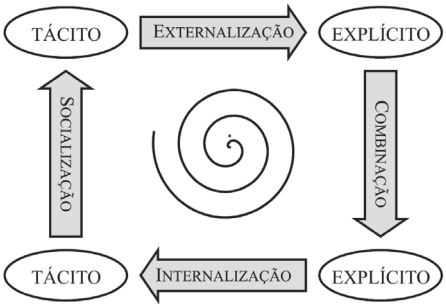


Figura 14.15 Espiral do conhecimento

- Externalização: consiste em registrar o conhecimento tácito de forma clara, tornando-o acessível a outros indivíduos, pela elaboração de procedimentos a serem seguidos em uma atividade. Por exemplo, pela explicitação na forma de catálogos, manuais, normas.
- Combinação: consiste em combinar diferentes conhecimentos explícitos, dando origem a outros, por exemplo, quando um procedimento documentado é melhorado por meio da combinação do conhecimento relacionado a outros procedimentos. O campo acadêmico se nutre desse conhecimento, a partir dos livros, artigos, relatórios técnicos, patentes.
- Internalização: consiste em adquirir o conhecimento explícito, tornando-o em seu conhecimento tácito, por exemplo, quando um técnico estuda um manual para aprender como uma tarefa deve ser executada. Esse processo pode ocorrer pela iniciativa de autodidatismo do indivíduo, por meio da leitura, ou por meio de cursos, seminários, aulas e palestras.
- Socialização: consiste no compartilhamento do conhecimento tácito com outros indivíduos, por exemplo, a transmissão de conhecimento do mestre ao aprendiz, nos programas de capacitação, no treinamento, com grande tendência para atividades práticas.

Devido à grande quantidade de informações coletadas durante uma análise de risco, a organização das mesmas é um problema constante, podendo comprometer a gestão do conhecimento. É preciso que a informação esteja disponível e, principalmente, seja facilmente

compreendida por todos os envolvidos nas atividades, como equipe responsável pela análise, equipes de manutenção, equipes responsáveis pela operação dos sistemas técnicos, setor de suprimentos etc.

Nessa condição, a metodologia ganha importância, dado que permite adquirir o conhecimento dos especialistas, concentra na estrutura de análise e torna-o disponível para a organização.

A metodologia de análise, por evidenciar causas, modos de falhas, incidentes e barreiras necessárias, favorece a modelagem das variáveis relacionadas aos riscos de uma organização. Como já visto, pode-se consultar especialistas, desde os processos envolvidos em suas atividades até equipamentos e ações a serem seguidas para gerenciar os riscos. A aplicação das técnicas auxilia na externalização do conhecimento de especialistas consultados, pois organiza e padroniza as informações coletadas. O conhecimento dos diferentes especialistas pode ser combinado, possivelmente gerando novos conhecimentos, podendo-se ainda racionalizá-los pela eliminação de informações desnecessárias (ruído). Com isso, é possível obter modelos bastante detalhados dos sistemas em análise e definir medidas efetivas para gerenciar os riscos.

Com o apoio de metodologia e uso de técnicas apropriadas, torna-se mais simples o processo de elicitação do conhecimento, combinação e externalização por meio de capacitação, tanto na implantação dos planos de ação e treinamento dos colaboradores, quanto no caso de alterações no quadro de integrantes da equipe responsável pela execução da análise de risco.

A capacitação é facilitada, pois, além de organizar as informações, a metodologia permite visualizar as relações entre os processos, sistemas técnicos, medidas de gerenciamento dos riscos e, como consequência, torna o entendimento do corpo técnico responsável mais simples.

Uma vez que o conhecimento foi estruturado, o programa de reavaliação fica pronto para ser implementado. A continuidade deste processo gera a cultura de qualidade em relação as ações para prevenir o risco e assim, a gestão do risco ficará facilitada.

REFERÊNCIAS BIBLIOGRÁFICAS

ABB – Catálogo. **Spring operating mechanism for highvoltage circuit breakers**. Disponível em: <http://library.abb.com/>, acessado em 27/05/2009.

ABNT(Associação Brasileira de Normas Técnicas). **ABNT NBR 10019:** Subestação blindada isolada a gás para tensões nominais iguais ou superiores a 72,5 kV. 1. ed. Rio de Janeiro, 1987.

_____. **ABNT NBR 11902:** Hexafluoreto de Enxofre – Especificação. 1. ed. Rio de Janeiro, 1992.

_____. **ABNT NBR 12318:** Hexafluoreto de enxofre. 1. ed. Rio de Janeiro, 1992.

_____. **ABNT NBR 5462:** Confiabilidade e matenabilidade – terminologia. Rio de Janeiro, 1994. 37 p.

_____. **ABNT NBR ISO 9000:** Sistemas de gestão da qualidade - Fundamentos e vocabulário. Rio de Janeiro, 2000.

_____. **ABNT ISO/IEC Guia 73:** Gestão de risco – vocabulário – recomendações para uso de normas. 1. ed. Rio de Janeiro, 2005.

_____. **NBR/IEC 62271-100**: Equipamentos de alta-tensão. Parte 100: Disjuntores de alta-tensão de corrente alternada. Rio de Janeiro, 2006.

_____. **ABNT NBR 7500:** Identificação para o transporte terrestre, manuseio, movimentação e armazenamento de produtos. Rio de Janeiro, 2009.

_____**. ABNT NBR ISO 9004:** Gestão para o sucesso sustentado de uma organização — Uma abordagem da gestão da qualidade. Rio de Janeiro, 2010.

ALONÇO, A. S. **Metodologia de projeto para a concepção de máquinas agrícolas seguras.** 221 p. Tese (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2004.

AREVA. **Curso tutorial sobre confiabilidade de equipamentos de alta tensão**. CEPEL, Rio de Janeiro, 2006.

AZEVEDO Jr., Altair Coutinho de, DIAS, Acires. **Análise e desenvolvimento de procedimentos para a operação e manutenção de disjuntores visando mitigar a emissão de SF6 – MitiSF6**. Seminário sobre gás SF6: Aspectos Técnicos, Ambientais e de Segurança. Florianópolis: sede da ELETROSUL, 21 e 22 de Agosto de 2007.

BACK, N. et al. **Projeto integrado de produtos:** planejamento, concepção e modelagem. 1. ed. São Paulo: Editora Manole Ltda., 2008. 601 p.

BERNARD, Georges. **Breaking by Auto-Expansion**. Cahiers Techniques, Schneider Electric's - Collection Technique, n. 171, p. 16, 1995.

BERTSCHE, B. **Reliability in Automotive and Mechanical Engineering.** [S.l.]: Springer, 2008. ISBN 978-3-540-33969-4.

BIASOTTO, E. **Modelo de gestão da manutenção para produtividade: uma aplicação para indústria de celulose e papel**. Florianópolis: UFSC. Dissertação de Mestrado. 170p. 2006.

BILLINTON, Roy, ALLAN, Ronald N., **Reliability Evaluation of Engineering Systems**. Editora Plenum Press, Second Edition, 1992.

BLANCHARD, B., VERNA, D., PETERSON, E.L. **Maintainability**. New York: John Wiley & Sons, Inc. 1995.

BRASIL. Ministério das Relações Exteriores. **Decreto Lei No 5.445 – 2005:** Promulga o protocolo de Quioto à convenção-quadro das nações unidas sobre mudança do clima, aberto a assinaturas na cidade de Quioto, Japão, em 11 de dezembro de 1997, por ocasião da terceira conferência das partes da convenção-quadro das nações unidas sobre mudança do clima. Brasília, DF, 2005.

BRASIL. Ministério do Planejamento e Orçamento. **Glossário de defesa civil, estudos de riscos e medicina de desastres.** Brasília, DF, 1998.

BUENO, F. d. S. **Grande Dicionário Etimológico-Prosódico da Língua Portuguesa**. São Paulo: Lisa, 1988.

CALIL, L. F. P. **Metodologia para gerenciamento de risco:** foco na segurança e na continuidade. 231 p. Tese (Doutorado em Engenharia Mecânica) – Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2009.

CIGRÉ (International Council on Large Electric Systems). **SF6 recycling guide:** Revised version 2003. Paris, França, 2003.

COLOMBO, Roberto. **Disjuntores de Alta Tensão**. Editora Nobel, 1986.

DELVOSALLE, C. et al. **Aramis project: a comprehensive methodology for the identification of reference accident scenarios in process industries**. Journal of hazardous materials, Elsevier, v. 130, p. 200 – 219, 2006.

DIANOUS, V.; FIÉVEZ, C. **Aramis project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance**. Journal of hazardous materials, Elsevier, v. 130, p. 220 – 233, 2006.

DIAS, A. **Metodologia para análise da confiabilidade em freios pneumáticos automotivos**. Campinas, SP: Universidade Estadual de Campinas – UNICAMP. Tese de doutorado. 1996.

DIAS, A. **Projeto para Confiabilidade: Conceitos e Fundamentos**. Livro: Gestão do Ciclo de Vida dos produtos. Coleção Fábrica do Milênio. Volume III. São Carlos, SP. Editora: Cubo Multimídia. Cap 16, p229-244. 2005.

ENERVAC CORPORATION. **Informações sobre o produto:** equipamento de tratamento de gás SF6. [S.l.], 2004. Disponível em: <http://www.enervac.com/Portuguese/01.shtml>. Acesso em: 14 de jul. de 2006.

ELETROSUL. **Análise e desenvolvimento de procedimentos para operação e manutenção de disjuntores visando mitigar a emissão de SF_6 – MitiSF6**. Projeto de pesquisa ELETROSUL/UFSC, 2008.

_____. **Missão, visão e valores.** Disponível em <http://www.eletrosul.gov.br/home/conteudo.php?cd=163>. Página atualizada em 30 julho 2010. Acesso em 16 agosto 2010.

EPA (Environmental Protection Agency). **Emission Reduction Partnership for Electric Power Systems:** 2003 annual report. [S.l.], 2004. Disponível em: <http://www.epa.gov/electricpower-sf6/resources/index.html>. Acesso em: 2 jun. 2008.

_____. **Emission Reduction Partnership for Electric Power Systems:** 2006 annual report. [S.l.], 2007. Disponível em: <http://www.epa.gov/electricpower-sf6/resources/index.html>. Acesso em: 2 jun. 2008.

ERICSON II, C. A. **Hazard analysis techniques for system safety.** New Jersey: John Wiley & Sons, Inc., 2005.

FERREIRA, A. B. de H. **Dicionário Aurélio básico da língua portuguesa.** Rio de Janeiro: Nova Fonteira, 1988. ISBN 8520908268.

FIENBERG, S. E. When did bayesian inference become "bayesian"? **Bayesian analysis - The journal**, v. 1 (Issue 1), p. 140, 2006.

FIHMAN, A. El SF6, características físicas y químicas. **Caderno Técnico Schneider**, Schneider Eletric, n. 79, 1997.

FUENTES, F. F .E. M**etodologia para inovação da gestão de manutenção industrial**. Florianópolis: UFSC. Tese de doutorado. 170p. 2006.

GANZON, R. D. **High Voltage Circuit Breakers:** Design and applications. 2a. ed. New York: Marcel Dekker, 2002. 456 p. ISBN 0824707990.

GOWLAND, R. **ARAMIS project: the accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: a step forward towards convergent practices in risk assessment?** *Journal of Hazardous Materials*, v.130, p.307–310. Elsevier, 2006.

HELMAN, H.; ANDERY, P. R. P. **Análise de falhas:** (aplicação dos métodos de fmea-fta. Belo Horizonte, Minas Gerais, Brasil: Fundação Cristiano Ottoni, 1995. ISBN 85-85447-17-6.

IANNACCHIONE, A. T.; ESTERHUIZEN, G. S.; TADOLINIM, S. C. **Using major hazard risk assessment to appraise and manage escapeway instability issues: A case study**. In: International Conference On Ground Control In Mining, 26., 2007

IEC (International Electrotechnical Commission). **IEC 60376:** Specification of technical grade sulfur hexafluoride (SF_6) for use in electrical equipment. [S.l.], 2005.

_____. **IEC 61025**: Fault Tree Analysis. 2 ed. Genebra, 2006.

_____. **IEC 60050:** International Electrotechnical Vocabulary. Electropedia: The World's Online Electrotechnical Vocabulary, disponível em: <http://www.electropedia.org/>. Acessado em 27 mai. 2009.

IGEO (Instituto Geográfico Português). RISE (Rede de Informação de Situações de Emergência). **Matériais Perigosas:** hexafluoreto de enxofre. [S.l.], 2000. Disponível em: <http://scrif.igeo.pt/ASP/>. Acesso em: 08 jan. 2009.

JENSEN, F. V. **Reliability in engineering design.** New York: Springer-Verlag, 2001.

KOCH, D. SF6 properties, and use in mv and hv switchgear. **Cahiers Techniques,** Schneider Eletric, n. 188, p. 26, 2003.

KUMAMOTO, H.; HENLEY, E. J. **Probabilistic risk assessment and management for engineers and scientist.** 2a. ed. New York: IEEE Press Marketing, 1996. ISBN 0780310047.

LAPLACE, P. S. A **Philosophical essay on probabilities.** New York: Springer-Verlag, 1995. Tradução por Andrew I. Dale da 5a edição francesa de 1825.

LÉGER, A. et al. Bayesian network modelling the risk analysis of complex socio technical systems. In: WORKSHOP ON ADVANCED CONTROL AND DIAGNOSIS, 4., Nancy, France. In: . [S.l.: s.n.], 2006. **Proceedings ...**

LEVESON, N. et al. **A systems theoretic approach to safety engineering.** Cambridge, MA, 2003.

LEWIS, S.; HURST, S. Bow-tie anelegant solution. **Strategic risk**, p. 8, November 2005.

MAURINO, D. E. et al. **Beyond aviation human factors:** safety in high technology systems. Aldershot, England: Ashgate Publishing Limited, 1995.

MOHR, R. R. **Failure modes and effects analysis**. 8th. ed. [S.l.], Jan. 1994. Disponível em: <http://www.fmeainfocentre.com/handbooks/fmeamanual.pdf>. Acesso em: 10 nov. 2008.

MONCHY, F., **A função manutenção**. São Paulo: Ebras/Durban. 1989. 424p.

MOSLEH, A. et al. An integrated framework for identification, classification, and assessment of aviation systems hazards. In: INTERNATIONAL CONFERENCE ON PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT (PSAM), 7., Berlin. In: . [S.l.: s.n.], 2004. **Proceedings ...**

MOSLEH, A., DIAS, A. **Towards an integrated framework for aviation hazard analysis**," University of Maryland Report, 2003.

MOUBRAY, John **Reliability Centered Maintenance (RCM)** - Manutenção Centrada em Confiabilidade. ISBN 0-9539603 publicado por Aladon Ltda. Edição Brasileira - Segunda Impressão, 2003.

NAKAJIMA, S., TMP **Development program, implementing total productive maintenance**, Cambridge Productivity Press, New York, NY., 1989.

NIST (National Institute of Standards and Technology). **FIPS PUBS 183:** Integration definition for function modeling (IDEFØ). Gaithersburg, MD, 1993. Draft Federal Information Processing Standards Publication.

NOWLAN, F. S.; HEAP, H. F. **Reliability centered maintenance**. National Technical Information Service, USA, Report n.AD/A066-579, 1978.

RAMZAN, A. **The application of thesis bow-ties in nuclear risk management**. The journal of the safety & reliability society, UK Safety and Reliability Society, v. 26, n. 1, 2006

REASON, J. **Managing the risk of organizational accidents.** England: Ashgate Publishing Limited, 1997.

RIGONI, E. **Metodologia para Implantação da Manutenção Centrada em Confiabilidade: uma abordagem fundamentada em Sistemas Baseados em Conhecimento e Lógica Fuzzy**. Florianópolis: UFSC. Tese de doutorado. 170p. 2009.

RAUSAND, M.; HØYLAND, A., **System reliability theory: models, statistical methods, and applications**. John Wiley & Sons, New York, 2004.

SAE (Society of Automotive Engineers). **JA1011**: Evaluation criteria for reliability-centered maintenance (rcm) processes. [S.l.], 1999.

_____. **JA1012**: A guide to the reliability-centered maintenance (RCM) standard. [S.l.], 2002.

_____. **J1739:** Potential failure mode and effects analysis in design (Design FMEA), potential failure mode and effects analysis in manufacturing and assembly processes (Process FMEA), and potential failure mode and effects analysis for machinery (Machinery FMEA). [S.l.], 2002.

SAKURADA, E. Y. **As técnicas de análise dos modos de falhas e seus efeitos e análise de árvore de falhas no desenvolvimento e na avaliação do produto.** Dissertação (Mestrado em Engenharia Mecânica) – Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2001.

SCAPIN, C. A., **Análise sistêmica de falhas**. Editora de Desenvolvimento Gerencial, 1 ed., Belo Horizonte, 1999.

SIHVENGER, J. C. et al. **Manuseio, Segurança e Manutenção de Hexafluoreto de Enxofre (SF_6) em Equipamentos Elétricos**. CIGRÉ CE D.1 - Comissão de Estudos de Materiais e Tecnologias Emergentes - Grupo de Trabalho de Líquidos Isolantes - GT D1.01. Dezembro de 2008.

SMITH, A. M. **Reliability-centered maintenance.** Boston, MA: Mc Graw Hill, 2001.

THEOLEYRE, S. MV Breaking Techniques. **Cahiers Techniques**, n. 139, p. 36, 1999.

TRAFO. **Catálogo – Disjuntores a gás SF6 para uso externo**. Trafo Equipamentos Elétricos S.A., 2009.

TRBOJEVIC, V. Linking risk assessment of marine operations to safety management in ports. In: BIENNIAL MARINE TRANSPORTATION SYSTEM RESEARCH AND TECHNOLOGY COORDINATION CONFERENCE, 6., Washington. In: . [S.l.: s.n.], 2001. **Proceedings ...**

_____. Linking risk analysis to safety management. In: INTERNATIONAL CONFERENCE ON PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT (PSAM), 7., Berlin. In: . [S.l.: s.n.], 2004. **Proceedings ...**

UNIÃO EUROPEIA. Regulamento (CE) **N° 305/2008 da Comissão de 2 de Abril de 2008:** que estabelece, nos termos do Regulamento (CE) no 842/2006 do Parlamento Europeu e do Conselho, os requisitos mínimos e as condições para o reconhecimento mútuo da certificação do pessoal que procede à recu-

peração de determinados gases fluorados com efeito de estufa em comutadores de alta tensão. Jornal Oficial da União Europeia, n. L092, p. 0017 – 0020, 2008. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:092:0017:0020:PT:PDF>. Acesso em: 8 jan. 2009.

UNO (United Nations Organization). IPCC (Intergovernmental Panel on Climate Change). Climate Change 2001: *The physical science basis. Cambridge, 2001.*

_____. **Climate Change 2007**: The physical science basis. Cambridge, 2007.

UNO (United Nations Organization). UNFCCC (United Nations Framework Convention on Climate Change). **The Kyoto Protocol**. Kyoto, Japan, 1998. D isponível em: <http://unfccc.int/kyoto protocol/items/2830.php>. Acesso em: 2 jun. 2008.

USA (United States of America). DOD (Department of Defense). **MIL-STD-1629A**: Procedures for performing a failure mode, effects and criticality analysis. Washington, 1980.

USA (United States of America). NRC (Nuclear Regulatory Commission). **NUREG 0492:** Fault tree handbook. Washington, 1981.

VORPE, Michel André, FILHO, Oscar Kastrup, FRANÇA, Wilson Jorge. **Disjuntores e Chaves: Aplicação em Sistemas de Potência** / Capítulo 1 – Aspectos Básicos e Construtivos. Editora da Universidade Federal Fluminense, Niterói – Rio de Janeiro, 1996.

AUTORES

Acires Dias é engenheiro mecânico, mestre em engenharia mecânica pela Universidade Federal de Santa Catarina (UFSC) e doutor em projeto e mecânica dos sólidos pela Universidade Estadual de Campinas, UNICAMP, em 1996. Realizou estágio de pós-doutorado em confiabilidade e análise de risco na University of Maryland, USA, em 2003. É professor do Departamento de Engenharia Mecânica da UFSC desde 1984. Desde 2009 é diretor geral do Centro de Engenharia da Mobilidade, Campus UFSC, em Joinville. Leciona os conteúdos de elementos de máquinas, manutenção, mantenabilidade, confiabilidade e análise de risco.

Luís Fernando Peres Calil é engenheiro mecânico e doutor em gerenciamento de risco pelo Departamento de Engenharia Mecânica da Universidade Federal de Santa Catarina (UFSC). É professor na UFSC, onde leciona sobre estatística, confiabilidade de sistemas técnicos, projeto de elementos de máquinas e pesquisa em gestão de risco em sistemas técnicos, tanto no que se refere à segurança do homem e do meio ambiente quanto à confiabilidade/continuidade.

Emerson Rigoni é graduado em Engenharia Elétrica pela Universidade Tecnológica Federal do Paraná (UTFPR). Fez o mestrado em Engenharia Elétrica e Informática Industrial pela UTFPR em 2002. Doutorou-se em Engenharia pela Universidade Federal de Santa Catarina (UFSC) em 2009. É professor da UTFPR desde 1996, atuando no ensino, pesquisa e extensão, junto aos seguintes temas: metodologias para gestão da manutenção, métodos multicritérios para apoio a tomada de decisão e confiabilidade aplicada à engenharia. Atual coordenador do curso de Engenharia Elétrica da UTFPR.

André Ogliari é engenheiro mecânico, graduado em 1985, na Universidade de Caxias do Sul, RS. Em 1990, obteve mestrado em Engenharia Mecânica, na Universidade Federal de Santa Catarina. Seu doutorado foi concluído em 1999, na Universidade Federal de Santa Catarina, onde é professor do Departamento de Engenharia Mecânica, desde 1995. Atua no desenvolvimento de produtos desde 1986, com pesquisas no desenvolvimento de protótipos de máquinas agrícolas, metodologia de projeto, ferramentas computacionais de apoio ao projeto, gerenciamento do desenvolvimento de produtos e inovação de produtos. Ministra conteúdos de metodologia de projeto na graduação em engenharia da UFSC e de gerenciamento do desenvolvimento de produtos, na pós-graduação.

Eduardo Yuji Sakurada concluiu a graduação em 1998 e o mestrado em 2001, ambos em Engenharia Mecânica pela Universidade Federal de Santa Catarina. Atuou como engenheiro pesquisador nas áreas de sistemas hidráulicos (LASHIP/UFSC), de 2003 a 2006, e análise de falhas (NeDIP/UFSC), de 2006 a 2009. É professor no Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC) desde 2009, onde ministra as disciplinas de hidráulica & pneumática e desenho técnico.

Heitor Azuma Kagueiama é engenheiro mecânico formado pela Universidade Federal de Santa Catarina em 2008. É mestrando em Engenharia Mecânica e pesquisador na área de análise de falhas e confiabilidade.

EQUIPE TÉCNICA DA ELETROSUL

Altair Coutinho Azevedo Jr. é graduado em Engenharia Mecânica na Universidade Federal de Santa Catarina. Especializou-se em Gestão do Mercado de Energia Elétrica, em 2004, na Estácio de Sá. É gerente de divisão de Coordenação da Manutenção da ELETROSUL desde 2008. Trabalhou por 15 anos como chefe do setor da oficina central de equipamentos de pátio de subestações da ELETROSUL.

Clóvis Nicoleit Carvalho é engenheiro eletricista, graduado pela Universidade Federal de Santa Catarina. Aluno de mestrado do Pro-

grama de Pós-Graduação do Departamento de Engenharia Elétrica da UFSC. Desde 2001 trabalha na ELETROSUL onde atuou na área de Operação do Sistema Elétrico, coordenou o Programa de Pesquisa e Desenvolvimento (P&D) e o Comitê de P&D da ELETROSUL. Atualmente, é chefe do setor de Eficiência Energética da Empresa.

Alzete Martins Quadros é graduada em Química na Universidade Federal de Santa Catarina – UFSC, em 1999. Obteve o título de Mestre em Ciência e Engenharia de Materiais, na área de concentração de Materiais Poliméricos, na UFSC, em 2007. É funcionária da ELETROSUL desde 1989, onde, atualmente, desenvolve atividades na área de Engenharia de Manutenção de equipamentos elétricos de alta e extra-alta tensão. Integrou o Conselho Regional de Engenharia, Arquitetura e Agronomia de Santa Catarina – CREA – SC, atuando como conselheira na Câmara Especializada de Engenharia Química, no período de 2005 – 2010.

Jovani Afonso de Souza é graduado em Química pela Universidade Federal de Santa Catarina. Participou, em 1993, do curso "Polymer Material and Technology" promovido pela JICA, no Japão. Atuou durante 23 anos no Laboratório Físico-Químico da ELETROSUL nas áreas de análises de materiais dielétricos e de Corrosão. Trabalha atualmente no Departamento de Manutenção da ELETROSUL, Divisão de Coordenação da Manutenção.

LISTA DE SIGLAS

Siglas das organizações ou unidades organizacionais citadas no texto:

ABNT –	Associação Brasileira de Normas Técnicas
ANEEL –	Agência Nacional de Energia Elétrica
CAPIEL –	Coordinating Committee for the Associations of Manufacturers of Industrial Electrical Switchgear and Control gear / European Union
CEPEL –	Centro de Pesquisas de Energia Elétrica / Eletrobras
CIGRÉ –	Comité International des Grands Réseaux Electriques
DMS –	Departamento de Manutenção do Sistema da Eletrosul
EMC –	Departamento de Engenharia Mecânica da Universidade Federal de Santa Catarina
EPA –	Environmental Protection Agency / United States of America
FEESC –	Fundação do Ensino da Engenharia em Santa Catarina
IEC –	International Electrotechnical Commission
ISO –	International Organization for Standardization
NASA –	National Aeronautics and Space Administration / United States of America
NeDIP –	Núcleo de Desenvolvimento Integrado de Produtos
NRC –	Nuclear Regulatory Commission / United States of America
ONU –	Organização das Nações Unidas (o mesmo que UNO)
SAE –	Society of Automotive Engineers
SAE –	Sociedade de Engenheiros da Mobilidade
UFSC –	Universidade Federal de Santa Catarina
UNICAMP –	Universidade Estadual de Campinas
UNO –	United Nations Organization (o mesmo que ONU)
USA –	United States of America

Outras siglas utilizadas no texto:

ALARA – *As low as reasonably achievable* (Tão baixo quanto se possa considerar razoável aceitar)

ALARP – *As low as reasonably practicable* (Tão baixo quanto e razoavelmente praticável)

BTA – *Bow-tie analysis* (Análise gravata borboleta)

CNEA – *Causal network event analysis* (Análise de eventos por rede causal)

DAG – *Directed acyclic graph* (Grafos acíclicos direcionados)

DMS – *Document management system* (Sistema de gerenciamento de documentos)

DNA – *Deoxyribonucleic acid* (Ácido desoxirribonucleico)

DRE – *Detail reference expression* (Expressão de referência de detalhe)

EPI – Equipamentos de proteção individual

ESD – *Event sequence diagram* (Diagrama sequencial de eventos)

ETA – *Event tree analysis* (Análise por árvore de evento)

FAST – *Functional analysis system technique*

FMEA – *Failure modes effects and analysis* (Análise do modo de falha e seus efeitos)

FMECA – *Failure modes, effects and criticality analysis* (Análise do modo de falha, efeitos e criticidade)

FTA – *Fault tree analysis* (Análise por árvore de falha)

GIS – *Gas insulated substation* (Subestação blindada)

GPL – *General public licens*e (Licença pública geral)

GWP – *Global warming potentia*l (Potencial efeito-estufa)

HAZOP – *Hazard and operability* (Perigos e operacionalidade)

ICOM – Código de entrada (*Input*), controle (*Control*), saída (*Output*) ou mecanismo (*Mechanism*) na técnica IDEF0

IDEFØ – *Integration definition for function modeling*

MARS – *Major accident reporting system database*

MCC – Manutenção centrada em confiabilidade (o mesmo que RCM)

MTBF – *Mean time between failure* (Tempo médio até a falha)

MTO – *Maximum tolerable outage* (Tempos máximos de interrupção tolerável)

MTTF – *Mean time to failure* (Tempo médio entre falhas)

MTTFF – *Mean time to first failure* (Tempo médio até a primeira falha)

NCAF – *Net cost of averting a fatality* (Custo líquido médio para prevenir uma fatalidade)

NPR – Número de prioridade de risco (*Risk priority number*)

OEE – *Overall equipment effectiveness* (Efetividade global do equipamento)

P&D – Pesquisa e desenvolvimento

PAC – Programa de Aceleração do Crescimento

PRA – *Probabilistic risk assessment* (Avaliação probabilística de risco)

RBD – *Reliability block diagram* (Diagramas de blocos de confiabilidade)

RCA – *Root Cause Analysis* (Análise da causa raiz)

RCM – *Reliability centered maintenance* (o mesmo que MCC)

RPO – *Recovery point objective* (Objetivos para os pontos de recuperação)

SGR – Sistema de gestão de risco (*Risk managment system*)

SOD – Concatenação das notas atribuídas ao índices Severidade (S), Ocorrência (O) e dificuldade de Detecção (D) na técnica FMECA

SOP – *Subtract and operate procedure* (Procedimento de retirar e operar)

STAMP – Systems-Theoretic Accidents model and Processes

TPM – *Total productive maintenance* (Manutenção produtiva total)

WBS – *Work breakdown structure* (Desdobramento da estrutura de trabalho)

GLOSSÁRIO

Aceitação do risco (*Risk acceptance*): Opção por conviver com o risco – planejando-se, ou não, para sua ocorrência.

Acidente (*Accident*): Eventos que resultem em dano ao homem ou ao ambiente. Neste trabalho, o termo incidente será preferencialmente utilizado – pois engloba o conceito de acidente.

Ameaça (*Threat*): Evento ou condição com potencial de causar um incidente.

Analise / avaliação de riscos (*Risk assessment*): "Processo completo de análise e avaliação de riscos" (ABNT, 2005, p. 4).

Analise de risco (*Risk analysis*): "Uso sistemático de informações para identificar fontes e estimar o risco" (ABNT, 2005, p. 4).

Análise do impacto no negócio (*Business impact analysis*): Processo que analisa as consequências de um incidente no negócio da organização.

Avaliação do risco (*Risk evaluation*): Confronto entre o risco analisado com os objetivos de risco definidos.

Aversão ao Risco (*Risk aversion*): É a atitude de preferir uma perda fixa em relação à "loteria" com a mesma perda esperada. Por exemplo: fazer seguro de um carro (evento certo, mesmo que incorra em custo) para evitar o risco de perdê-lo (evento incerto, pode-se incorres em prejuízo ou não). Aversão ao risco é evidenciada em eventos catastróficos. Enfatiza-se muito mais um acidente de avião, com várias fatalidade (catástrofe), que acidentes de carro, responsáveis por inúmeras fatalidade anualmente.

Barreiras (*Barriers*): Podem ser barreiras físicas, procedimentos, manuais, educação, capacitação, motivação ou qualquer medida que vise atuar na corrente causal evitando o incidente ou mitigando suas consequências.

Cenário (*Scenario*): Um modelo ou esboço de uma esperada ou suposta sequência de eventos.

Cenário causal (*Causal scenario*): O cenário causal identifica (1) as causas do incidente, (2) a sequência de eventos propagados pela sua ocorrência e (3) o efeito esperado para a combinação dos eventos.

Chance (*Chance*): Grau de confiança que um evento irá ocorrer – por exemplo, improvável / remota / ocasional / provável.

Comunicação do risco (*Risk communication*): "Troca ou compartilhamento de informações sobre o risco entre o tomador de decisões e outras partes envolvidas" (ABNT, 2005, p. 3).

Confiabilidade (*Reliability*): "capacidade [ou habilidade] de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo" (ABNT, 1994, p. 3).

Contingência (*Contingency*): O termo "contingência" é muito utilizado para designar todas as ações após o incidente – tanto a resposta emergencial quanto a "operação alternativa". Alguns altores, entretanto, utilizam o termo "contingência" em substituição à "operação alternativa". Assim, nesse trabalho, este termo será evitado, sempre que possível, para evitar problemas de interpretação. No entanto, quando utilizado, contemplará todas as ações após o incidente (i.e., gestão do incidente).

Controle ativo de risco (*Active controllability of risk*): São barreiras para prevenir o risco.

Controle do risco (*Risk control*): Comparação entre o risco analisado e os critérios de risco. Caso o risco não possa ser aceito, deve ser tratado – inclui também o planejamento dos riscos aceitos. Assim, o controle do risco contempla a avaliação do risco e o tratamento.

Controle passivo de risco (*Passive controllability of risk*): São barreiras para mitigar as consequências.

Cópias de segurança (*Backup*): Cópia de um item (arquivo, documento, etc.) guardada sob condições específicas, objetivando garantir a disponibilidade do item, caso a integridade do original venha a ser comprometida.

Crise (*Crisis*): Situação decorrente da ocorrência de um incidente que, se não for gerenciada apropriadamente, pode resultar em perdas significativas para a organização.

Evento gatilho (*Trigger event*): Evento que, quando associado a uma condição perigosa, pode – caso as barreiras sejam atravessadas – deflagrar um incidente.

Evitar o risco (*Risk avoidance*): Não se expor a um determinado risco – implica em eliminar o perigo.

Gerenciamento de continuidade do negócio (*Business continuity management*): Gerenciamento sistemático de atividades e recursos objetivando manter o risco de incidentes que resultem em interrupção do negócio em um patamar aceitável e, caso o incidente ocorra, objetivando mitigar suas consequências.

Gerenciamento de continuidade operacional: Gerenciamento sistemático de atividades e recursos objetivando manter o risco de incidentes que resultem em interrupção das funções críticas da unidade organizacional em um patamar aceitável e, caso o incidente ocorra, objetivando mitigar suas consequências.

Gerenciamento de segurança (*Safety management*): Gerenciamento sistemático de atividades e recursos objetivando manter o risco de incidentes que resultem em dano – material, ao homem ou ao ambiente – em um patamar aceitável e, caso o incidente ocorra, objetivando mitigar suas consequências.

Gerenciamento do incidente (*Incident management*): Gerenciamento sistemático de atividades e recursos objetivando mitigar as consequências de um incidente – mitigando os dano e / ou a condição de interrupção do negócio.

Homeostase do risco (*Risk homeostasis*): É a tendência das pessoas de manterem o nível do risco constante, mesmo que exista a viabilidade de uma alternativa mais segura. Por exemplo: quando se suaviza uma curva,

para prevenir acidentes, os motoristas tendem a correr mais, mantendo o mesmo nível de risco.

Identificação do risco (*Risk identification*): "Processo para localizar, listar e caracterizar elementos do risco" (ABNT, 2005, p. 4).

Incidente (*Incident*): Incidente é todo evento que tem consequências negativas. Assim, o termo incidente engloba o conceito de acidente – que é restrito a eventos que acarretem dano.

Mantenabilidade (*Maintainability*): "Capacidade de um item ser mantido ou recolocado em condições de executar suas funções requeridas, sob condições de uso especificadas, quando a manutenção é executada sob condições determinadas e mediante procedimentos e meios prescritos" (ABNT, 1994, p. 3).

Máximos de interrupção tolerável (*Maximum tolerable outage*): Tempo máximo que a organização admite ficar sem o processo.

Meta-incerteza (*Meta-uncertainty*): Meta-incerteza é a incerteza associada a incerteza. Por exemplo: na avaliação de um acidente, não se tem como ter certeza do valor da probabilidade de ocorrer o acidente, nem de determinar precisamente a gravidade do acidente. Assim, a meta-incerteza é uma forma de erro epstemológico, i.e., está associada a imprecizão do modelo.

Mitigação do risco (*Risk mitigation*): Limitação de quaisquer consequências negativas de um determinado incidente, atuando após sua ocorrência.

Modo de falha (*Failure mode*): É a maneira pela qual um sistema pode deixar de cumprir as funções pretendida.

Negócio (*Business*): Atividade fim da organização.

Objetivos para os pontos de recuperação (*Recovery point objective*): Ponto em que se aceita retornar o estado do processo – por exemplo, cópias de segurança diárias garantem que os dados não estarão mais que um dia desatualizados.

Organização (*Organization*): Companhias, firmas, instituições, órgãos de governo, fundações, e outras entidades – independente da natureza do empreendimento (como ou sem fins lucrativos).

Partes envolvidas (*Stakeholder*): "Um indivíduo, grupo ou organização que pode afetar, ser afetado, ou perceber-se afetado por um risco" (ABNT, 2005, p. 3).

Percepção do risco (*Risk perception*): Maneira que as pessoas percebem um risco, com base em um conjunto de valores ou interesses.

Perfil do risco (*Risk profile*): É o vetor (Li, Oi, Ui, CSi, POi), onde Oi é o resultado; Li é a chance do resultado ocorrer; Ui é utilidade; CSi é o cenário causal; e POi é a população afetada.

Perigo (*Hazard*): Qualquer ato (omissão ou ação), condição ou estado do sistema – ou uma combinação desses – com o potencial de resultar em um acidente, ou, de maneira mais abrangente, em um incidente (MOSLEH, et al., 2004).

Planejamento da continuidade do negócio (*Business continuity planning*): Parte do gerenciamento da continuidade do negócio que se refere ao planejamento dos riscos aceitos.

Prevenção do incidente (*Incident prevention*): Equivalente ao "monitoramento e controle". Nesse trabalho será evitada a designação "prevenção do incidente" para facilitar a distinção do contexto da "redução do risco".

Probabilidade (*Probability*): Número, entre 0 e 1, que representa a frequência relativa de ocorrência de um evento em inúmeras observações.

Recuperação do negócio (*Disaster recovery*): Processo de recuperação da organização para uma condição aceitável de operação, após o incidente ter ocorrido.

Redução do risco (*Risk reduction*): Trabalhar o risco a fim de diminuir a probabilidade de ocorrência do incidente e sua gravidade.

Retenção do risco (*Risk retention*): Aceitação do ônus da perda associada a um determinado risco – tanto dos riscos voluntariamente retidos (conviver com um risco acima do aceitável) quanto os involuntariamente (riscos não identificados). A retenção do risco exclui o tratamento envolvendo seguro ou qualquer outra forma de transferência do risco (ABNT, 2005).

Risco (*Risk*): Risco é a chance de ocorrência de um estado futuro "x", dada a ocorrência de um estado inicial – que pode ser expressa pela probabilidade condicional P (Estado futuro "x" | Estado inicial) –, sendo necessário para sua completa caracterização o delineamento dos dois estados, além dos cenários que possibilitem esta transição (que compõem o perfil do risco).

Severidade (*Severity*): Associação do impacto e da abrangência do incidente.

Significância do resultado risco (*Significance of outcome*): É o quanto se perdeu – ou ganhou – com a escolha de uma alternativa. É diretamente proporcional a perda e inversamente proporcional ao ganho.

Sistema de gestão de risco (*Risk management system*): "Conjunto de elementos de um sistema de gestão da organização relativo à gestão do risco" (ABNT, 2005).

Sistema técnico (*Technical system*): O sistema técnico pode, então, ser entendido como um conjunto de equipamentos e instalações que têm uma (ou mais) função para ser desempenhada e, a todo o momento, está interagindo como o ambiente, o homem e outros sistemas técnicos, influenciando e sendo influenciado.

Transferência do risco (*Risk transfer*): Está associada à contratação de seguro ou à "terceirização" do sistema técnico que está exposto ao risco, ou seja, transferir para outros a responsabilidade pelo incidente – o que, por si só, não exclui o risco do ciclo de vida. Note-se que a norma ABNT ISO/IEC Guia 73 exclui da transferência estratégias de reposicionamento de uma fonte de risco, como na terceirização (ABNT, 2005).

Tratamento do risco (*Risk treatment*): "[...] seleção e implementação de medidas para modificar um risco" (ABNT, 2005, p. 4). Estas medidas são no sentido de evitar, reduzir e/ou transferir o risco.

Unidade organizacional (*Organizational unit*): Parte da organização (normalmente departamentos, setores, etc) composta por sistemas técnicos e colaboradores a fim de desempenhar uma, ou mais, funções – interagindo com outras unidades organizacionais da organização em que está inserida e de outras, influenciando e sendo influenciado.

Utilidade do resultado risco (*Utility of outcome*): Inverso de significâncias.

Verossimilhança (*Likelihood*): É a probabilidade de se obter o dado observado. Para ilustrar essa idéia Souza, Tenorio e Nassar (2002) apresentam a seguinte relação: "é mais verossímil que um pássaro voe do que um peixe".