Luís Fernando Peres Calil

METODOLOGIA PARA GERENCIAMENTO DE RISCO: FOCO NA SEGURANÇA E NA CONTINUIDADE

Florianópolis

Março de 2009

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM
ENGENHARIA MECÂNICA

METODOLOGIA PARA GERENCIAMENTO DE RISCO: FOCO NA SEGURANÇA E NA CONTINUIDADE

Tese submetida à

UNIVERSIDADE FEDERAL DE SANTA CATARINA

para a obtenção do grau de

DOUTOR EM ENGENHARIA MECÂNICA

LUÍS FERNANDO PERES CALIL

Florianópolis, março de 2009.

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM
ENGENHARIA MECÂNICA

METODOLOGIA PARA GERENCIAMENTO DE RISCO: FOCO NA SEGURANÇA E NA CONTINUIDADE

LUÍS FERNANDO PERES CALIL

Esta tese foi julgada adequada para a obtenção do título de
DOUTOR EM ENGENHARIA

ESPECIALIDADE ENGENHARIA MECÂNICA
sendo aprovada em sua forma final.

Prof. Acires Dias, Dr. Eng. – Orientador

Prof. Nelson Back, Ph.D. – Co-orientador

Prof. Eduardo Alberto Fancello, D.Sc. –
Coordenador do Curso

BANCA EXAMINADORA

Prof. Acires Dias, Dr. Eng. – Presidente

Prof. Bernardo Luís Rodrigues de Andrade, Dr. Eng. – Relator

Prof. André Ogliari, Dr. Eng.

Prof. Franco Giuseppe Dedini, Dr.

Prof. Ubirajara Franco Moreno, Dr. Eng.

A minha família.

Agradecimentos

Aos Professores Acires Dias e Nelson Back pela orientação no desenvolvimento deste trabalho.

Ao colegas Eduardo Yuji Sakurada e Heitor Azuma Kagueiama pelas proveitosas discussões.

A Daniel Koudi Nakano, Glauco Vinicius Gil Peron e Gleber Estefani Diniz pela dedicação na implementação do *software* OpenFMECA.

A minha família e amigos pela compreensão e carinho.

Às empresas que permitiram a realização das visitas técnicas.

À Eletrosul e à Celesc pela oportunidade de realizar os estudos de caso apresentados nesta tese – destacadamente aos colaboradores Altair Coutinho de Azevedo Jr. (Eletrosul), Clóvis Nicoleit Carvalho (Eletrosul), Renato Borba Rolim (Celesc) e Ricardo Haus Guembarovski (Celesc).

Ao Conselho Nacional de Pesquisa e Desenvolvimento Científico (CNPq) pelo auxílio financeiro na forma de bolsa de doutorado.

Pode-se utilizar a ocasião da tese [...] para recuperar o sentido positivo e progressivo do estudo, entendido não como coleta de noções, mas como elaboração crítica de uma experiência, aquisição de uma capacidade (útil para o futuro) de identificar os problemas, encará-los com método e expô-los segundo certas técnicas de comunicação.

Umberto Eco (1977)

Resumo

O presente trabalho versa sobre gerenciamento de risco em organizações, focando não somente os possíveis danos ao homem, ao meio ambiente e ao sistema técnico resultante de um incidente, mas também os riscos de o negócio ser interrompido pela ocorrência de um evento indesejado. As questões relacionadas aos danos, principalmente as que se referem ao homem e ao meio ambiente, têm sido tratadas pelo gerenciamento de segurança, enquanto as relacionadas às interrupções, na operação do negócio, vêm sendo tratadas pelo gerenciamento de continuidade – que é um conceito ampliado do planejamento de contingências. Apesar de a gestão de segurança e a de continuidade terem objetivos distintos, ambas são gerenciamento de risco. Este trabalho apresenta uma metodologia de gerenciamento de risco que considera esses dois aspectos. Este tipo de enfoque tem benefícios mais evidentes em organizações cujo empreendimento é portador de riscos à segurança e à continuidade, como na área de petróleo; geração, transmissão e distribuição de energia; setor naval; petroquímico; entre outros. É dentro desta perspectiva que a metodologia foi desenvolvida e parcialmente aplicada em duas empresas do setor elétrico, uma distribuidora e outra transmissora, que lidam com grande potencial de danos e, também, têm grande potencial de prejuízos , no caso de uma interrupção do negócio – tanto para a organização (financeiros, à imagem da organização, etc.) quanto para a sociedade. Como resultados deste trabalhado, além da metodologia, destacam-se os seguintes pontos: foi definido um vocabulário único para suprir as necessidades do gerenciamento de continuidade e de segurança; foi elaborada uma estrutura de trabalho – baseada nas técnicas IDEF0 (*integration definition for function modeling*), FHA (*functional hazard assessment*), FMECA (*failure modes effects and criticality analysis*), CNEA (*Causal network event analysis*), redes bayesianas, FTA (*fault tree analysis*) e atualização bayesiana – que contribui para a unificação do gerenciamento de risco; e foi desenvolvida uma ferramenta computacional (*software*) a fim de auxiliar na aplicação da técnica FMECA. No que se refere aos estudos de caso nas duas empresas do setor elétrico, a aplicação da metodologia implicou recomendações e alterações nos procedimentos internos e na estrutura das empresas. No caso da distribuidora de energia, destaca-se a elaboração de uma instrução (norma interna) para atendimento emergencial diante de tempestades severas; a adequação das instalações, equipamentos e ferramental para possibilitar o atendimento nesta condição; a implementação de sistemas alternativos de comunicação; a implementação do esquema de prioridade para restabelecimento de carga (religamento); a aquisição de geradores portáteis; a disponibilização de uma verba anual para contingência; entre outras. Quanto à transmissora, destacam-se as recomendações referentes à política de atualização tecnológica; à política de atualização dos procedimentos; e à política de capacitação. Também foram elencadas algumas recomendações de responsabilidade da ANEEL (Agência Nacional de Energia Elétrica) referentes à política regulatória.

Palavras-chave: Gerenciamento de risco. Gerenciamento de segurança. Gerenciamento de continuidade. FMECA / CNEA. OpenFMECA.

Abstract

The present thesis treats of risk management in organizations, focusing not only on the possible risks to man, to the environment and to the technical system resulting from an incident, but on the business activities interruption due to the occurrence of an undesirable event, as well. The issues related to harm, especially those that refer to man and to environment, have been assessed by safety management, while those related to interruptions of the business operation belong to the field of continuity management – which is an amplified concept of contingency planning. Despite the distinct objectives of safety and continuity management, both of them are risk management. This thesis presents a methodology for risk management that considers both of these aspects. The benefits of this kind of approach are more evident in organizations which activity bears risks to both security and continuity, such as in the sectors of oil; power generation; transmission and distribution; marine operations; chemical process; among others. It is in this perspective that a methodology was developed and partially applied in two companies from the power sector, a electric power transmission company and a electric power distribution one, that deal with great potential of harm as well as great potential of loss, in case of business interruption – both for the organization (financial, public image, *et cetera*) and the society. As a result of this work, aside the developed methodology, the following stand out: a single vocabulary was established to supply the continuity and safety management needs; a framework has been developed – based on the techniques IDEF0 (integration definition for function modeling), FHA (functional hazard assessment), FMECA (failure modes effects and criticality analysis), CNEA (Causal network event analysis), bayesianas networks, FTA (fault tree analysis) and bayesian update – that contributes to the risk management unification; and a software has been developed to assist in the application of the FMECA technique. Referring to the case studies in the two companies from the power sector, the application of the methodology resulted in recommendations and changes in the companies' internal procedures and structure. In the case of the power distribution company, should be highlighted the elaboration of a set of instructions (internal standard) for emergency attendance in case of severe storms; the adequacy of installations, equipment and tools to allow the attendance in this circumstance; the implementation of alternate communication systems; the implementation of priority schemes for power reestablishment; the acquisition of portable generators; the availability of a annual budget to be used in contingencies; among other results. In the case of the power transmission company, should be highlighted the recommendations regarding the policy to upgrade technology; the policy to upgrade procedures; and the training policy. Also, a list of recommendations was also made, regarding some responsibilities attributed to the brazilian electricity regulatory agency ANEEL (Agência Nacional de Energia Elétrica) referring to the regulatory policy.

Keyword: Risk management. Safety management. Continuity management. FMECA / CNEA. OpenFMECA.

Lista de figuras

Lista de quadros

Lista de siglas

Siglas das organizações ou unidades organizacionais citadas no texto:

ABNT	Associação Brasileira de Normas Técnicas
ABS	American Bureau of Shipping
ANEEL	Agência Nacional de Energia Elétrica
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BCI	Business Continuity Institute
BSI	British Standards Institution
Celesc	Centrais Elétricas de Santa Catarina S.A.
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
COD	Centro de operação da distribuição da Celesc
DMS	Departamento de Manutenção do Sistema da Eletrosul
DNV	Det Norsk Veritas
DOD	Department of Defense / United States of America
DRI	Disaster Recovery Institute International
FAA	Federal Aviation Administration / United States of America
HSE	Health and Safety Executive
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission

IMO	International Maritime Organization
ISO	International Organization for Standardization
JAA	European Joint Aviation Authoritie
KTDMS	Knowledge Tree Document Management System
MIT	Massachusetts Institute of Technology / United States of America
NASA	National Aeronautics and Space Administration / United States of America
NeDIP	Núcleo de Desenvolvimento Integrado de Produtos
OGC	Office of Government Commerce / United Kingdom
PMI	Project Management Institute
SAE	Sociedade de Engenheiros da Mobilidade
UFSC	Universidade Federal de Santa Catarina
USNRC	United States Nuclear Regulatory Commission

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)
ATCC	*Air traffic control center* (Central de controle de tráfego aéreo)
BCM	*Business continuity management* (Gerenciamento da continuidade do negócio)
BIA	*Business impact analysis* (Análise do impacto no negócio)
BTA	*Bow-tie analysis* (Análise gravata borboleta)
CNEA	*Causal network event analysis* (Análise de eventos por rede causal)
CRM	*Continuous risk management* (Metodologia da NASA para "gerenciamento de risco contínuo")
DAG	*Directed acyclic graph* (Grafos acíclicos direcionados)

DMS *Document management system* (Sistema de gerenciamento de documentos)

EATMP *European air traffic management programme* (Programa europeu de gerenciamento de tráfego aéreo)

EMC Departamento de Engenharia Mecânica da UFSC

ESD *Event sequence diagram* (Diagrama sequencial de eventos)

ET&A *Educations, training and awarenes* (Educação, treinamento e conscientização)

ETA *Event tree analysis* (Análise por árvore de evento)

FAR *Federal aviation regulations*

FHA *Functional hazard assessment* (Análise / avaliação do perigo funcional)

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)

FSA *Formal safety assessment* (Análise / avaliação formal de segurança)

FTA *Fault tree analysis* (Análise por árvore de falha)

Gross CAF *Gross cost of averting a fatality* (Custo bruto para evitar uma fatalidade)

GWP *Global warming potential* (Potencial efeito-estufa)

HAZOP *Hazard and operability* (Perigos e operacionalidade)

IDEF0 *Integration definition for function modeling*

JAR *Joint airworthiness requirements*

MTO *Maximum tolerable outage* (Tempos máximos de interrupção tolerável)

NetCAF *Net cost of averting a fatality* (Custo líquido para evitar uma fatalidade)

NPR Número de prioridade de risco (*Risk priority number*)

PDP Processo de desenvolvimento de produto

P&D Pesquisa e desenvolvimento

PRA *Probabilistic risk assessment* (Avaliação probabilística de risco)

PSSA *Preliminary system safety assessment* (Análise / avaliação preliminar de segurança do sistema)

QFD *Quality function deployment* (Desdobramento da função qualidade)

RBD *Reliability block diagram* (Diagramas de blocos confiabilísticos)

RPO *Recovery point objective* (Objetivos para os pontos de recuperação)

RVSM *Reduced vertical separation minimum* (Redução da distância vertical mínima)

SADT *Structured analysis and design technique* (Técnica de delineamento e análise estruturada)

SAM *Safety assessment methodology* (Metodologia de análise / avaliação de segurança do EATMP)

SGR Sistema de gestão de risco (*Risk managment system*)

SSA *System safety assessment* (Análise / avaliação de segurança do sistema)

STAMP *Systems-theoretic accidents model and processes* (Modelo de acidente pela teoria dos sistemas)

TI Tecnologia de informação (*Information technology*)

WBS *work breakdown structure* (Desdobramento da estrutura de trabalho)

Lista de símbolos e operadores

$P(A)$	Probabilidade da variável aleatória "A"
$P(a)$	Probabilidade da variável aleatória "A" ser igual ao valor "a" – ou $P(A = a)$
$P(\overline{a})$	Probabilidade da variável aleatória "A" não ser igual ao valor "a", que é complementar a $P(a)$
$P(B\|A)$	Probabilidade condicional da variável aleatória "B" dada a ocorrência da variável aleatória "A"
i	Índices de iteração
∞	Infinito
$\int$	Integral
θ	Parâmetro desconhecido de uma distribuição
$f(\theta)$	Função densidade de probabilidade do parâmetro θ
$E(\theta)$	Valor esperado do parâmetro θ
$\hat{\theta}$	Estimador do parâmetro desconhecido

Sumário

1 Introdução

O presente trabalho versa sobre gerenciamento de risco focando não somente os possíveis danos ao homem, ao meio ambiente e ao sistema técnico resultantes de um incidente, mas também os riscos de o negócio ser interrompido pela ocorrência deste evento indesejado.

Kirchsteiger (1999) define sistemas como sendo um agrupamento de elementos que operam em conjunto, relacionando-se, a fim de atingir algum objetivo. O sistema técnico pode, então, ser entendido como um conjunto de equipamentos e instalações que tem uma (ou mais) função para ser desempenhada e, a todo momento, interage com o ambiente, o homem e outros sistemas técnicos, influenciando e sendo influenciado[1].

Unidade organizacional, por sua vez, pode ser entendida como uma 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 e com outras organizações, influenciando e sendo influenciada.

É interessante observar que as consequências de um incidente, no sistema técnico e na unidade organizacional, podem interferir tanto na manutenção de sua função, quanto na integridade de bens (incluindo o próprio sistema técnico), do homem e/ou do ambiente.

As questões relacionadas aos danos, principalmente as que se referem ao homem e ao meio ambiente, têm sido tratadas pelo gerenciamento de segurança, enquanto as relacionadas às interrupções, na operação do negócio, vêm sendo tratadas pelo gerenciamento da continuidade do negócio – que é um conceito ampliado do planejamento de contingências.

Observe-se que a diferença entre esses dois sistemas de gestão está no tipo da consequência do incidente. No entanto, ambos são sistemas de gerenciamento de risco, embora sejam tratados, em grande parte da literatura e na prática nas empresas, de forma separada.

Este trabalho objetiva elaborar uma metodologia que possibilite tratar esses dois aspectos em apenas um sistema de gerenciamento de risco. Esta é uma percepção que vem sendo dis-

[1] A nomenclatura adotada neste trabalho está sendo apresentada ao longo do texto e, também, no Glossário.

cutida a partir da análise dos grandes sistemas, em que o problema do risco da segurança não pode mais ser visto dissociado da continuidade operacional.

A metodologia desenvolvida tem seu foco no sistema técnico e na unidade organizacional em que está inserido; contudo, contextualiza o sistema de gestão de risco desde o planejamento estratégico da organização – pois o sistema técnico existe para desempenhar alguma função requerida pelo negócio.

1.1 Motivação para a seleção do tema

A literatura reconhece que desastres podem ser deflagrados por diferentes tipos de perigo, tais como: perigos naturais (furacões, enchentes, por exemplo), biológicos, civis e tecnológicos. Para tratar esses incidentes, Chapman (2005) conclui que, para se progredir, são necessários melhores modelos conceituais e estruturas que revelem a complexidade dos sistemas, tornando-os mais transparentes, e abordagens de gerenciamento de risco mais satisfatórias.

Catástrofes como a ocorrida na China em 13 de novembro de 2005 – onde cerca de 100 toneladas de benzeno foram jogadas no rio Songhua, depois de um incidente em uma indústria química, afetando milhares de habitantes da China e Rússia (BBC BRASIL, 2005) – demonstram a importância do desenvolvimento de pesquisas no contexto da segurança.

Infelizmente, também ocorreram incidentes no Brasil que poderiam ter suas consequências mitigadas, caso tivessem sido estabelecidas barreiras para isso. Em algumas situações, sequer foram dimensionados os impactos do incidente, como exposto no texto extraído do Jornal da Câmara:

> O médico do Sindicato dos Químicos de São Paulo, Roberto Ruiz, confirmou a ocorrência de alterações hepáticas e neurológicas e problemas de tireoide nos trabalhadores da fábrica de pesticidas da Shell de Paulínia (SP). Eles foram expostos à contaminação por produtos tóxicos que vazaram das instalações, em acidente ocorrido em 1995, que atingiu também moradores da área próxima à fábrica. (BRASIL, 2003, p. 4).

A necessidade de um programa de gerenciamento da continuidade do negócio (BCM – *business continuity management*) ficou evidenciada no episódio do "*bug* do milênio". Saldanha (2000) constata que parte do mérito de o termo "continuidade" ser atualmente adotado se deve ao fato de as organizações, diante do "*bug* do milênio", perceberem que a recuperação de desastre é apenas uma parte da continuidade.

Desastres, crises ou perturbações prolongadas podem resultar em perdas de ativos vitais para a organização, de fatia de mercado e / ou do momento oportuno do negócio (KARAKASIDIS,

1997). Mesmo uma interrupção ou um desastre menor podem causar danos irreversíveis à organização e a sua imagem pública (BOTHA; VON SOLMS, 2004).

Apesar de ser possível calcular as perdas financeiras de uma interrupção, geralmente o impacto mais significativo é quanto à reputação e à perda da confiança nos resultados pela má gestão do incidente. Por outro lado, um incidente bem gerenciado pode trazer uma melhora na reputação da organização e da equipe de gestores (BCI, 2005).

Alguns órgãos reguladores, como o UK Financial Services Authority, consideram que o BCM é um custo inerente aos negócios e precisa ser devidamente financiado (BCI, 2005).

A certificação BS 7799 (norma da BSI – British Standards Institution – equivalente a ISO 17799) em sistema de gestão da segurança da informação, que contempla a gestão da continuidade, é uma evidência de que o assunto está ganhando importância e ocupa posição similar aos sistemas de gestão da qualidade e de meio ambiente (ISO 9000 e 14000, respectivamente).

Mais recentemente, a BSI publicou a norma BS25999[2] – que substituiu a especificação PAS-56[3] (*publicly available specification*) –, que define um código de práticas (parte 1) e especificações (parte 2) para programas de BCM, não se restringindo a sistemas de informação (BCI, 2005), como a norma ABNT ISO/IEC 17799 – o que demonstra a preocupação dos gestores em atender a todas as áreas necessárias para manter o negócio.

Assim, pesquisas relacionadas ao risco são oportunas e fundamentais para atenuar as consequências de incidentes.

No Brasil, os estudos sobre segurança e, principalmente, sobre continuidade ainda são incipientes. A necessidade de desenvolver atividades nestas áreas fica evidente em estudos como o de "Análise dos procedimentos para operação e manutenção na geração de energia elétrica no Brasil", desenvolvido pela UFSC junto à ANEEL e publicado no seminário da ANEEL/2000 (DIAS et al., 2000). Neste trabalho foi constatado que os maiores percentuais de não conformidades, das 36 hidroelétricas e 5 termoelétricas analisadas, foram quanto aos planos de segurança das plantas (76%), planos de ações de emergência (49%) e planos contingenciais de cheias (38%).

Sistemas técnicos nos setores de geração e fornecimento de energia, aéreo, petróleo, gás, naval, siderurgia, química, etc., têm importância destacada para a sociedade, quer pelo potencial de gerar danos, quer pela dependência que a sociedade tem de seus produtos.

[2]Vide BSI (British Standards Institutio). **BS 25999-1:** Business continuity management – Code of practice. ISBN: 0 580 49601 5. BSI, 2006 e BSI (British Standards Institutio). **BS 25999-2:** Specification for business continuity management. ISBN: 978 0 580 59913 2 . BSI, 2007.

[3]Vide: BSI (British Standards Institutio). **PAS 56:** Guide to business continuity management. ISBN: 0 580 41370 5. BSI, 2003.

Note-se que, para um pequeno escritório de contabilidade, por exemplo – que normalmente não é portador de risco com potenciais significativos de dano ao homem ou ao ambiente –, a questão chave passa a ser a continuidade.

No entanto, organizações como uma usina nuclear para geração de energia elétrica primam fundamentalmente pela segurança. Um incidente nesse ambiente pode ter consequências catastróficas. Assim, as tomadas de decisões são sempre conservativas, no sentido da segurança – mesmo que isto implique interromper o negócio, obrigando o sistema elétrico a se balancear com a geração de outras usinas. Neste caso, a continuidade é levada a um segundo plano, embora prioritária para a sobrevivência da empresa.

Para Nicki Dennis, responsável pela área de desenvolvimento de mercado de risco da British Standards, eventos recentes têm enfatizado a necessidade de as companhias integrarem continuidade de negócio e o gerenciamento de risco às estratégias da corporação, a fim de minimizar as perdas ou danos às finanças, às pessoas ou à reputação da organização (WANE, 2005).

De fato, para empresas como uma distribuidora de energia elétrica, tanto os aspectos de segurança quanto os de continuidade são fundamentais. Se, por um lado, a segurança é prioritária, por outro, uma interrupção prolongada do fornecimento de energia pode implicar consequências severas para a sociedade.

Em uma pesquisa junto a duas empresas do setor de energia elétrica que têm programas de gerenciamento de risco (uma geradora, transmissora e distribuidora; e outra geradora), foi possível constatar que a preocupação em garantir a continuidade operacional, usualmente, parte da iniciativa pessoal ou de um pequeno grupo, que consegue demonstrar a necessidade de preparar a empresa para a ocorrência de eventos indesejados.

As duas empresas mantêm uma estrutura considerável objetivando garantir a continuidade operacional – vide Capítulo 3. No entanto, nenhuma das empresas estudadas dispunha de uma metodologia que desse suporte à implementação de seus respectivos programas.

De fato, o interesse da organização é continuar operando – manter a continuidade. No entanto, não pode, com isto, comprometer a segurança da comunidade, de seus colaboradores ou do meio ambiente.

Por outro lado, dependendo do tipo de negócio da organização, uma interrupção prolongada também pode implicar risco de dano para o homem e o ambiente.

A segurança é colocada pelos autores (BCI, 2005; HENG, 1996; SAVAGE, 2002; SALDANHA, 2000, e outros) como um requisito primordial no gerenciamento de continuidade, que destacam a necessidade de sempre considerar este requisito ao elaborar os planos. No entanto, não

apresentam uma metodologia que traga, de forma integrada, os conceitos de gerenciamento da continuidade e de gerenciamento da segurança.

Portanto, ficou evidente a necessidade de integrar a gestão destes dois atributos, o que contribuirá para uma abordagem de gerenciamento de risco mais satisfatória – que Chapman (2005) concluiu ser necessária.

Mas como integrar estes dois conceitos de gestão? De que forma os riscos dos sistemas devem ser abordados para considerar os aspectos relativos à segurança e à continuidade? Quais riscos devem ser reduzidos e quais aceitos? Como proceder na avaliação dos riscos para decidir quais devem ser priorizados na utilização dos recursos da organização? Como se planejar para a ocorrência dos incidentes identificados?

1.2 Objetivos do trabalho

Diante do que já foi exposto e a fim de responder às questões anteriores, apresenta-se este trabalho de doutorado, que tem os objetivos expostos a seguir.

1.2.1 Geral

O objetivo geral do trabalho é desenvolver uma metodologia para gerenciamento de risco com foco em unidades organizacionais e em sistemas técnicos durante o uso, integrando o gerenciamento da continuidade e o gerenciamento de segurança em um único sistema de gestão. Entende-se que este objetivo geral contempla sistemas já existentes e os que vão entrar em operação – neste caso, pode-se contribuir também com a etapa de projetação.

1.2.2 Específicos

Para se alcançar o objetivo geral deste trabalho, prevem-se os seguintes objetivos específicos:

1. compatibilizar conceitos e nomenclatura adotados no gerenciamento de segurança e de continuidade;
2. propor e sistematizar técnicas de suporte consolidadas que possam contribuir com a unificação do gerenciamento de risco;
3. desenvolver uma estrutura de trabalho que integre essas técnicas; e

4. desenvolver ferramenta computacional (*software*) para dar suporte à utilização da técnica FMECA.

1.3 Definição do escopo do trabalho

Diante da motivação e dos objetivos apresentados, constata-se que a metodologia desenvolvida mostra-se mais interessante para organizações relacionadas com algum empreendimento que seja portador de riscos à segurança e à continuidade – ficando fora do escopo, por exemplo, o estudo de desastres no âmbito da sociedade, que é foco do Sistema Nacional de Defesa Civil.

Assim, uma organização na qual os riscos significativos sejam relacionados apenas a sistemas de informações teria poucos benefícios em adotar a metodologia desenvolvida em substituição a uma de gerenciamento da continuidade. No entanto, a metodologia aborda a gestão de risco à continuidade de forma estruturada – em contraposição à maior parte das metodologias de gestão da continuidade levantadas durante este trabalho, que são mais holísticas –; desta forma, a metodologia apresentada neste trabalho pode trazer benefícios para a implementação do sistema de gestão.

Já para empresas como refinarias de petróleo; distribuidoras de energia elétrica; indústrias químicas; e outras organizações que lidam com grande potencial de dano, e também têm grandes prejuízos no caso de uma interrupção no negócio – tanto para a organização (financeiros, à imagem da organização, etc.) quanto para a sociedade –, os benefícios por adotar a metodologia desenvolvida são mais evidentes.

Portanto, a metodologia deve ser adaptada às peculiaridades de cada setor e organização, já que as necessidades e a disponibilidade de recursos são distintas, apesar de compartilharem das mesmas dificuldades na gestão dos riscos (BOTHA; VON SOLMS, 2004).

A metodologia desenvolvida está direcionada para a etapa de uso do sistema técnico e da unidade organizacional em que ele está inserido; contudo, leva em consideração a organização de maneira geral. Também não é razoável pensar na etapa do uso sem ter como referência o ciclo de vida do sistema técnico – particularmente, a fase de processo de projeto. É interessante notar que muitos sistemas técnicos, hoje em funcionamento, foram projetados há algum tempo, em muitos casos sem o suporte de uma metodologia que tratasse de todas as fases do ciclo de vida. Assim, neste contexto, o trabalho foi desenvolvido para ser aplicado à etapa de uso, mas a sistematização da informação deve alimentar o projeto. Isto porque, na gestão de risco, é requerido tratar atributos de confiabilidade, mantenabilidade e segurança, sendo que a melhoria destes atributos só é possível pela ação de projeto. A Figura 1.1 ilustra este ciclo de vida – sem

apresentar as realimentações (da etapa de uso para o projeto, por exemplo).

Figura 1.1: Ciclo de vida de um produto (um sistema técnico, por exemplo), desconsiderando as realimentações

Note-se que, ao tratar o risco, pode-se evidenciar a necessidade de fazer alterações no sistema estudado, o que caracteriza um reprojeto dele.

É importante salientar que este trabalho procura contribuir para uma abordagem de gerenciamento de risco mais satisfatória, mas não tem pretensão de desenvolver modelos para descrever a complexidade dos sistemas ou que possibilitem o completo levantamento dos perigos a que a organização pode estar exposta.

Por fim, esclarece-se que a elaboração desta metodologia é oportuna e está aderente a estudos que vêm sendo veiculados no campo científico e na elaboração de normas técnicas. Versa, portanto, sobre um tema que está sendo estruturado há muito pouco tempo e deve assim contribuir com algum conhecimento, sem ter a pretensão de esgotar o assunto.

1.4 Diretrizes utilizadas para o desenvolvimento da metodologia

A fim de orientar o desenvolvimento deste trabalho de doutorado, foram adotadas – de maneira geral – algumas diretrizes, a saber:

- Para fazer a fundamentação da metodologia, optou-se por seguir duas linhas: (1) pesquisa bibliográfica sobre gestão da seguraça, gestão da continuidade e gestão de rico de maneira geral; e (2) pesquisa de campo, estudando sistemas de gestão de risco já implementados e participando da implementação de outros.
- Uma vez que um sistema de gestão de risco pode ser entendido como um produto que se deseja desenvolver, optou-se por organizar a metodologia de gestão de risco com base na estrutura do PDP (processo de desenvolvimento de produto), destacadamente o modelo PRODIP – vide (BACK et al., 2008).
- Para dar suporte à metodologia de gestão de risco, optou-se por utilizar técnicas e modelos

consagrados, a exemplo do modelo da corrente causal de Mosleh & Dias[4] e das técnicas FMECA, FTA, entre outras. Sendo que, na necessidade de se desenvolver alguma técnica, esta deveria ser baseada em outras já consagradas.

- Para compatibilizar os conceitos e nomenclatura adotados no gerenciamento de segurança e de continuidade, optou-se por seguir, sempre que pertinente, os termos e definições apresentados na norma ABNT ISO/IEC Guia 73[5].
- Para a concepção da ferramenta computacional (*software*), optou-se pelo modelo de desenvolvimento incremental; pelo paradigma de programação orientado a objetos; e pela estruturação em camadas, no caso: armazenamento (base de dados), aplicação e interface.

1.5 Estrutura deste documento

Este documento está estruturado em sete capítulos, conforme apresentados a seguir.

O Capítulo 2 aborda o gerenciamento de risco apresentando conceitos e nomenclatura.

No Capítulo 3, apresenta-se como é abordada a gestão de risco em algumas áreas de aplicação, e, no Capítulo 4, apresentam-se algumas técnicas de suporte utilizadas no gerenciamento de risco.

No Capítulo 5, apresenta-se a metodologia desenvolvida, e, no Capítulo 6, está apresentada sua aplicação.

Por fim, no Capítulo 7, apresentam-se as conclusões e recomendações para trabalhos futuros.

[4] Vide: Mosleh & Dias (2004) e Mosleh et al. (2004).
[5] Vide: ABNT (2005).

2 *Conceitos e nomenclatura relativos à gestão de risco*

Neste capítulo, estão apresentados alguns conceitos e nomenclatura referentes à gestão de risco. Na próxima seção, fazem-se considerações sobre a terminologia adotada por alguns autores e, também, propõe-se a definição de termos, a fim de atender a um dos objetivos deste trabalho, que é compatibilizar conceitos e nomenclatura adotados no gerenciamento de segurança e de continuidade. Posteriormente, na Seção 2.2, apresentam-se os conceitos e nomenclatura referentes à modelagem de um incidente e, na Seção 2.3, referentes ao gerenciamento de segurança, de continuidade e de disponibilidade. Por fim, na Seção 2.4, apresentam-se as considerações finais sobre este capítulo.

2.1 Nomenclatura adotada neste trabalho

De acordo com Bernstein (1997), o termo "risco" é uma derivação do italiano antigo "*risicare*" (que, por sua vez, deriva do baixo-latim *risicu, riscu*), que significa ousar.

É interessante destacar que o risco é inerente a qualquer empreendimento, e nossa cultura aceita o risco como o motor propulsor do progresso (MORAND DEVILLER, 2005).

Desta forma, companhias, firmas, instituições, órgãos de governo, fundações e outras entidades – que serão designadas, neste trabalho, por "organizações" –, independente da natureza do empreendimento (com ou sem fins lucrativos), estão inevitavelmente sujeitas a algum tipo de risco, que deve ser gerenciado.

O gerenciamento de risco, para Ayyub (2005), consiste na análise e no controle do risco. Análise é definida como um processo técnico e científico pelo qual os riscos de um sistema, em uma dada situação, são modelados, quantificados e ponderados. Quanto ao controle, este inclui a prevenção do incidente e a mitigação de suas consequências.

A norma ABNT ISO/IEC Guia 73 (ABNT, 2005), por sua vez, salienta que a gestão do risco

engloba a análise / avaliação, o tratamento, a aceitação e a comunicação de riscos – sendo esta última a troca ou compartilhamento das informações sobre o risco com as partes envolvidas (*stakeholders*).

Note-se que o tratamento e a aceitação de riscos vão no sentido de controlá-los, como proposto por Ayyub (2005).

A análise / avaliação envolve a identificação dos riscos a que se está exposto, e a avaliação destes baseada em critérios pré-definidos. Desta forma, podem-se assumir, para cada risco, três estratégias de tratamento[1] – 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 de o perigo vir a se tornar um incidente. Ademais, todo sistema técnico é portador de perigo (DIAS et al., 2005), 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[2]. Esta estratégia não é objeto de estudo deste trabalho, apesar de ser considerada na metodologia desenvolvida.

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.

A norma ABNT ISO/IEC Guia 73 (ABNT, 2005) inclui ainda uma quarta estratégia para o tratamento, que é a retenção. O conceito de retenção está associado à alternativa de se aceitar um risco mesmo quando ele está acima dos limites estabelecidos – chamados de relutantemente aceitos por Kumamoto & Henley (1996). Esta estratégia pode não parecer prudente, mas, em alguns casos, pode ser a melhor opção. Esta decisão passa, então, por uma análise de custo / risco / benefício. É interessante salientar que o processo de retenção do risco também inclui os

[1] Não há um consenso quanto aos termos para designar as estratégias. O PMBOK (PMI, 2004), por exemplo, adota para os "riscos negativos": prevenir; transferir; mitigar; e não distingue reter de aceitar. Assim, neste trabalho, será adotada a nomenclatura apresentada na ABNT, por considerá-la mais adequada.

[2] A norma ABNT ISO/IEC Guia 73 (ABNT, 2005) não inclui a tercerização como uma forma de transferência.

riscos que a organização não sabe que existem – os chamados involuntariamente retidos.

Observe-se que, ao reter um risco, não se está efetivamente fazendo o tratamento dele. Assim, neste trabalho, o processo de retenção está sendo considerado como um tipo de aceitação.

Tanto para o caso de se aceitar o risco ou retê-lo, ainda é possível planejar para a ocorrência do incidente, a fim de mitigar suas consequências – o que é designado aceitação ativa. Esta prática é fomentada por muitas seguradoras e tem resultado em reduções nos valores das apólices (SALDANHA, 2000).

Desta 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.

De fato, o conceito de risco está associado à incerteza de um resultado. No entanto, não existe um consenso quanto à definição de risco e aos elementos que o compõem. É possível dar diferentes abordagens ao risco dependendo do enfoque que se quer dar, como ilustrado no Quadro 2.1 – que apresenta um comparativo entre as definições de risco elaboradas por diversos autores.

Note-se que todas as definições consideram a incerteza do resultado como um componente do risco.

Bühlmann (1970) aborda o risco como a relação entre o que se pode ganhar com o que se pode perder, pois a preocupação é quanto à possibilidade de ocorrer o sinistro.

No contexto da segurança, Kumamoto & Henley (1996) também consideram o possível benefício, no item significância (que é o oposto da utilidade) do perfil do risco.

É interessante destacar, na definição apresentada na norma STD-8719.13A (NASA, 1997), a inclusão da metaincerteza, ou incerteza epistemológica – que também é citada por alguns autores, entre eles Kumamoto & Henley (1996), mesmo não estando inserida na definição.

Quadro 2.1: Comparativo entre algumas definições de risco e elementos que o compõem

Fontes	**Definição de risco proposta pelos autores**	**Elementos que se podem destacar**
Holton (2004)	Definição geral: É a exposição a algo, o qual é incerto.	– Algo; – exposição; e – incerteza.
Saldanha (2000)	Definição geral: É a probabilidade de se concretizar um evento.	– Evento; e – incerteza.

(continua na próxima página)

Quadro 2.1: Comparativo entre algumas definições de risco e elementos que o compõem
(continuação)

Fontes	**Definição de risco proposta pelos autores**	**Elementos que se podem destacar**
ABNT (2005) – ISO/IEC Guia 73	Definição geral:Combinação da probabilidade de um evento e de suas consequências.	– Evento – consequências; – incerteza.
Kumamoto & Henley (1996)	Definição geral: É a combinação de cinco fatores: o resultado; a chance; a significância (ou a utilidade, que é seu oposto); o cenário causal (como aconteceu); e a população afetada.	– Resultado; – significância; – cenário causal; – população; – incerteza.
PMI (2000) – PMBOK	Para projetos: É um evento ou uma condição incerta, que, se ocorrer, tem efeito positivo ou negativo nos objetivos do projeto.	– Evento (ou condição); – consequências; e – incerteza.
NASA (2005) – NPR 7120.5	Para projetos: É a combinação de 1) a probabilidade de um projeto (ou programa) ser atingido por um evento indesejado, como sobrecustos, deslizes no cronograma, etc; 2) as consequências, impacto, ou severidade do evento indesejado, quando ele ocorrer.	– Evento (ou condição); – consequências; e – incerteza.
NASA (1997) – STD-8719.13A.	Para segurança: É a exposição à probabilidade de ferimento ou perdas. É uma função da possível frequência do evento indesejado ocorrer; da potencial severidade das consequências; e da incerteza associada com a frequência e a severidade.	– Evento; – consequências; – incerteza; – metaincerteza (incerteza na avaliação da incerteza).
Brasil (2004) – NR 10	Para segurança humana: É "a capacidade de uma grandeza com potencial para causar lesões ou danos à saúde das pessoas" Brasil (2004, p. 15).	– Capacidade; – consequências; – incerteza.
Bühlmann (1970)	Para questões de seguro: É uma relação entre a probabilidade de um determinado prêmio, num intervalo de tempo, e a soma da quantia que pode ser reivindicada, isto é: o que se poderá receber (num período de tempo) relativo ao que se poderá ter que pagar.	Duas variáveis estocásticas: – P_t (prêmio, num intervalo de tempo); e – S_t (soma da quantia reivindicada).
DRJ / DRI (2005) – Glossário	Para recuperação de desastres: Potencial para exposição a perdas. O potencial é usualmente medido pela probabilidade – em anos.	– Consequências; – exposição; e – incerteza.

(continua na próxima página)

Quadro 2.1: Comparativo entre algumas definições de risco e elementos que o compõem
(continuação)

Fontes	**Definição de risco proposta pelos autores**	**Elementos que se podem destacar**
Castro et al. (2005) – Manual de defesa Civil do Ministério da Integração Nacional	Para recuperação de desastres: É a "medida de danos e prejuízos potenciais, expressa em termos de: • probabilidade estatística de ocorrência; • intensidade ou grandeza das consequências possíveis. Relação existente entre: • a probabilidade estatística de que uma ameaça de evento adverso ou de acidente determinado se concretize com uma magnitude definida; • o grau de vulnerabilidade do sistema receptor e seus efeitos."	– Evento (ameaça); – vulnerabilidade; – consequências; – incerteza.

Kumamoto & Henley (1996) incluem, ainda, a população afetada e o cenário causal como componentes do risco, que indicam, respectivamente: a proporção entre as consequências e a população afetada; e os caminhos possíveis para que as consequências ocorram, sendo este último especialmente interessante para a avaliação de medidas para prevenir o incidente ou para mitigar suas consequências.

Observe-se que, em todas as definições, o risco representa a incerteza da alteração de um estado inicial (que pode ser o estado atual ou um hipotético) para um determinado estado futuro (a ocorrência de um incidente, por exemplo).

Assim, neste trabalho, propõe-se uma definição para o termo "risco" no Quadro 2.2, ilustrado na Figura 2.1.

Quadro 2.2: Definição de risco

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).

Neste contexto, elementos como "população afetada" e "utilidade" — utilizados por Kumamoto & Henley (1996) — estão associados à definição de estado futuro. Já a incerteza epis-

temológica está na incapacidade de caracterizar, com exatidão, todos os cenários e os estados inicial e futuro.

Assim, pode-se entender confiabilidade como sendo a chance de um item não falhar até um determinado estado futuro, dada a ocorrência do estado presente – isto é: o risco de se manter em operação (que é um resultado positivo).

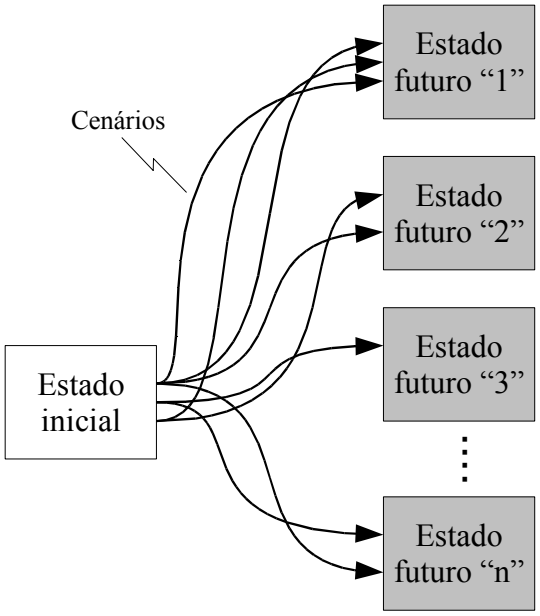


Figura 2.1: Representação da definição de risco

Note-se que o termo confiabilidade é definido pela norma NBR 5462 (ABNT, 1994, p. 3) como sendo a “capacidade [ou habilidade] de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo”. No entanto, inúmeros autores incluem na definição de confiabilidade a probabilidade de ocorrência da falha. Dias (1996) confronta diversas definições de confiabilidade e conclui que o conceito do termo se fundamenta em quatro pontos fundamentais: (1) probabilidade; (2) comportamento adequado; (3) período de uso (ou de vida); e (4) condições de uso. O que pode ser entendido como sendo risco, pois se trata da probabilidade (ou chance) de ocorrência de um estado futuro, que neste caso é o item operar de maneira adequada em um determinado período de uso. Adicionalmente, também se estipula a condição de uso, que faz parte do cenário causal.

De forma análoga, pode-se entender a segurança como sendo a chance de ocorrer um estado futuro caracterizado por não existir dano ao homem ou ao meio.

A exemplo da definição de confiabilidade e segurança apresentada acima, alguns autores – PMI (2000), NASA (2004b), Bühlmann (1970), entre outros – consideram como risco a possi-

bilidade de o estado futuro ser positivo, como, por exemplo, em um investimento na bolsa de valores, o que também é aceito coloquialmente.

No entanto, no que se refere às analises de risco relativas à segurança e à continuidade, usualmente se consideram apenas os resultados negativos. Mais especificamente à chance de uma condição perigosa (estado inicial) vir a se tornar um determinado incidente ou vir a resultar em determinadas consequências (estado futuro) –; neste contexto, cada cenário é uma possível corrente causal.

A norma ISO/IEC Guide 51 "*Safety aspects – Guidelines for their inclusion in standards*" define incidente como um evento que, na sua ocorrência, resulta em dano à saúde de pessoas, à propriedade ou ao meio ambiente (ABNT, 2005). Para a gestão da continuidade, por sua vez, um incidente é qualquer evento que possa resultar em uma interrupção do negócio. Alguns autores, como o DRI (Disaster Recovery Institute International), também consideram ainda a possibilidade de o incidente resultar em impacto no lucro, na reputação e na habilidade de operar (DRJ / DRI, 2005).

Também é comum, na literatura, o uso do termo acidente, que se refere aos eventos que resultam em dano ao homem ou ao ambiente.

Note-se que as definições de incidente apresentadas englobam este conceito de acidente[3]. Assim, neste trabalho, propõe-se, no Quadro 2.3, a seguinte definição para o termo "incidente", ilustrada na Figura 2.2.

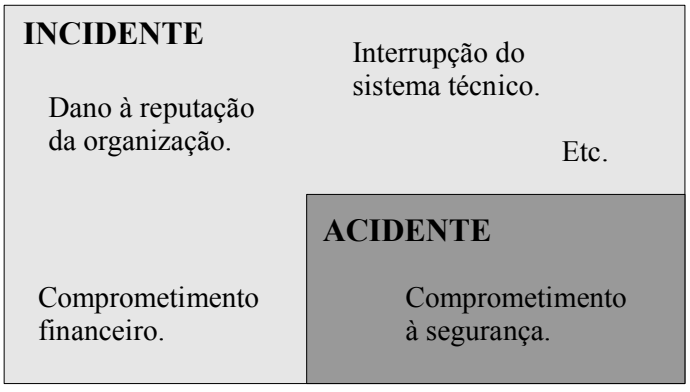


Figura 2.2: Representação da definição de incidente

Independentemente do tipo de consequência, o incidente não poderia ocorrer se algum perigo não estivesse presente. Perigo, por sua vez, é definido pela norma ABNT ISO/IEC Guia 73 (ABNT, 2005) como a fonte potencial de dano. Mosleh et al. (2004) ampliam este conceito

[3] Alguns autores consideram incidente como sendo um quase-acidente.

Quadro 2.3: Definição de incidente

Incidente é todo evento que tem consequências negativas. Desta forma, o termo incidente engloba o conceito de acidente – que é restrito a eventos que acarretem dano.

e definem perigo 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.

Neste 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 é na incerteza desta alteração de estado que está o risco.

Laplace (1995) ilustra esta 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 do universo até as menores partículas. Assim "Para esta inteligência nada seria incerto, e o futuro, assim como o passado, estaria presente diante dos seus olhos." (LAPLACE, 1995, p. 2, tradução nossa). 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."(LAPLACE, 1995, p. 2, tradução nossa). Desta forma, para o Demônio de Laplace não existiria risco, pois o futuro não seria incerto.

No entanto, o homem não é capaz de entender a realidade em sua totalidade. Assim faz-se uso de modelos para representá-la da melhor maneira possível – conforme expresso por Capra (1988, p. 30):

> Ao pensarmos acerca do mundo, deparamos com o mesmo tipo de problema que o cartógrafo quando tenta cobrir a face recurvada da Terra com uma sequência de mapas planos. Só podemos esperar uma representação aproximada da realidade a partir de um procedimento dessa espécie, o que torna todo o conhecimento racional limitado.

No que se refere aos incidentes, existem inúmeros modelos que procuram representar sua ocorrência. Na próxima seção, serão discutidos alguns deles.

2.2 Modelagem de um incidente

Kumamoto & Henley (1996) alertam que, à primeira vista, as falhas de equipamentos são as causas dominantes dos incidentes – como o de Chernobyl, Challenger ou Three Mile Island. No entanto, uma análise mais cuidadosa poderá revelar que outros fatores contribuíram (ou até determinaram) para sua ocorrência, tais como: erro na operação, no projeto ou na manufatura; problemas de comunicação; falta de clareza na definição de responsabilidades; entre outros.

De fato, a visão de que todo incidente tem um culpado ainda é bastante comum. Esta visão possivelmente tem sua origem no sistema legal, no qual o acusador procura punir o suposto culpado (PARADIES; UNGER, 2000). Hammer & Price (2001), por exemplo, acreditam que a primeira regra escrita para penalidades de um incidente seja o código de Hamurábi, aproximadamente 1750 a.C.: "Se um construtor fizer uma casa para um homem e não contruí-la com firmeza e a casa colapsar e causar a morte de seu proprietário, o construtor deve ser levado a morte." (HAMMER; PRICE, 2001, p. 15, tradução nossa).

Atualmente, na maioria dos países, as penalidades são menos severas e não seguem mais a "lei de talião". Ademais, 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. Esta abordagem, a qual procura explicar um incidente por uma única causa, é chamada, no âmbito da segurança no trabalho, de teoria monocausal (CARPES JÚNIOR, 2004). Em contrapartida, as teorias que consideram mais de uma causa são denominadas multicausais.

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 (LÉGER et al., 2006). Reason (1997) destaca, ainda, que os erros dos operadores podem ter como causa raiz um problema organizacional, por exemplo, no caso de ele não ter sido adequadamente capacitado.

De acordo com Lima (1985), as teorias multicausais – a exemplo das teorias de Heinrich (1959) e da Tríade Ecológica (LEAVELL; CLARK, 1976) – se consolidaram na década de 60, quando as monocausais se mostraram custosas e insuficientes para explicar a ocorrência de acidentes de trabalho, de forma que se pudessem identificar ações para evitar ou reduzir a chance de aquele incidente ocorrer novamente – ou mitigar suas consequências.

Para Alonço (2004), as teorias multicausais, de forma geral, consideram a coexistência de

várias causas, diretas ou indiretas, formando uma cadeia de eventos que resultam no incidente. Essas causas foram sistematizadas em fatores relativos ao homem, ao ambiente e à máquina (ou ao sistema técnico, em uma visão mais abrangente) – além da interação entre estes fatores, conforme ilustrado na Figura 2.3.

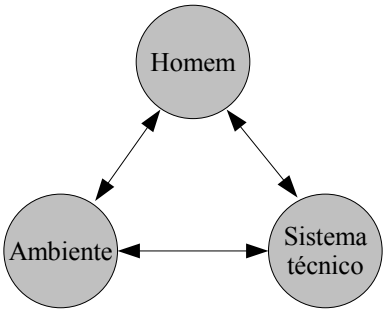


Figura 2.3: Relação entre os envolvidos no sistema da teoria multicausal da ocorrência de incidentes

Fonte: Adaptado de Alonço (2004)

É interessante observar que os sistemas técnicos também consideram *softwares*, além de componentes físicos. Assim, a segurança nesses sistemas está intimamente ligada ao estudo de falhas de *software*, de componentes físicos, do homem e das perturbações do ambiente.

Existe uma série de outros modelos que procuram representar a ocorrência de um incidente. Leveson (1995) os classifica em 4 tipos: (1) modelos básicos de energia, que considera o incidente como resultado de uma liberação de energia indesejada ou fora de controle; (2) modelos de evento único ou dominó, a exemplo do modelo proposto por Heinrich, em 1931, que considera o incidente causado por questões relativas ao ambiente social ou à descendência, que levam a uma falha humana, que é a razão aproximada de uma condição ou ato inseguro, que resulta em um acidente que leva a lesões; (3) modelos de cadeias de eventos, que consideram o incidente resultado de uma série de eventos, normalmente encadeados cronologicamente, a exemplo dos propostos por Mosleh et al. (2004); (4) modelos baseados na teoria dos sistemas, que considera um incidente resultado da interação entre homem, ambiente e sistema técnico que viole as restrições do sistema, a exemplo dos propostos por Leveson et al. (2003).

O modelo proposto por Leveson et al. (2003), denominado STAMP (Systems-Theoretic Accidents Model and Processes), foi apresentado no simpósio internacional do Massachusetts Institute of Technology (MIT / USA), em maio de 2002. Ele se fundamenta na teoria dos sistemas – dos anos 30 e 40 –, que foi uma resposta às limitações das técnicas de análise clássica que não atendiam à crescente complexidade dos sistemas que estavam sendo construídos.

Para o STAMP, os incidentes não são causados por falha de um componente – evento

inicializador (causa raiz) –, mas por inadequados controles ou restrições relativas à segurança impostas no projeto, no desenvolvimento e no uso do sistema, que não estavam aptos a controlar os distúrbios existentes (LEVESON et al., 2003).

Desta forma, incidentes são vistos pela teoria dos sistemas como resultado de processos defeituosos envolvendo interação entre os componentes dos sistemas, incluindo: pessoas, estrutura organizacional e social, atividades de engenharia e componentes físicos.

Neste trabalho, será adotado o modelo proposto por Mosleh et al. (2004) – apresentado na Figura 2.4 –, no qual o incidente é resultado de uma condição perigosa aliada a um evento deflagrador, atravessando as barreiras.

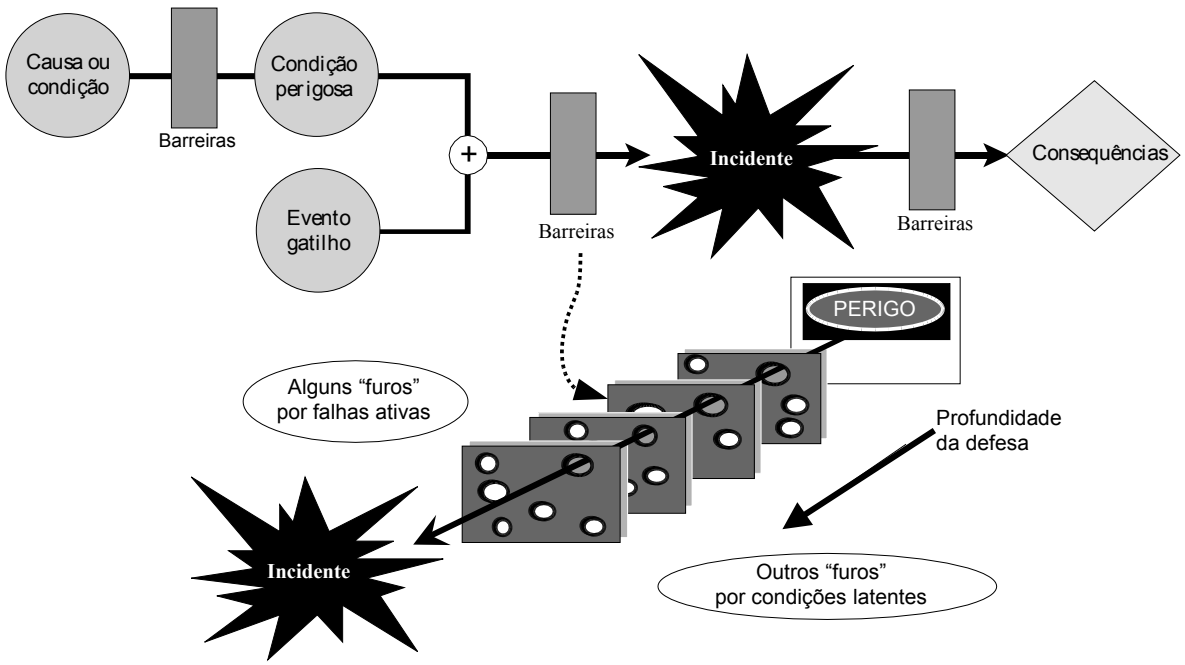


Figura 2.4: Desencadeamento de um incidente e sua trajetória através de barreiras
Fonte: Adaptado de Mosleh et al. (2004) e Reason (1997)

A fim de diminuir a probabilidade de ocorrência do incidente ou, ainda, mitigar suas consequências, implementam-se barreiras ao longo da corrente causal. Estas podem ser barreiras físicas, 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, tornando-se uma condição perigosa. Uma parede-corta-fogo, por sua vez, visa não permitir 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.

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".

Outro ponto a se destacar é o tipo de consequência que o incidente provoca. Neste sentido, o Quadro 2.4 apresenta uma proposta de classificação do incidente, ilustrada na Figura 2.5, que é uma adaptação da classificação de falhas apresentada por Smith (2001a).

Quadro 2.4: Classificação de um incidente

Um incidente pode ser classificado como A, B, C, D/A, D/B ou D/C, isto é:
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 com comprometimento à segurança;
D/B – incidente desconhecido com comprometimento à continuidade;
D/C – incidente desconhecido com comprometimento à situação econômica e financeira.

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 desconhecidos (D), e portanto involuntariamente retidos, podem ser gerenciados de acordo com o plano de gerenciamento de crises, conforme proposto em BCI (2005). 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.

Note-se que esta classificação não contempla os incidentes com comprometimento à imagem da empresa, pois ela 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. Para o BCI (2005), um incidente bem gerenciado pode até trazer uma melhora na reputação da organização e da equipe de gestores.

Observe-se que esta taxonomia, apresentada na Figura 2.5, está em consonância com a proposta pela NASA, que apresenta 5 tipos de riscos e suas respectivas consequências (STAMATELATOS, 2000):

1. relativo à segurança (humana) – consequência: morte, doença, mutilação, etc.;
2. relativo ao meio ambiente – consequência: contaminação, perda de uso, etc.;
3. relativo à programação – consequência: prejuízo à missão, programação, etc.;
4. relativo ao custo – consequência: perdas financeiras;
5. outros ou combinação dos tipos anteriores.

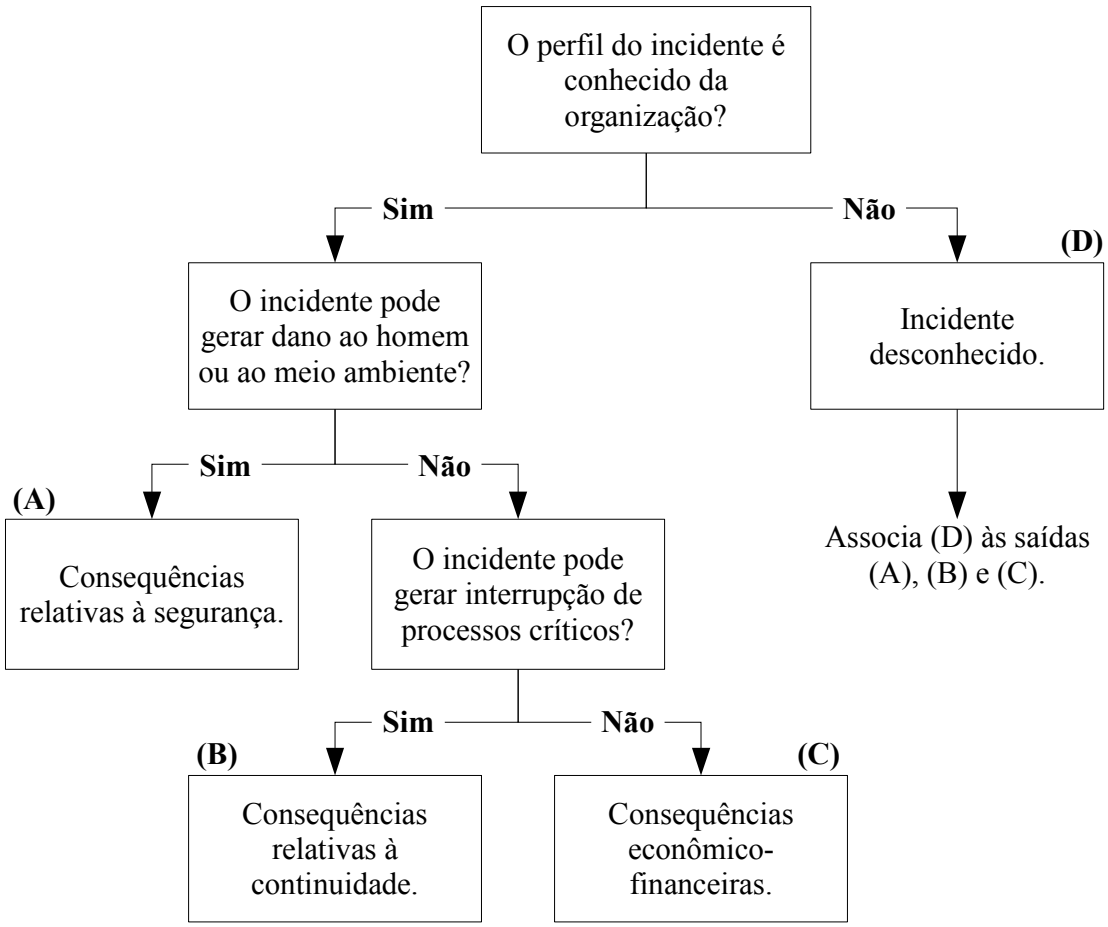


Figura 2.5: Classificação de incidentes em uma unidade organizacional
Fonte: adaptado de Smith (2001a)

É interessante, ainda, distinguir o conceito de segurança relativa a danos (expressa em inglês pelo termo *safety*) do conceito de segurança relativa a patrimônio e privacidade (expressa em inglês pelo termo *security*). Leveson (1995) destaca que o último foca principalmente em ações maliciosas – tais como: invasões, vírus de computador, etc. – e enfatiza que os dois conceitos se misturam quando o resultado destas ações maliciosas são considerados danos. No entanto, normalmente eles são tratados separadamente. A norma ISO/IEC Guide 51 "*Safety aspects – Guidelines for their inclusion in standards*", por exemplo, trata segurança relativa a dano, enquanto a série ISO/IEC 27000 "*Information technology – Security techniques*" se atém à

segurança da informação (que está inserida na gestão da continuidade).

Assim, neste trabalho, 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 – que será apresentada na próxima seção.

2.3 Gerenciamento de segurança e de continuidade

O gerenciamento de segurança desenvolveu-se nos mais diversos setores, destacando o aeronáutico, o químico e o de energia nuclear – cujos sistemas técnicos são portadores de perigos com grande potencial de impacto.

Pode-se definir gestão de segurança como o gerenciamento sistemático de todas as atividades para assegurar um nível aceitável de segurança (GEEST et al., 2003), isto é, manter o risco de dano material, ao ambiente e ao homem em um nível que se considere aceitável.

Para o Departamento de Defesa Civil, a análise de segurança de um sistema tem por finalidade aumentar a confiabilidade e o nível de segurança de um sistema (BRASIL, 1998b).

De fato, sistemas de segurança surgiram principalmente como resultado dos estudos de falha (SMITH, 2001b), que também é objeto de estudo da 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, está indo de encontro à confiabilidade do equipamento.

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 que não ocorram danos materiais, ao ambiente e / ou ao homem, ou que ocorram em menores proporções, dentro do que se considera aceitável.

O gerenciamento da continuidade do negócio, por sua vez, objetiva, de acordo com a norma ABNT ISO/IEC 17799[4] (ABNT, 2001, p. 45): "Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falha ou desastres significativos", combinando ações de prevenção e recuperação.

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

[4] A ABNT ISO/IEC 17799 foi renomeada para ABNT ISO/IEC 27002, mas manteve o conteúdo idêntico.

utilizado para designar a atividade fim da organização.

O BCI (2005) define, então, gerenciamento da continuidade do negócio (*business continuity management* – BCM) como um processo de gerenciamento holístico que identifica potenciais impactos e ameaças a uma organização e fornece a ela uma estrutura de trabalho que a possibilite se adaptar às situações de crise e uma habilidade de ser capaz de responder efetivamente à crise, a fim de salvaguardar os interesses das partes envolvidas, a reputação, a marca e as atividades que agregam valor.

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 (SALDANHA, 2000), enquanto a continuidade trabalha para não permitir que haja interrupções e, caso elas ocorram, procura garantir que elas não atinjam um nível que se considera inaceitável.

De acordo com Saldanha (2000), nos EUA, a denominação mais usada até 1997 era "recuperação do negócio", quando o Disaster Recovery Institute International (DRI) optou pelo termo "continuidade", que atualmente é o termo mais adotado no âmbito de negócios, especialmente quando se refere à tecnologia de informação – TI.

Glenn (2005) considera que a continuidade do negócio engloba a continuidade dos processos da organização e a recuperação dos sistemas de informação, de forma a garantir que a organização poderá continuar operando – como usualmente ou em um nível aceitável – na ocorrência de um desastre; e que os recursos de TI sejam restabelecidos a um estado similar ao existente antes do desastre.

Savage (2002) alerta para o fato de muitos equivalerem o BCM à recuperação de desastres restrita aos sistemas de informação – possivelmente pela característica da TI de permear toda a organização.

Com a implementação dos computadores, os sistemas de informações foram completamente remodelados e hoje são dependentes da informática – a maioria das organizações não mais sobreviveriam sem seus computadores (BOTHA; VON SOLMS, 2004).

Com base nessa situação, alguns autores alegam que a realização de cópias de segurança (*backup*), e a sua devida guarda, representam 99% do plano de continuidade (SALDANHA, 2000). De fato, a recuperação de desastre originalmente objetivava minimizar o período em que as bases de dados ficavam fora de operação (BOTHA; VON SOLMS, 2004), procurando agilizar o

processo de retorno à operação e recuperando as cópias de segurança, caso tivesse ocorrido perda de dados.

No entanto, o BCM procura minimizar – ou até evitar – o impacto de interrupções do negócio e, portanto, deve abranger todos os processos críticos da organização, não se restringindo aos sistemas de informações.

Vale salientar que se deve 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 (movimento sem terra, movimento contra barragens, por exemplo); greve; ameaça de bomba; problemas com fornecedores; etc.

Neste sentido, má gestão da cadeia de suprimentos, falta de política ambiental, não clareza em planos de salários, gratificações ou incentivos, podem aumentar o risco de interrupção.

Note-se que o gerenciamento da continuidade do negócio não deixa de ser um gerenciamento de risco e, portanto, também procura avaliar e controlar os riscos existentes na organização. No entanto, o foco principal é a elaboração de planos de como proceder diante dos riscos que foram aceitos.

Também não existe um consenso do que exatamente compõe o plano de continuidade do negócio e tampouco quanto à designação de cada parte – Saldanha (2000), por exemplo, exclui do plano o retorno à condição normal. Neste sentido, o Quadro 2.5 apresenta brevemente a estrutura e a nomenclatura adotada neste trabalho, ilustrada na Figura 2.6.

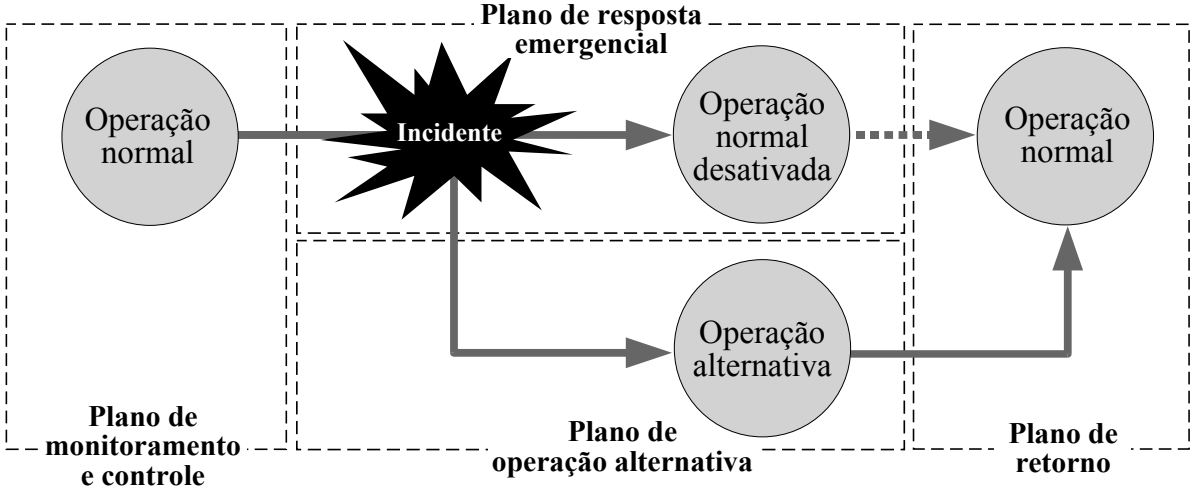


Figura 2.6: Estados de operação do sistema e os respectivos planos, para o caso de ativação do plano de operação alternativa

Quadro 2.5: Tipos de planos inseridos na continuidade do negócio

1. **Monitoramento e controle:** procura monitorar indicadores com o intuito de prevenir a ocorrência do incidente ou alertar da possível ocorrência para que se possa estar preparado e, assim, acionar os procedimentos de resposta emergencial e, eventualmente, de operação alternativa.
2. **Resposta emergencial:** procura minimizar o impacto e a abrangência do incidente.
3. **Operação alternativa (ou operação interina):** procura fornecer alternativas para se executar os processos críticos a fim de mantê-los ativos, mesmo durante o incidente.
4. **Retorno:** retornar à condição normal de operação, recuperando os processos da organização e transferindo os processos alternativos para os processos usuais, quando aplicável.

Essa definição é corroborada pela norma ABNT ISO/IEC 17799 que, apesar de não ter designado nomes para cada parte, refere-se aos procedimentos relativos ao monitoramento e controle; emergência; operação alternativa; e retorno – conforme apresentado a seguir (ABNT, 2001, p. 46 e 47):

1. "as condições para ativação dos planos, os quais descrevem os processos a serem seguidos previamente à ativação (como se avaliar a situação, quem deve ser acionado, etc.)" ;
2. "os procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência do incidente [...]";
3. "procedimentos de recuperação que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infraestrutura para localidades alternativas temporárias [...]"; e
4. "procedimentos de recuperação que descrevam as ações a serem adotadas quando do restabelecimento das operações".

Observe-se que o termo "recuperação", no último tópico, se refere ao retorno às operações normais e não à recuperação de desastres.

Outros dois conceitos que são bastante utilizados no BCM estão apresentados a seguir[5]:

1. Vulnerabilidade – Weichselgartner (2001) apresenta três abordagens para a vulnerabilidade: como sendo relativa à exposição a um risco (que pode ser relacionado aos perigos); como sendo relativa à capacidade de responder ao incidente a fim de minimizar as consequências (que pode ser relacionada a uma característica social); e uma terceira abordagem, que combina elementos das duas primeiras, no entanto está mais focada na

[5]Outros termos estão apresentados no Glossário.

localização – assim, a vulnerabilidade pode ser vista como uma característica do domínio geográfico.

2. Ameaça – Para Saldanha (2000, p. 52), ameaça é "toda e qualquer condição adversa capaz de vir a causar alguma perda para a empresa. Uma ameaça é uma condição latente e potencial. Ela não irá causar necessariamente um dano."

Note-se que, apesar de não existir um consenso sobre a nomenclatura utilizada, o processo de gerenciamento de risco é utilizado por inúmeras organizações, basicamente contendo os mesmos ingredientes essenciais. Por exemplo: o gerenciamento da continuidade considera ameaças, vulnerabilidade e impacto como elementos-chaves na identificação do risco – que são equivalentes aos eventos indesejados, à chance de ocorrência e à severidade das consequências, respectivamente, para o gerenciamento de segurança (NASA, 2004a).

É interessante destacar que a segurança deve ser levada em consideração no gerenciamento de continuidade da unidade organizacional. De maneira análoga, a segurança não deve ser gerenciada sem considerar a disponibilidade do sistema técnico, por exemplo.

A Figura 2.7 ilustra a relação entre segurança e continuidade – ou disponibilidade, dependendo do caso –, resumida no Quadro 2.6.

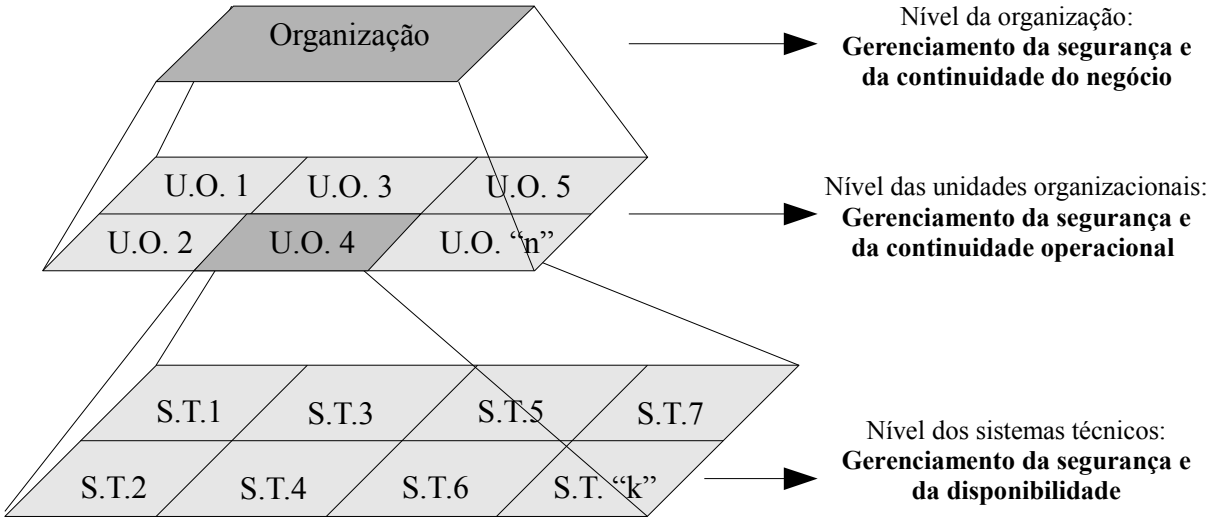


Figura 2.7: Níveis para o gerenciamento de risco em uma organização

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.

A segurança nem sempre tem uma interação positiva com a disponibilidade. 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.

Quadro 2.6: Níveis para gestão de risco

- **Nível da organização:** A gestão de um incidente pode ser feita por um plano de continuidade do negócio e de gerenciamento de crises, que aborde as ações a serem tomadas pela organização em casos de incidentes aceitos e voluntária ou involuntariamente retidos. A continuidade do negócio contribui para atingir a missão da organização.
- **Nível da unidade organizacional:** O monitoramento & controle e a gestão do incidente se dão principalmente por ações de continuidade. A continuidade operacional (dentro dos níveis de segurança) das unidades organizacionais contribuem para a continuidade do negócio.
- **Nível do sistema técnico:** Tanto o monitoramento & controle quanto o planejamento para a ocorrência do incidente se dão, fundamentalmente, por ações de manutenção e garantia de confiabilidade. A disponibilidade, com segurança, dos sistemas técnicos contribui para a continuidade operacional da unidade organizacional.

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 não garante, pois esta depende de outros fatores, como: política econômica, tendências de mercado, boatos, etc.

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

2.4 Considerações finais

Ao longo do Capítulo 2, foram apresentados alguns conceitos importantes relativos ao risco.

Quanto ao gerenciamento de risco, constatou-se que este contempla a análise / avaliação, o tratamento, a aceitação e a comunicação de riscos – conforme proposto na norma ABNT ISO/IEC Guia 73 (ABNT, 2005).

Diante da comparação de algumas abordagens do risco, foi apresentada uma definição para este termo. Também, optou-se pelo modelo de representação do incidente pela corrente causal,

apresentado por Mosleh et al. (2004). É com base no conceito da corrente causal que será feita a análise dos riscos, que – por sua vez – fornecerá os fundamentos para o gerenciamento dos riscos.

Destacou-se, então, o fato de o gerenciamento de segurança e de continuidade se diferenciarem pelos tipos das consequências de um incidente e propôs-se uma classificação delas. Esta classificação pode ser transposta para o nível dos sistemas técnicos considerando a disponibilidade em substituição da continuidade.

Assim, ficou evidente a possibilidade de consolidar, em um único sistema de gestão, as questões relacionadas à continuidade e à segurança.

A diferença de nomenclatura foi evidenciada como uma das dificuldades para a integração dos sistemas de gestão de risco, sendo um dos objetivos específicos deste trabalho compatibilizar conceitos e nomenclatura adotados no gerenciamento de segurança e de continuidade.

A nomenclatura adotada neste trabalho está, sempre que pertinente, baseada nas recomendações da norma ABNT ISO/IEC Guia 73. A norma apresenta definições genéricas, que serão adaptadas ao contexto deste trabalho. A terminologia adotada está sendo apresentada ao longo do texto; no entanto, o Quadro 2.7 apresenta um resumo das principais definições abordadas até o momento – estas definições também podem ser encontradas no Glossário, bem como de outros termos pertinentes à gestão de risco.

Quadro 2.7: Terminologia proposta para gerenciamento de risco

Risco: 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 $P(Estado\ futuro\ \text{“}x\text{”} \mid Estado\ inicial)$ –, sendo necessário, para sua completa caracterização, o delineamento dos dois estados, além dos cenários que possibilitem esta transição (que compõem o perfil do risco).
Evitar o risco: Não se expor a um determinado risco – implica eliminar o perigo.
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. Note-se que a norma ABNT (2005) exclui da transferência estratégias de reposicionamento de uma fonte de risco (como na terceirização).
Redução do risco: Trabalhar o risco a fim de diminuir a probabilidade de ocorrência do incidente e sua gravidade.

(continua na próxima página)

Quadro 2.7: Terminologia proposta para gerenciamento de risco

(continuação)

Retenção do risco: 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).
Incidente: Incidente é todo evento que interfere negativamente na organização. Desta forma, o termo incidente engloba o conceito de acidente – que é restrito a eventos que acarretem dano.
Prevenção do incidente: Equivalente ao "monitoramento e controle". Neste trabalho, será evitada a designação "prevenção do incidente", para facilitar a distinção do contexto da "redução do risco".
Gerenciamento do incidente: Gerenciamento sistemático de atividades e recursos objetivando mitigar as consequências de um incidente – mitigando os danos e / ou a condição de interrupção do negócio.

Neste sentido, também foi apresentada a estrutura adotada para o gerenciamento da continuidade, que contempla o monitoramento e controle, a resposta emergencial, a operação alternativa (ou operação interina) e o retorno à operação normal.

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. Com isso foi possível correlacionar os conceitos de segurança, confiabilidade, mantenabilidade e continuidade.

3 *Abordagens de gerenciamento de risco em diferentes setores*

Este capítulo apresenta uma breve revisão histórica e uma descrição da aplicação da gestão de risco nos setores: nuclear (principalmente americano); marítimo; aéreo; aeroespacial; empresarial; e elétrico brasileiro – destacando as metodologias, técnicas e diretrizes adotadas em cada setor.

3.1 Gestão de risco no setor nuclear

Para o setor nuclear, a segurança é o foco do gerenciamento de risco. Um incidente em uma planta nuclear pode ter proporções catastróficas, o que deflagra o mecanismo de aversão ao risco[1]. É fato que, para garantir a segurança, é necessário garantir a disponibilidade de uma série de sistemas técnicos, o que corrobora com a ideia de gerenciar o risco de maneira abrangente.

Historicamente, o setor nuclear vem fazendo a análise / avaliação da segurança de plantas nucleares com base numa abordagem determinística, que surgiu na década de 1940 e ainda hoje é a base para a aprovação de plantas nucleares nos EUA (DIAS et al., 2007a). A abordagem probabilística ganhou força na década de 1970, com a publicação do relatório WASH-1400[2] – também conhecido como "Rasmussen Report" –; no entanto, somente após o incidente de Three Miles Island, em 1979, o relatório se tornou referência para as PRAs (*probabilistic risk assessment*) no setor nuclear. Keller & Modarres (1998) destacam que muitos dos procedimentos e técnicas descritos no WASH-1400 ainda são utilizados nos dias de hoje – a técnica ETA, por exemplo, foi proposta neste relatório.

Na abordagem determinística, a análise / avaliação é feita de forma a garantir que um con-

[1] Aversão ao risco é a postura de se valorizar mais um incidente com 1000 fatalidades, por exemplo, que 1000 incidentes com 1 fatalidade.

[2] Vide: USNRC (United States Nuclear Regulatory Commission). **WASH-1400 (NUREG-75/014):** *reactor safety study, an assessment of accident risks in* U.S. *commercial nuclear power plants*. USNRC, 1975.

junto básico de "incidentes de projeto" não ocorram. Isso é feito atendendo a uma série de premissas previamente definida. Como consequência dessa abordagem, o projeto das plantas nucleares se caracteriza por ser bastante conservativo – apesar do grande conhecimento sobre os sistemas envolvidos –, fazendo uso de elevadas margens de segurança e de múltiplas barreiras e/ou sistemas de segurança independentes (KELLER; MODARRES, 1998).

Na análise / avaliação probabilística de risco (PRA), o sistema técnico é analisado de forma sistemática objetivando delinear o perfil dos riscos que se está exposto, para posteriormente avaliá-los.

Com o crescimento em tamanho e complexidade das plantas, evidenciou-se a necessidade de uma abordagem baseada no desempenho da planta. Neste sentido, a abordagem quantitativa, destacadamente a probabilística, ganhou ênfase.

Embora o primeiro guia da USNRC (United States Nuclear Regulatory Commission) tenha sido publicado em 1982 (o NUREG/CR-2300 "*PRA procedures guide: A guide to the performance of probabilistic risk assessments for nuclear power plants*"[3]), a PRA foi efetivamente considerada e incorporada no processo de aprovação e licenciamento de plantas nucleares nos EUA, em meados da década de 1990 (KELLER; MODARRES, 1998).

Com a obrigatoriedade do uso da PRA, inicia-se, em 1997, o processo de elaboração de normas para padronizar procedimentos. Em 2002, a primeira dessas normas, a ASME RA-S-2002 "*Standard for probabilistic risk assessment for nuclear power plant applications*"[4], foi homologada pelo ANSI (American National Standards Institute). Em 2003, foi publicada a primeira norma que considera os eventos externos na planta, a ANSI/ANS-58.21-2007 "*External events in PRA methodology*"[5]. (DIAS et al., 2007b).

O guia NUREG/CR-2300 ainda é utilizado e foi o primeiro que propôs a divisão da PRA em três níveis, dependendo da profundidade da análise, a saber (IAEA, 2002 apud DIAS et al., 2007b):

- **Nível 1**: identificar a sequência de eventos que podem levar a danos no núcleo; estimar a frequência de danos no núcleo; fornecer indicativos das capacidades e fraquezas dos sistemas de segurança e dos procedimentos para prevenir danos ao núcleo.
- **Nível 2**: agrupar as sequências de acidentes conforme características si-

[3]Vide: USNRC (United States Nuclear Regulatory Commission). **NUREG/CR-2300:** PRA procedures guide. A guide to the performance of probabilistic risk assessments for nuclear power plants. Final report, Vol. 1-2. USNRC, 1983

[4]Vide: ASME (American Society of Mechanical Engineers). **RA-S-2002:** Standard for probabilistic risk assessment for nuclear power plant applications. New York: ASME, 2002

[5]Vide: ANS (American Nuclear Society). **ANSI/ANS-58.21-2007:** External events in PRA methodology. ANS, 2007.

milares dos estados de danos na planta; identificar os modos pelos quais vazamentos radioativos da planta podem ocorrer; estimar a intensidade e frequência dos vazamentos.

- **Nível 3**: agrupar as categorias de vazamento; estimar consequências e riscos para a saúde pública e ambiental.

Esta estrutura fica clara na abordagem de Kumamoto & Henley (1996) para a corrente causal do incidente. Para os autores, o incidente inicia-se com uma falha ou um outro distúrbio, como apresentado na Figura 3.1.

Na figura, a trajetória do incidente está destacada em cinza. Nela, as elipses representam o estado do sistema ou componente, e os retângulos as medidas para prevenir ou gerenciar o incidente (representadas pelas duas caixas à esquerda).

Para os autores, a primeira medida para se prevenir o incidente é a prevenção da falha. Mas, dada a ocorrência da falha (ou de um distúrbio), pode-se prevenir sua propagação e, por consequência, o incidente – o que está representado pelas setas provenientes das duas elipses em branco, retornando no ponto em que encontram a prevenção da propagação.

No entanto, se a prevenção da propagação falha ou se o distúrbio supera as premissas de projeto (um vento acima do que a estrutura é capaz de suportar, por exemplo), o incidente irá ocorrer – o que está representado pela terceira elipse.

Nesta situação, pode-se agir para mitigar as consequências dentro da planta e não permitir que elas extrapolem os limites da organização. No entanto, caso elas extrapolem, existe, ainda, a possibilidade de mitigar as consequências fora dos limites da organização – ou graves consequências podem ocorrer.

Para Kumamoto & Henley (1996), o processo de gerenciamento de risco consiste em:

1. identificar o risco;
2. gerar um perfil do risco (resultado, chance, cenário causal, população e significância) para cada alternativa possível de controle ativo ou passivo; e
3. cada perfil de risco é avaliado (relação custo-risco-benefício) para se tomar decisões adequadas.

No processo considerado, controles ativos são aqueles que atuam na prevenção do incidente (“prevenção de falha” e “prevenção de propagação”), e controles passivos, na mitigação das consequências (tanto de mitigação interna à planta quanto externa).

O primeiro meio de prevenir falhas é se esforçar para que se tenha uma qualidade de projeto, manutenção, construção e operação da planta – de tal maneira que desvios da operação normal

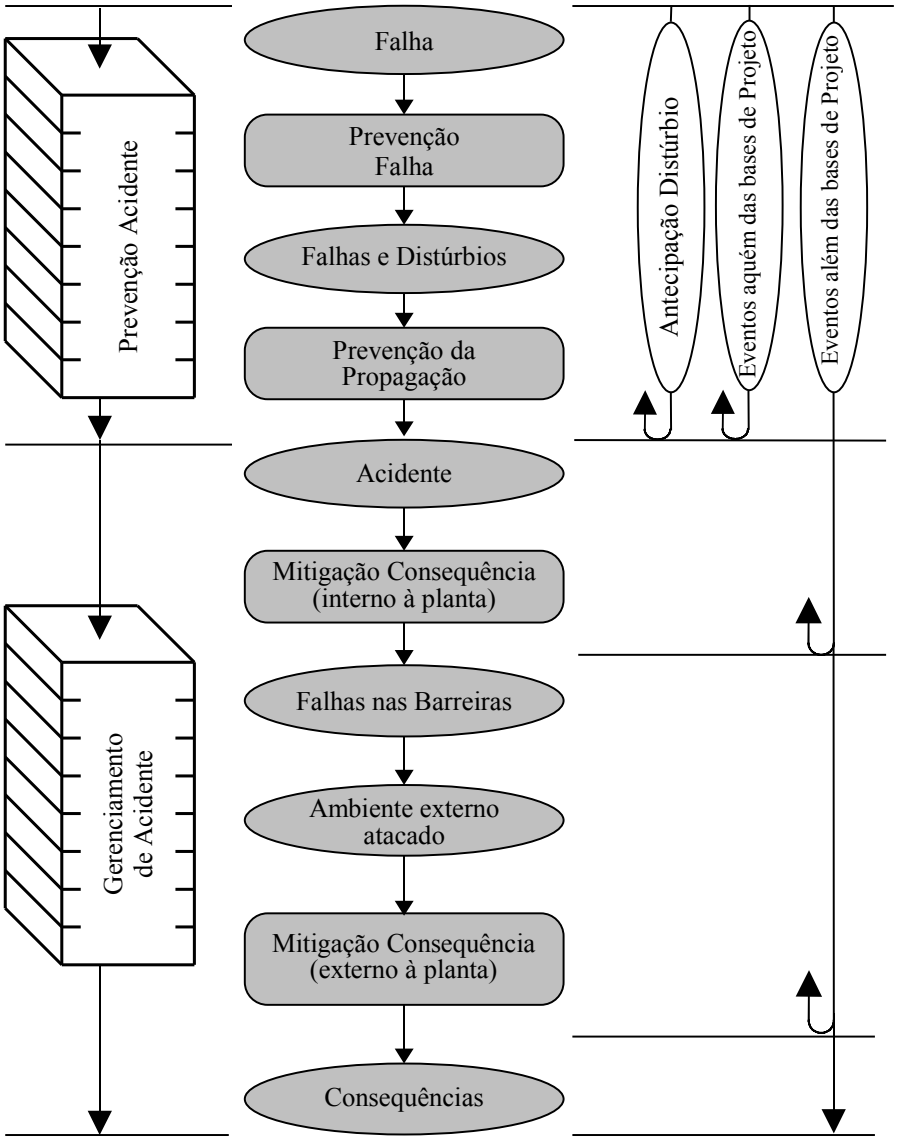


Figura 3.1: Modelo de ocorrência de um incidente
Fonte: Kumamoto & Henley (1996, p. 79, tradução nossa)

não sejam frequentes e que se façam produtos de qualidade (KUMAMOTO; HENLEY, 1996).

Os autores orientam para a implementação de um programa de qualidade assegurada, que é o ciclo de monitoramento e controle das práticas comprovadas de engenharia, dos procedimentos e das atividades.

O programa de qualidade assegurada é mais abrangente que o programa de controle de qualidade e tem por meta garantir que todos os itens produzidos, serviços realizados e tarefas executadas alcancem a especificação requerida.

A prevenção da propagação visa assegurar que a perturbação ou a falha incipiente não se desenvolva, transformando-se em uma situação mais séria.

Uma vez que ocorreu o incidente, deve-se controlar o seu curso e mitigar suas consequências por meio de medidas como: executar desligamento de segurança; manter a continuidade das utilidades, manter a integridade das clausuras; e manter ambiente externo à planta preparado. Estas medidas devem ser fundamentadas na experiência operativa, na análise de segurança e nos resultados de pesquisa sobre segurança.

Incidentes com alta severidade e consequências são extremamente improváveis, se forem efetivamente prevenidos ou mitigados, utilizando a filosofia da defesa-em-profundidade (sequência de controles).

A mitigação interna à planta inclui práticas previamente planejadas e com finalidade específica, que utilizam os recursos da planta, de forma normal ou excepcional.

No caso remoto de as medidas de segurança (mitigação interna) falharem, medidas preventivas devem ser tomadas a fim de mitigar as consequências à população e ao meio ambiente na redondeza da planta (mitigação externa) – como evacuação da população, por exemplo, o que envolve atividades coordenadas em conjunto com as autoridades locais.

3.2 Gestão de risco no setor marítimo

Assim como no setor nuclear, a análise / avaliação de segurança no setor marítimo era essencialmente determinística – por meio de regulamentos, regras, leis, etc. impostos por diferentes estados, organizações e instituições – e passou, recentemente, a contar também com abordagem probabilística, com a publicação da análise / avaliação formal de segurança (FSA – *formal safety assessment*) pela International Maritime Organization (IMO).

A regulamentação do setor é estabelecida fundamentalmente pela IMO e, de forma complementar, pelas sociedades classificadoras, tais como a Det Norsk Veritas (DNV), American Bureau of Shipping (ABS) e outras, pelo uso de suas regras para classificação de navios. Das regulamentações, as mais notórias são as convenções SOLAS[6] e a MARPOL[7], acrônimos para "*safety of life at sea*" e "*marine pollution*", que estabelecem requisitos e padrões mínimos relativos à segurança dos navios e à prevenção da poluição marinha, respectivamente.

Na abordagem determinística, muitas das especificações foram baseadas na experiência passada e, muitas delas, após a ocorrência de algum acidente importante. A primeira versão da convenção SOLAS, por exemplo, foi estabelecida em 1914, logo após o acidente com o Titanic.

[6] Vide: IMO (International Maritime Organization). **SOLAS:** International convention of safety of life at sea. Consolidated edition. IMO, 2004.

[7] Vide: IMO (International Maritime Organization). **MARPOL:** International convention for the prevention of pollution from ships. Consolidated edition. IMO, 2004.

(DIAS et al., 2007b).

Em resposta ao incidente ocorrido em Piper Alpha, em 6 de julho de 1988, que resultou em 167 mortes, a divisão de segurança *offshore* da HSE (Health and Safety Executive) desencadeou a revisão de toda a legislação de segurança de *offshores*. Como resultado, foi proposto que se substituíssem as regras prescritivas por um regime de metas. Em 1992, foi publicada uma versão preliminar, que foi submetida à consulta pública, e, em 1993, após considerar os comentários feitos à revisão anterior, foi divulgada a regulamentação. Ela requer que se demonstre que os perigos com potencial de causar incidentes de maiores proporções foram identificados, os riscos avaliados e medidas foram tomadas para reduzi-lo "tão baixo quanto e razoavelmente praticável" (ALARP [8] – *as low as reasonably practicable*).

Paralelamente, na indústria de navios, incidentes com grande proporção chocaram a opinião pública e atraíram a atenção para a segurança das embarcações. A investigação de um destes incidentes, o afundamento do *ferry* "Herald of Free Enterprise", ocorrido em 1987, resultou no relatório conhecido como "Lord Carver's report", publicado em 1992 , que recomendou – encorajado pela adoção de regime de metas para instalações *offshore* – que fosse adotada uma abordagem regulatória não-prescritiva, baseada em desempenho. Esta era a ideia inicial da análise / avaliação formal de segurança de embarcações. (WANG, 2001).

A FSA é uma metodologia estruturada que envolve o uso de técnicas de análise de risco e avaliação de custo-benefício para dar suporte ao processo de tomada de decisões. A metodologia, brevemente apresentada a seguir, compreende 5 etapas – ilustradas na Figura 3.2 – e está descrita no documento "*Guidelines for formal safety assessment (FSA) for use in the IMO rule-making process*" (IMO, 2002).

De maneira geral, essas cinco etapas podem ser descritas pelas seguintes questões:

- O que pode sair errado? (identificação dos perigos)
- Quão ruim e quão provável? (análise de risco)
- Isso pode ser melhorado? (opções de controle de risco)
- Qual o custo e quão melhor iria ficar? (avaliação do custo benefício)
- Quais ações devem ser tomadas? (recomendações para a tomada de decisão)

A identificação dos perigos visa listar os perigos e cenários associados, priorizados pelo nível de risco específico para o problema que se está estudando.

Usualmente a identificação dos perigos compreende a combinação de técnicas criativas e

[8] Alguns autores, ex. Kumamoto & Henley (1996) e NASA (2004b), adotam a designação ALARA (*as low as reasonably achievable*)

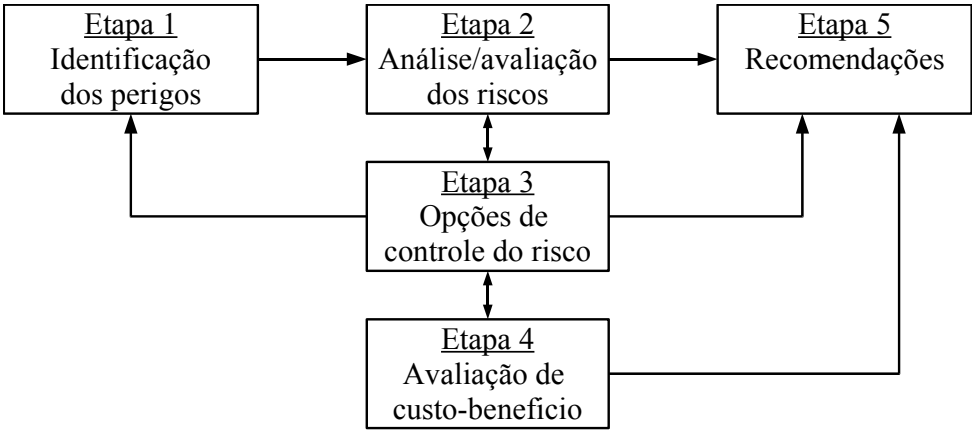


Figura 3.2: Metodologia FSA
Fonte: adaptado de IMO (2002)

analíticas objetivando identificar tanto as situações que já ocorreram (abordagem reativa) quanto as novas (abordagem proativa). Também se analisam a corrente causal e os possíveis resultados de cada incidente considerado.

Uma vez identificados os perigos e os cenários associados, na avaliação, pode-se classificá-los e priorizá-los – descartando os cenários considerados "menores".

A análise de risco, por sua vez, objetiva detalhar a investigação das causas e consequências dos cenários mais importantes, identificados na etapa anterior. Isso permite que a atenção esteja voltada para as áreas de alto risco e para a identificação e análise de fatores que possam influenciar no nível do risco.

No que se refere à análise quantitativa, pode-se fazer uso de base de dados e, quando não se tem dados disponíveis, devem-se utilizar cálculos, simulações ou outro tipo de técnica reconhecida, baseada no conhecimento dos especialistas.

A terceira etapa objetiva propor opções de controle de risco práticas e efetivas seguindo quatro principais passos: (1) focar nas áreas que necessitam de controle de risco; (2) identificar potenciais medidas de controle de risco; (3) avaliação da efetividade das medidas na redução do risco, reavaliando seu perfil; e (4) agrupar as medidas em opções de regulamentações práticas.

Para a determinação das áreas que necessitam controles, deve-se avaliar o resultado da segunda etapa, baseando-se principalmente em:

- Nível de risco, considerando a frequência de ocorrência em conjunto com a severidade dos resultados – assim, incidentes considerados inaceitáveis são prioritários.
- Probabilidade, identificando as áreas que têm alta probabilidade de ocorrência – elas de-

vem ser avaliadas independentemente da severidade.

- Severidade, identificando as áreas que têm alta severidade – elas devem ser avaliadas independentemente da probabilidade de ocorrência.
- Confiança, identificando as áreas com erro epistemológico considerável.

O levantamento de medidas dos riscos que não estão suficientemente controlados pelas medidas existentes deve, de maneira geral, objetivar um ou mais dos seguintes fatores: (i) reduzir a frequência de falha por meio de melhores projetos, procedimentos, políticas organizacionais, treinamento, etc.; (ii) mitigar os efeitos das falhas, a fim de prevenir o incidente; (iii) abrandar as circunstâncias em que a falha pode ocorrer; e (iv) mitigar as consequências do incidente.

As medidas de controle devem, então, ser avaliadas quanto à eficácia da redução do risco, conforme Etapa 2, para posteriormente serem grupadas em opções de regulamentações práticas.

Na avaliação do custo-benefício, por sua vez, deve-ser identificar e comparar os benefícios e os custos associados com a implementação das opções de controle do risco.

Esse processo deve ser conduzido para situações genéricas e, posteriormente, para as partes afetadas que são mais influenciadas, direta ou indiretamente, pelos efeitos do incidente ou pelas novas medidas reguladoras propostas.

As opções de controle devem, então, ser expressas utilizando algum índice de eficácia, por exemplo: "custo bruto para evitar uma fatalidade" (Gross CAF – *Gross cost of averting a fatality*) e "custo líquido para evitar uma fatalidade" (NetCAF – *Net cost of averting a fatality*) (SKJONG, 2002).

Assim, baseadas na comparação de opções alternativas, na potencial redução dos riscos e nos custos para implementar as alternativas é possível definir as recomendações para a tomada de decisão.

3.3 Gestão de risco no setor aéreo

Metas de segurança numéricas para definição de condições de operação foram propostas pela International Civil Aviation Organization (ICAO) na década de 1950 (LEDERMAN F. NIEHAUS, 1996). No entanto, somente no início dos anos 60, com o aumento da complexidade do projeto das aeronaves, a indústria aeronáutica buscou o desenvolvimento estruturado de teorias de probabilidade, em relação ao projeto e à análise / avaliação de segurança (SILVA, 2006).

Foi nesta época, por exemplo, que H. A. Watson, do Bells Laboratory, em parceria com a força aérea norte-americana, concebeu a FTA (*fault tree analysis*) para estudar o sistema de

controle de lançamento do míssil Minuteman. Técnica que, posteriormente, a Boeing começou a usar durante o projeto de aeronaves comerciais (ERICSON II, 1999).

Atualmente, existem inúmeras organizações – tais como: SAE (Society of Automotive Engineers), FAA (Federal Aviation Administration / United States of America), JAA (European Joint Aviation Authorities) e Eurocontrol (European Organization for the Safety of Air Navigation) – trabalhando para desenvolver regulamentações, recomendações e metodologias na perspectiva de garantir a segurança.

No caso da Eurocontrol, ela propõe a EATMP SAM (*European air traffic management programme safety assessment methodology*), ilustrada na Figura 3.3. A SAM é similar à metodologia proposta pela SAE nas recomendações práticas ARP 4761[9], mas seu escopo é expandido para todo o sistema de navegação – cobre os serviços de informação aeronáutica; busca e resgate; e gerenciamento do tráfego aéreo –, enquanto a ARP 4761 restringe-se à aeronave (EVERDIJ; BLOM, 2008).

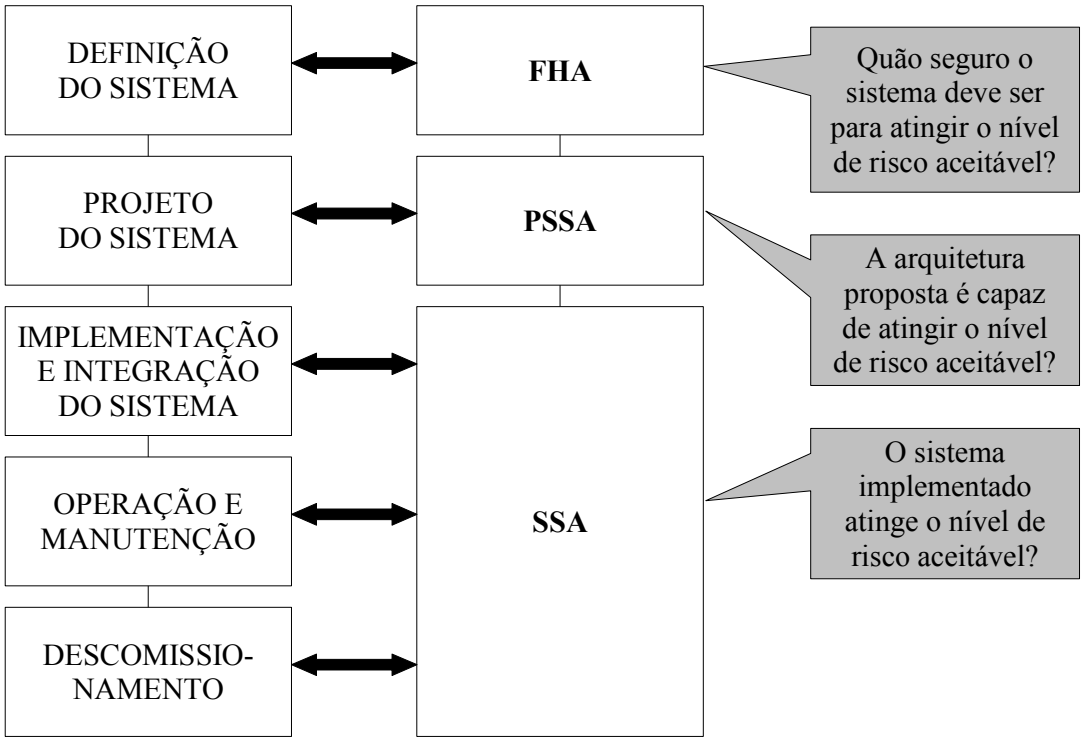


Figura 3.3: Processo de análise / avaliação da segurança e o ciclo de vida do sistema
Fonte: EUROCONTROL (2006, Level 1 / SAM / p. 4, tradução nossa)

A verificação da execução da metodologia apresentada na ARP 4761 é feita utilizando-se a ARP 4754, que foi elaborada para ser um guia para a equipe de certificadores e para a equipe

[9] Vide: SAE (Society of Automotive Engineers). **ARP 4761:** Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. Warrendale, 1996.

de desenvolvedores dos sistemas, particularmente sistemas complexos e altamente integrados, com significativa importância de *softwares*. A ARP 4754 foi desenvolvida no contexto da FAR (*federal aviation regulations*) e da JAR (*joint airworthiness requirements*) parte 25 – também pode ser aplicada a outras regulamentações, como as partes 23, 27, 29 e 33. (SAE, 1996).

A Figura 3.3 ilustra como a metodologia utilizada para a avaliação da segurança abrange todo o ciclo de vida de um sistema de navegação aéreo, das definições iniciais do sistema até seu descomissionamento, passando pelo projeto, implementação, integração, transferência para operações, operações e manutenção.

A metodologia envolve basicamente três fases principais (EUROCONTROL, 2006):

- Na análise / avaliação do perigo funcional (*functional hazard assessment* – FHA) identificam-se os modos de falha, os perigos e suas consequências para a segurança das operações dentro de um ambiente específico. Utilizando-se a experiência e o julgamento operacional e de engenharia, a severidade de cada efeito é determinada e classificada em 5 níveis. Podem-se, então, especificar os objetivos de segurança, i.e., especificar o nível de segurança que o sistema deve atingir. Objetivo de segurança é uma declaração, quantitativa ou qualitativa, que define a máxima frequência (ou probabilidade) na qual um risco pode ser aceito.
- Análise / avaliação preliminar de segurança do sistema (*preliminary system safety assessment* – PSSA) é fundamentalmente um processo *top-down* iterativo que se inicia no começo do projeto (ou do re-projeto) e objetiva demonstrar se o sistema analisado atende aos objetivos de segurança estabelecidos. A PSSA examina a arquitetura do sistema proposto e determina como as falhas dos componentes e/ou eventos externos podem causar ou contribuir para os riscos identificados na FHA. Na PSSA, os objetivos de segurança são desdobrados em requisitos de segurança alocados em cada componente do sistema, i.e., especifica-se o nível de risco a ser alcançado por cada elemento do sistema. Requisitos de segurança são medidas de redução de risco definidas para alcançar um objetivo de segurança particular. Uma arquitetura de sistema somente alcançará os objetivos de segurança estabelecidos na FHA se os elementos do sistema cumprirem os requisitos de segurança.
- A análise / avaliação de segurança do sistema (*system safety assessment* – SSA) se inicia com a implementação do sistema de navegação aérea. A SSA objetiva demonstrar que o sistema, como implementado, tem um nível de risco aceitável (ou pelo menos tolerável) e consequentemente atende aos objetivos de segurança estipulados na FHA. Os elementos do sistema, por sua vez, também devem atender aos requisitos de segurança especifica-

dos na PSSA. Demonstra-se que todos os riscos foram eliminados ou minimizados tanto quanto praticável razoavelmente (*as low as reasonably practicable* – ALARP) e, posteriormente, monitora-se o desempenho de segurança do sistema durante sua operação. A Figura 3.4 ilustra o processo da SSA.

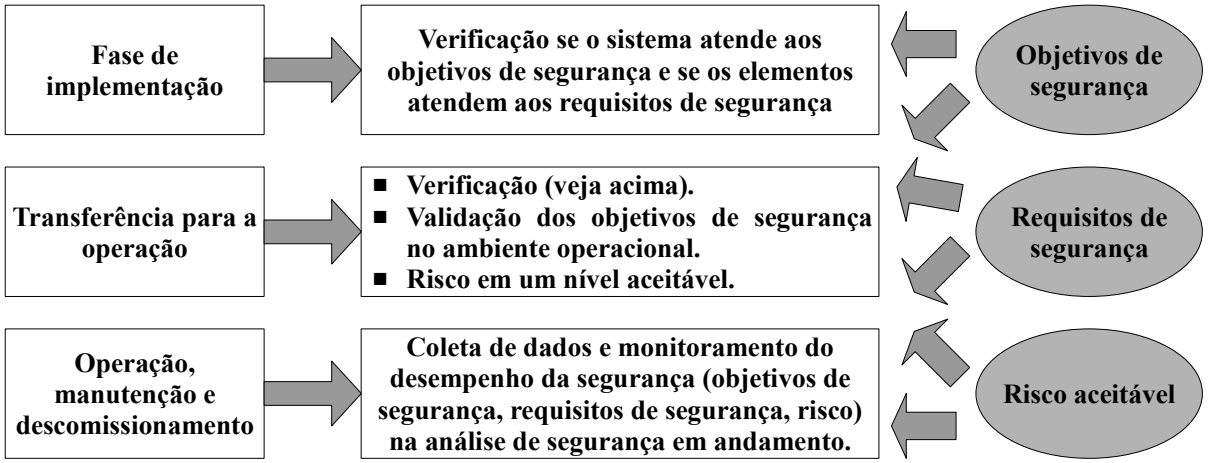


Figura 3.4: Processo de análise / avaliação de segurança do sistema (SSA)
Fonte: EUROCONTROL (2006, Level 1 / SSA / p. III-6, tradução nossa)

É interessante destacar que a FHA – normalmente – é implementada antes de o sistema existir, durante a fase de projeto, no entanto o documento RVSM 697 traz uma análise feita em um estágio avançado do programa de redução da distância vertical mínima (*reduced vertical separation minimum* – RVSM[10]) entre aeronaves de 2.000ft (609,6m) para 1.000ft (304,8m), para aeronaves voando entre 29.000ft (8.839,2m) e 41.000ft (12.496,8m). O programa RVSM estava tão adiantado, que seria difícil mudar muitos (ou algum) procedimentos de operação ou requisitos do sistema. No entanto, a análise foi feita na perspectiva de que, se algum problema fosse identificado, isto seria levado em consideração pelo programa RVSM. (EUROCONTROL, 2006).

No total, foram identificados e analisados 73 perigos. Para cada um deles, foi estabelecido um objetivo de segurança. Estes objetivos foram, então, confrontados com o resultado da análise após as medidas de redução de risco, a fim de verificar se o programa RVSM atingiu o especificado. (EUROCONTROL, 2006).

[10]O programa RVSM está implementado na Europa desde janeiro de 2002 (FAA, 2007).

3.4 Gestão de risco no setor aeroespacial

No setor aeroespacial, especificamente o norte-americano, a NASA (National Aeronautics and Space Administration – USA) destaca que pretende implementar análise / avaliação de risco probabilística em todos os seus programas e se tornar referência em PRA. Para a NASA, uma PRA objetiva garantir o sucesso da missão e do programa, e atingir e manter um alto padrão de segurança. (NASA, 2002b).

Note-se que, para a NASA, a PRA extrapola a preocupação com a segurança e visa garantir o sucesso da missão.

Tendo em vista que o desenvolvimento da PRA no setor aéreo iniciou-se na década de 1960, era de se esperar que a NASA tivesse, desde então, adotado esta prática. De fato, no começo do projeto Apollo, questionou-se qual era a probabilidade de sucesso em enviar astronautas à Lua e retorná-los em segurança. De alguma forma, foi feito um cálculo de risco / confiabilidade e a probabilidade obtida foi considerada inaceitavelmente baixa. Isso teria desencorajado a NASA a fazer outros estudos probabilísticos, adotando, em contrapartida, análises de risco qualitativa, como a FMEA. No entanto, após o incidente com a Challenger, em 1986, a importância da PRA veio à tona e seu uso começou a crescer. (NASA, 2002a).

A NASA adota a metodologia de gerenciamento de risco contínuo (*continuous risk management* – CRM) para todo o ciclo de vida de seus programas (NASA, 2002b) e salienta que uma comunicação aberta entre os seus membros e uma visão ampla do programa e de seus critérios de sucesso são pontos essenciais para um gerenciamento de risco bem sucedido (NASA, 2004a).

Apesar de a metodologia atender a todo o ciclo de vida, tem ênfase nas etapas anteriores à operação, uma vez que a NASA exige que se tenha um posicionamento de todos os riscos antes da entrega para a operação (NASA, 2004a).

O principal objetivo de um sistema de segurança – para a NASA – é fornecer uma abordagem organizada e disciplinada de como identificar e trabalhar precocemente os perigos às pessoas, às instalações e equipamentos, ou ao sucesso do programa até atingir níveis tão baixos quanto se possa considerar razoável aceitar (*as low as reasonably achievable* – ALARA[11]) (NASA, 2004b). As atividades do sistema de segurança estão subdivididas conforme apresentado na Figura 3.5.

A identificação procura levantar cada risco, em relação ao evento indesejado, e as consequências que este evento pode causar. Adicionalmente, devem-se incluir todas as informações necessárias para localizar o risco no contexto (o que; quando; onde; como; e por quê)

[11] Que é um conceito equivalente ao ALARP (*as low as reasonably practicable*).

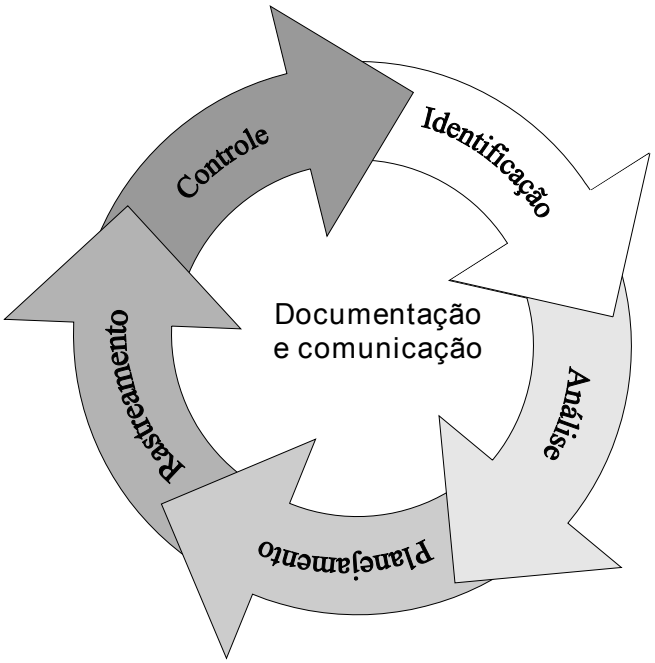


Figura 3.5: O processo de gerenciamento contínuo de risco
Fonte: (NASA, 2002b, p. 8, tradução nossa)

do programa – o que é importante para outras pessoas entenderem, especialmente quando já se passou algum tempo (NASA, 2002b; NASA, 2004a). Nessa fase, devem-se fazer as seguintes questões – não se restringindo a elas –, mesmo para os casos que estão sendo bem sucedidos (NASA, 2004a): O que pode dar errado? Quais as consequências possíveis – à segurança, aos objetivos do programa, ao cronograma, e aos custos – se isto der errado?

Técnicas como árvore de evento (*event tree analysis* – ETA) e árvore de falha (*fault tree analysis* – FTA) podem ser utilizadas nessa fase (NASA, 2002b).

Os resultados principais dessa fase são a "declaração de cada risco" (contendo todas as informações sobre o risco, de forma concisa) e a lista dos riscos (ordenada por prioridade com as informações necessárias para gerenciar e documentar a evolução dos riscos ao longo do ciclo de vida).

Na análise dos riscos, as seguintes questões devem ser respondidas, mas sem se restringir a elas (NASA, 2004a): Qual a chance de esse risco ocorrer? Quão cedo devem ser tomadas as ações relativas a esse risco? Como esse risco pode ser comparado com outros riscos?

A análise do risco procura identificar a chance de o risco ocorrer e o momento em que se devem tomar ações para que o risco identificado não cause danos (por exemplo: curto-prazo; médio-prazo; e longo-prazo). A estimativa pode ser tanto qualitativa quanto quantitativa e deve possibilitar que se classifiquem e priorizem os riscos em relação a seu impacto.

Pode-se fazer uso de técnicas como: FTA; análise do modo de falha, efeitos e criticidade (FMECA); escalas de risco; análise estatística dos históricos; comparação com sistemas análogos; etc.

No planejamento dos riscos, por sua vez, procura-se responder às seguintes questões, mas sem se restringir a elas (NASA, 2004a): O que pode ser feito para prevenir, ou pelo menos diminuir a probabilidade ou a severidade das consequências? Quem deve ser acionado para tomar essas providências?

O planejamento envolve delegar a responsabilidade e determinar a abordagem que deve ser adotada em resposta a cada risco identificado e, caso se opte por mitigá-lo, devem-se elaborar e implementar as subsequentes ações.

As seguintes abordagens podem ser adotadas:

1. mitigação: envolve eliminar o risco ou reduzir a chance de ele ocorrer, ou o impacto de suas consequências (o que implica definir o escopo do plano de mitigação, estabelecendo metas e determinando os recursos necessários para sua implementação);
2. aceitação: devem-se estabelecer critérios para aceitar um risco (um critério pode ser, por exemplo, o fato de existirem planos de contingência ou de recuperação documentados, testados e aprovados para mitigar as consequências, caso o risco ocorra);
3. pesquisa: inclui coleta de novas informações, avaliação e documentação dos resultados, nos quais se basearão as próximas decisões, ou – em alguns casos – para reduzir as incertezas envolvidas na estimativa do risco (metaincertezas);
4. monitoramento: decide-se não tomar medidas imediatas, mas rastrear, levantar e observar as tendências no comportamento dos indicadores do risco no decorrer do tempo.

No rastreamento do risco, pretende-se avaliar o progresso do programa de gerenciamento de risco. Para tanto, as seguintes questões devem ser respondidas, mas sem se restringir a elas (NASA, 2004a): As ações para mitigação dos riscos estão sendo efetivas e estão dentro dos limites do orçamento? O risco geral do programa está aumentando ou diminuindo? Se o risco geral está diminuindo e se está diminuindo ao máximo que se pode praticar?

Rastrear os riscos envolve coleta, atualização, processamento, organização e análise dos dados para indicar as tendências de um determinado risco no decorrer do tempo. No caso de o risco estar sendo monitorado, devem-se definir os limites de controle ou de alerta (*trigger levels*).

No controle do risco, tomam-se decisões quanto à implementação de medidas relativas a um determinado risco, com base nas informações coletadas no rastreamento do risco (NASA,

2004a). Para tanto, as seguintes questões devem ser respondidas, mas sem se limitar a elas: Quais riscos ainda necessitam ser pesquisados? Quais medidas para mitigar o risco precisam ser revisadas? O risco atingiu um nível que o plano de contingência deve ser acionado? Quais riscos podem ser aceitos e formalmente retidos, aceitando o risco residual?

Cada risco deve ser periodicamente revisado para assegurar que as decisões tomadas estão sendo efetivas e que as ações relacionadas a ele se mantêm aplicáveis.

O gerenciamento de risco deve contar com uma comunicação aberta, clara e contínua dos membros da equipe do programa. A documentação deve assegurar que a política do gerenciamento de risco estabelecida foi entendida, implementada e mantida, e que se executem auditorias para identificar a origem e o raciocínio para todas as decisões relativas a riscos. Adicionalmente, indicam-se alguns requisitos e recomendações relativas aos riscos para: o plano do programa; o plano de aquisições; o plano de gerenciamento de risco; a declaração de risco; e a lista de riscos. (NASA, 2004a).

3.5 Gestão de risco no setor empresarial, quanto ao gerenciamento de continuidade

Como apresentado no Capítulo 2, o gerenciamento de continuidade foi uma evolução da recuperação de desastres.

Atualmente, existem diversas metodologias para gerenciamento de continuidade – algumas delas citadas no Quadro 3.1, na Seção 3.7. A seguir, será brevemente apresentada a metodologia proposta pelo Business Continuity Institute, conforme BCI (2005). É interessante destacar que as metodologias indicadas no Quadro 3.1 se diferenciam quanto à estrutura, no entanto abordam basicamente os pontos – o que será salientado ao longo da Seção 3.7.

O BCI propõe um ciclo de vida do gerenciamento da continuidade do negócio, ilustrado na Figura 3.6, dividido em 5 estágios – não necessariamente seguindo uma progressão rígida –, além do gerenciamento do programa.

O gerenciamento do programa de continuidade do negócio pode ser dividido em três partes: política do BCM, gerenciamento do programa e preparação e resposta a incidentes.

A política do BCM objetiva produzir um documento, elaborado pelos executivos, que apresente os princípios e a estrutura da gestão que norteará o delineamento e a construção do BCM. Cabe, nessa fase, a definição do modelo de BCM que será seguido, o levantamento de normas, leis e diretrizes que podem influenciar no BCM, etc.

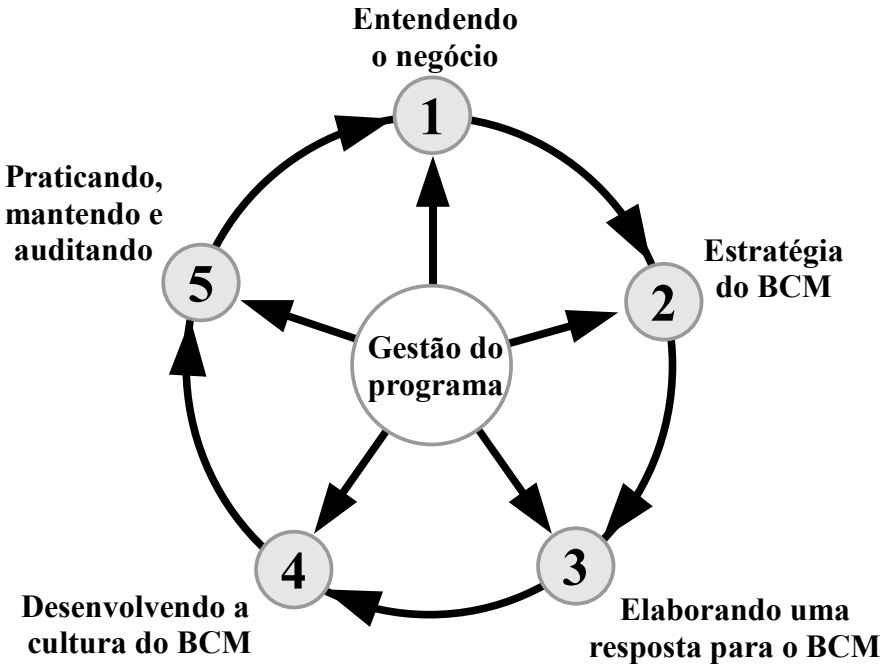


Figura 3.6: Ciclo de vida do gerenciamento da continuidade do negócio
Fonte: BCI (2005, p. 8, tradução nossa)

O gerenciamento do programa contempla processos como definição de pessoal, definição de escopo e monitoramento do desempenho do programa.

Por fim, a preparação e resposta a incidentes objetiva manter a organização atenta para que, no caso de ocorrer um incidente, a resposta seja feita de maneira tranquila e tenha como saída o retorno bem sucedido à condição normal.

O primeiro estágio visa entender o negócio. Para tanto, prevê-se estudar a estratégia da organização, analisar os impactos de incidentes no negócio e a análise de risco desses incidentes.

O estudo da estratégia da organização procura alinhar o BCM com o plano de negócios da organização. Devem-se prever, durante a elaboração do BCM, os planos de longo e médio prazo da organização, para que seja elaborado um BCM capaz (flexível o suficiente) de ser adaptável às situações futuras. Nessa fase, devem-se definir quais os tempos máximos de interrupção que a organização suporta – levando em consideração, por exemplo, falha do sistema de informática; falha de equipamentos; interrupção por parte dos fornecedores; perda de pessoal; etc.

Na análise do impacto no negócio (*business impact analysis* – BIA), procura-se identificar, quantificar e qualificar o impacto de perdas, interrupções ou distúrbios nos processos da organização e fornecer dados para definir a estratégia da continuidade. Contempla a identificação e compreensão dos objetivos críticos e os respectivos critérios de sucesso; a definição

dos tempos máximos de interrupção tolerável (*maximum tolerable outage* – MTO); a definição dos objetivos para os pontos de recuperação (*recovery point objective* – RPO); o delineamento das dependências internas e externas para se atingir os objetivos críticos; a identificação dos impactos que podem resultar em perdas de reputação ou financeira; etc.

A avaliação de risco, então, deve ser conduzida conforme a estratégia de gerenciamento de risco da organização e tem como propósito identificar e avaliar as probabilidades de ocorrência das ameaças e dos respectivos impactos. A avaliação deve focar, dentre as que podem causar interrupção do negócio, nas funções mais críticas identificadas na BIA e pode usar técnicas como FTA; ETA; matriz de risco; análise custo-benefício; etc.

No segundo estágio, procura-se estabelecer as estratégias do BCM no âmbito da organização, dos processos e dos recursos.

O propósito da definição da estratégia do BCM na organização é esclarecer e documentar a política, a estrutura do trabalho e as diretrizes operacionais para garantir a continuidade da organização. A estratégia do BCM contempla: a seleção de alternativas a serem utilizadas, caso haja uma interrupção, para manter ativos os processos críticos identificados na BIA e suas dependências (internas e externas); e proteger das vulnerabilidades e das falhas de primeira ordem identificados na avaliação de risco.

A estratégia no nível de processo objetiva definir a estratégia para manter a continuidade dos processos e elaborar o planejamento para o projeto de sua implementação.

A estratégia de recuperação de recursos, por sua vez, tem como propósito coordenar e fornecer um nível pré-determinado de recursos para permitir a implementação das estratégias no nível de processo e da organização.

Uma vez estabelecidas as estratégias, pode-se elaborar uma resposta para a gestão da continuidade do negócio – terceiro estágio. Para tanto, preveem-se planos de gerenciamento de crise, de continuidade do negócio e de reativação da unidade de negócio, quais sejam:

1. **Plano de gerenciamento de crise:** Visa fornecer à equipe de gerenciamento de crise 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. Ele contempla todo tipo de crises, incluindo aquelas que não foram previstas no BCM, tais como crises que não resultem na interrupção do negócio ou que tenham proporções além do escopo do BCM.
2. **Plano da continuidade do negócio:** Tem como propósito fornecer uma estrutura de trabalho e procedimentos que possibilitem a recuperação de todos os processos do negócio

dentro do MTO.

3. **Plano de reativação da unidade de negócio:** Objetiva estruturar a resposta de cada departamento às interrupções.

O quarto estágio objetiva desenvolver a cultura do BCM na organização. Primeiramente é feita a avaliação da conscientização, que tem como propósito avaliar o nível atual e o desejável de conscientização – além de definir quais áreas devem ser alvo de campanhas e como a campanha pode ser executada com eficiência. A avaliação da conscientização envolve o levantamento do nível atual de conscientização sobre BCM; especificação do nível desejado e métricas para avaliá-lo; e identificação da natureza e do escopo das lacunas de treinamento que devem ser preenchidas pelas campanhas.

Assim, com base nas lacunas identificadas, delineia-se o programa de educação, treinamento e conscientização (*educations, training and awareness* – ET&A), a fim de desenvolver a cultura do BCM. O pessoal sem uma específica responsabilidade no BCM pode se ater somente à conscientização ou a um nível de proficiência pré-estabelecido de como proceder nas tarefas gerais da organização. Já os participantes devem receber um treinamento estruturado que implemente habilidades, competência (colocando em prática o BCM) e conhecimento necessário.

Por fim, monitoram-se as mudanças culturais, a fim de avaliar se a qualidade e a eficácia da campanha de ET&A está adequada. Faz parte dessa fase avaliar opiniões sobre cada treinamento; monitorar a eficácia da campanha (tanto curto-prazo quanto longo); e monitorar periodicamente a conscientização.

O quinto estágio refere-se à auditoria, manutenção e prática do BCM.

O BCM não pode ser considerado confiável até que sejam feitos os exercícios que visam avaliar a competência do BCM; identificar áreas que necessitam de aprimoramento ou informações; destacar pressuposições que precisem ser questionadas; fornecer informação e confiança aos participantes do exercício; desenvolver uma equipe de trabalho; aumentar o nível de conscientização da organização com exercícios públicos; etc.

A manutenção do BCM, por sua vez, objetiva garantir que o BCM se mantenha efetivo, apesar das mudanças internas e externas, o que resulta em um programa de manutenção e monitoramento que orienta as circunstâncias de se fazer as revisões. Os relatórios de cada processo de manutenção devem ser assinados pelos gestores apropriados.

Finalmente, a auditoria visa avaliar a conformidade com normas (internas e externas) e a política do BCM – além de revisar as soluções adotadas no BCM; validar os planos de continuidade do negócio; verificar se os exercícios e as atividades de manutenção estão sendo adequa-

damente executados; e destacar deficiências e problemas, garantindo as respectivas soluções.

3.6 Gestão de risco no setor elétrico brasileiro

Dias et al. (2000) apresentam um estudo junto às principais usinas geradoras de energia elétrica do país, a fim de fazer um diagnóstico dos procedimentos de operação e manutenção delas. Foi analisado um conjunto de 36 usinas hidrelétricas e 5 usinas termelétricas, selecionadas pela potência instalada, superior a 500 MW, ou pela sua importância na operação do sistema. Os autores constataram que 11% do número total de itens das listas de verificações apresentavam não-conformidades, sendo que os maiores percentuais foram referentes aos planos de segurança da planta (76%), aos planos de ações de emergência (49%) e aos planos contingenciais de cheias (38%). Estas não-conformidades referentes à inexistência ou inadequação dos planos totalizam 69% das não-conformidades identificadas. Os itens referentes às instruções e normas correspondem a 14% do total de não-conformidades; recursos humanos, treinamento e manuais operativos, a 6%; e restabelecimento autônomo a 11% (1% referente ao grau de automação e 10% à manobra de restabelecimento autônomo – *black start*). Os autores destacam que estes últimos procedimentos "[...] estão diretamente relacionados com a operação cotidiana da planta e influenciam diretamente o índice de disponibilidade, possuindo portanto uma importância significativa [...] " e que os planos de segurança da planta, de ações emergenciais e contingenciais de cheias são "[...] considerados de alta importância estratégica para o setor de energia elétrica." Dias et al. (2000, p. 13).

Diante dos resultados desta pesquisa, ficou evidenciada a carência do setor de geração por uma metodologia que tratasse estes assuntos – sendo um dos motivadores para este trabalho de doutorado.

Esta situação confirmou-se em uma pesquisa, realizada neste trabalho de doutorado, junto a duas empresas do setor de energia que mantêm programas de gerenciamento de risco (uma geradora, transmissora e distribuidora; e outra geradora). Nos dois casos, os respectivos programas foram implementados pelo esforço de suas equipes, ponderando o que deviam fazer – já que não dispunham de uma metodologia para isso.

As pesquisas foram realizadas por meio de entrevistas "não estruturadas" – em que todos os participantes puderam questionar e opinar – e por observação, no ambiente de trabalho.

A segunda empresa é uma usina hidrelétrica de grande porte e teve seu plano de contingência de cheias elaborado em 1984. Por muitos anos, existiu a intenção de realizar uma análise de outros incidentes. No entanto, somente em 1995 – após a ocorrência de um incidente, ficou

evidenciada a falta de preparação adequada da equipe, e foi criada uma comissão para elaborar os planos de ação emergencial.

De acordo com um dos entrevistados, o apoio da alta gerência foi extremamente importante nesse momento, para conseguir o comprometimento das áreas, liberando os colaboradores para os trabalhos, e também para analisar o investimento de cada ação. Em 2001, foi constituída uma comissão permanente para gerenciamento das ações para minimização dos riscos e efeitos de contingências críticas na usina. Na data da visita técnica (31 de maio de 2007), existiam 12 planos de ações emergenciais na usina.

Na primeira empresa, no que se refere à geração, foi destacado que, desde a década de 80, existe a preocupação de se aprender com a análise dos incidentes ocorridos (com a visão de que não poderia ocorrer mais o mesmo incidente), e que, aproximadamente em 1990, foram feitas videoconferências para discutir os incidentes que ocorreram (participavam da videoconferência responsáveis de todas as usinas). Em torno do ano 2000, foram realizados planos de emergência, começando pelo de rompimento de barragem. Sendo que, por volta de 2003, já tinham sido elaborados planos de forma proativa, não apenas de incidentes que já tinham ocorrido. Na data da visita (15 de março de 2006), existiam de 12 a 15 planos de ações emergenciais (PAE) por usina e 7 ou 8 por PCH.

Quanto à transmissão e distribuição, houve uma reestruturação dos centros de operação da distribuição (COD), reduzindo o número de centros e mantendo a estrutura de um *call center* por COD.

Com esta reestruturação, foi possível manter instalações desativadas para funcionar como *hot-site*[12]. A arquitetura do sistema permite, ainda, trabalhar por transbordo[13] e fazer a distribuição de serviços na área de responsabilidade de um COD, por outro – o que caracteriza redundância ativa. Adicionalmente, existe um revezamento entre os operadores de cada mesa (que são as áreas de atuação das equipes) para que, "em uma contingência", se possa operar com 2 equipes em uma mesma área – isso é feito particionando a mesa em duas, uma subárea para cada equipe.

A comunicação entre os colaboradores no campo e o COD também é redundante, pois se trata de recurso crítico para a garantia da continuidade operacional do COD.

Por fim, salienta-se que as duas empresas pesquisadas dedicam-se ao aprimoramento do

[12]São instalações completas, prontas para operar, caso ocorra a interrupção do negócio na instalação original – por exemplo, um *Call Center* redundante. Isso inclui equipamentos, móveis, instalações, e outros itens necessários para a operação.

[13]É a transferência de serviço de uma unidade para outra, quando a primeira teve o limite de sua capacidade atingido.

programa de gerenciamento de risco e fazem, periodicamente, simulações dos planos e revisão do que foi estabelecido.

É interessante destacar que, em uma visita técnica a uma distribuidora na Espanha, realizada em 02 outubro de 2008, foram identificadas práticas equivalentes às identificadas na distribuidora pesquisada, no que se refere ao transbordo, à redundância da comunicação, à disponibilidade de *hot site* e à redundância ativa de instalações.

Destaca-se, ainda, que parte da metodologia desenvolvida no presente trabalho foi aplicada em uma distribuidora, no caso a Celesc (Centrais Elétricas de Santa Catarina S.A.), e em uma transmissora, a Eletrosul Centrais Elétricas S.A., conforme descrito no Capítulo 6. Nos dois casos, pode-se confirmar a carência de uma metodologia para o gerenciamento de risco no setor elétrico.

Esta carência de uma metodologia levou empresas a desenvolverem suas próprias formas de trabalhar. Lefevre et al. (2001), por exemplo, apresentam os passos seguidos na implementação do sistema de gerenciamento na Usina Hidroelétrica Binacional ITAIPU, conforme listado a seguir.

1. **Identificação das possíveis contingências:** Este trabalho baseia-se na experiência dos membros da comissão, suportada pela equipe técnica.
2. **Avaliação sucinta do risco e das consequências de cada contingência:** Essa atividade é fundamental para definição de prioridades para a análise das contingências, uma vez que o número de itens levantados exigiriam muito tempo de trabalho para que se analisem todos.
3. **Estabelecimento dos grupos de análise:** Com base na lista de prioridade elaborada no item anterior, formam-se grupos de estudos – um para cada contingência.
4. **Missão de cada grupo de análise:** Cada grupo analisa, com profundidade, cada contingência. Na análise, deve-se verificar se o risco é real ou se medidas estruturais podem minimizar, ou até eliminar, a probabilidade de ocorrência. Também é tarefa do grupo examinar as ações para mitigar as consequências. Finalmente, é de responsabilidade do grupo a elaboração do Plano de Ações que devem ser tomadas no caso de a contingência ocorrer.
5. **Envolvimento dos colaboradores:** Ficou decidido que, antes de ser considerado concluído, o plano deve ser submetido a uma apresentação aberta às áreas técnicas da Itaipu. Esta medida permitiu uma considerável contribuição dos profissionais que não participaram do grupo de estudo. À parte desta apresentação, todas as recomendações ou decisões apresentadas que incorram em grande custo são objetos de avaliação da superintendência

ou até da diretoria da corporação.

6. **Treinamento:** É considerada fundamental a prática de simulações do combate às contingências. Assim, periodicamente, são programadas simulações. A experiência mostra que a análise dos resultados dessas simulações geram importantes ajustes no plano e melhoram o treinamento para a aplicação deles.
7. **Natureza permanente do PAE:** Mesmo quando os estudos de todas as contingências, até então identificadas, tenham sido concluídos, é fundamental que a comissão permaneça. Isto é: ela deve ser de natureza permanente para tratar adequadamente novas contingências que sejam identificadas.
8. **Revisão da metodologia:** Muito do trabalho é feito com base na experiência e no senso comum. Um estudo sobre metodologias está sendo realizado para verificar se uma abordagem mais científica pode ser incorporada às práticas presentes.

3.7 Considerações finais

Ao longo do Capítulo 3, foram apresentadas algumas abordagens de gestão de risco.

Observou-se que as metodologias de gerenciamento de risco vêm sendo desenvolvidas principalmente nos últimos 50 anos, especialmente nos 15 últimos, quando atingiu um nível de maturidade maior – no entanto, somente a partir de 2000 foi possível consolidar regras e normas.

Quanto ao BCM, concluiu-se que ele não se restringe aos sistemas de informações e inclui medidas de monitoramento e controle; de resposta emergencial; de operação alternativa; e de retorno à situação normal.

De fato, Karakasidis (1997) constatou que tanto os profissionais atuantes em recuperação de desastres (para sistemas de tecnologia de informação) quanto os atuantes em recuperação de negócios (para atividades principais do negócio) concordam que recuperar os sistemas de informação não assegura a sobrevivência do negócio. Essa lição aprendida na vida real, de acordo com o autor, acarretou uma inundação de metodologias de contingências, ferramentas, serviços de consultorias, etc., além de um constante refinamento dos processos e metodologias utilizadas pelos auditores – a fim de assegurar que as perguntas corretas estejam sendo feitas na execução de revisões de planos, estruturas de trabalho, estratégias, recomendações, políticas e normas.

O Quadro 3.1 compara a estrutura de algumas metodologias de gerenciamento de risco, tanto abordagens gerais quanto relativas à segurança ou à continuidade. É interessante observar

que, apesar de estruturadas de forma diferente, os pontos abordados são muito próximos do que propõe a norma ABNT ISO/IEC Guia 73, que divide a gestão de risco em: análise / avaliação de risco; tratamento do risco; aceitação do risco; e comunicação do risco.

Quadro 3.1: Comparativo entre algumas metodologias de gerenciamento de risco

Fontes	**Foco**	**Processo**
ABNT (2005) – ABNT/ISO/IEC Guia 73.	Geral.	– Análise / avaliação de risco. – Tratamento do risco. – Aceitação do risco. – Comunicação do risco.
ABNT (2001) – ABNT/ISO/IEC 17799.	Continuidade.	– Entender os riscos a que a organização está exposta. – Identificar e priorizar os processos críticos. – Avaliação do impacto das interrupções. – Objetivos do negócio (MTO, RPO, etc.). – Estratégia da continuidade. – Planos da continuidade. – Testar e atualizar. – Incorporar BCM à estrutura da organização.
BCI (2005).	Continuidade.	– Política do BCM. – Gerenciamento do programa. – Preparação e resposta a incidentes. – Estratégia da organização. – Análise do impacto no negócio (BIA). – Avaliação de risco. – Estratégia do BCM da organização. – Estratégia no nível de processo. – Estratégia de recuperação de recursos. – Plano de gerenciamento de crise. – Plano de continuidade. – Plano de reativação da unidade de negócio. – Avaliação da conscientização. – Desenvolvendo a cultura. – Monitoração de mudanças culturais. – Exercícios. – Manutenção. – Auditoria.

(continua na próxima página)

Quadro 3.1: Comparativo entre algumas metodologias de gerenciamento de risco

(continuação)

Fontes	**Foco**	**Processo**
Botha & Von Solms (2004).	Continuidade.	– Planejamento do projeto. – Análise do impacto no negócio (BIA). – Estratégia da continuidade. – Implementação da estratégia da continuidade. – Treinamento da continuidade. – Testes da continuidade. – Manutenção do Plano de continuidade. – As fases anteriores devem ser aplicadas aos 4 ciclos: ciclo de cópias de segurança; ciclo de recuperação de desastre; ciclo de planejamento de contingência; ciclo de planejamento de continuidade.
Cooper (2004) – SAA AS/NZS 4360:2004.	Segurança.	– Estabelecer o contexto. – Identificar o risco. – Analisar o risco. – Avaliar o risco. – Tratar o risco. – Monitoramento e revisão. – Comunicação e consulta.
EUROCONTROL (2004).	Segurança.	– Análise / avaliação do perigo funcional (FHA). – Análise / avaliação preliminar de segurança do sistema. – Análise / avaliação de segurança do sistema.
Karakasidis (1997).	Continuidade.	– Aprovação da alta gerência. – Comitê de planejamento da continuidade. – Análise do impacto no negócio (BIA). – Avaliar necessidades críticas. – Estratégia da continuidade e processos de recuperação. – Aprovação pelos executivos do plano de implementação. – Elaborar o plano de recuperação. – Elaborar os procedimentos e critérios dos testes. – Testar os processos de recuperação. – Consensar os níveis de serviço. – Atualizar / revisar os padrões e procedimentos.

(continua na próxima página)

Quadro 3.1: Comparativo entre algumas metodologias de gerenciamento de risco
(continuação)

Fontes	**Foco**	**Processo**
Kranidiotis (2001).	Segurança.	– Identificação dos perigos do risco. – Identificação das pessoas afetadas pelos perigos. – Avaliação do risco. – Definição de medidas de segurança. – Documentação e revisão da avaliação.
Kumamoto & Henley (1996).	Segurança.	– Identificar o risco. – Gerar o perfil do risco das combinações de controles ativos e passivos. – Avaliar os perfis e tomar decisão adequada.
NASA (2002b), NASA (2004b), NASA (2004a).	Segurança.	– Identificação dos riscos. – Análise dos riscos. – Planejamento de risco. – Rastreamento do risco. – Controle do risco. – Documentação e comunicação.
Lefevre et al. (2001).	Geral.	– Identificação das possíveis contingências. – Avaliação sucinta do risco e das consequências de cada contingência. – Estabelecimento dos grupos de análise. – Missão de cada grupo de análise. – Envolvimento dos colaboradores. – Treinamento. – Natureza permanente do PAE. – Revisão da metodologia.
SAE (1996) – SAE ARP 4761.	Segurança.	– Análise / avaliação do perigo funcional (FHA). – Análise / avaliação preliminar de segurança do sistema. – Análise / avaliação de segurança do sistema.
Saldanha (2000).	Continuidade.	– Avaliação do impacto (BIA). – Avaliação do grau de exposição. – Definição da estratégia da continuidade. – Plano de monitoramento e controle. – Plano de resposta emergencial. – Plano de contingência. – Implementação. – Testes. – Manutenção.

No entanto, destaca-se a preocupação, das metodologias de gerenciamento de continuidade, de compreender a organização, antes de iniciar a análise de risco. BCI (2005), por exemplo, procura identificar os valores da organização e alinhar o gerenciamento da continuidade ao

planejamento estratégico da organização. Já Karakasidis (1997) destaca o apoio dos executivos para viabilizar o BCM, que também é abordado por todas as metodologias de gerenciamento da continuidade – no entanto, não destacam em um tópico específico, mas apresentam esta informação ao longo do texto.

No que se refere à análise de risco, observou-se que, na gestão de continuidade, normalmente é chamada de BIA e está associada à identificação dos processos críticos. Note-se que Saldanha (2000) divide a análise de risco em BIA e avaliação do grau de exposição.

Quanto ao processo de comunicação do risco, destaca-se a identificação da necessidade de se construir uma cultura de continuidade – apresentada em BCI (2005) e Saldanha (2000). Essa necessidade também é uma característica fundamental no gerenciamento de segurança e deve abranger toda a organização, conforme destacado por Kumamoto & Henley (1996).

De fato, Kumamoto & Henley (1996) propõem, como estratégia de tratamento, o aprimoramento da qualidade das práticas da empresa para diminuir o risco e alcançar uma cultura do risco – política também adotada por outras metodologias, tais como TapRoot (PARADIES; UNGER, 2000).

De acordo com o documento 75-INSAG-3 do International Nuclear Safety Advisory Group (IAEA, 1999), a cultura de segurança é crucial para o gerenciamento de risco.

Outro ponto relevante é o fato de a NASA (2004a) levar em consideração a existência de planos de contingência na tomada de decisão de aceitar ou não o risco.

Já a norma SAA AS/NZS 4360:2004 inclui, no tratamento dos riscos identificados, a elaboração de planos de contingência para fazer a recuperação, caso o incidente ocorra (COOPER, 2004).

É interessante destacar que, nas metodologias de gestão da continuidade, não há distinção entre o tratamento do risco e o planejamento ativo do risco aceito. Possivelmente, isto tem origem na recuperação de desastre, que tem seu foco no pós-incidente. Assim, na definição das estratégias, são consideradas tanto medidas para a redução do risco (ou até evitá-lo), quanto para o planejamento referente aos riscos aceitos.

Destaca-se, ainda, o fato de o BCI (2005) trazer a necessidade de se criar um plano de gerenciamento de crises que fogem do escopo do plano de continuidade, que incluem, por exemplo, uma exposição negativa na mídia causada por um incidente – mesmo que não tenha ocorrido interrupção nos processos críticos do negócio.

Note-se que as metodologias de gestão de continuidade, adicionalmente às quatro fases propostas na ABNT ISO/IEC Guia 73, trazem a preocupação de revisar o processo de geren-

ciamento para que ele se mantenha atualizado e se possam fazer melhorias – que também é evidenciada na gestão da segurança por Kranidiotis (2001), na norma SAA AS/NZS 4360 (COOPER, 2004), e pela NASA (2002b), NASA (2004b), NASA (2004a).

De fato, além de poderem ser estruturadas da mesma forma, a gestão de segurança e a de continuidade interagem em vários aspectos.

Saldanha (2000), por exemplo, salienta que, ao identificar a criticidade de um processo ou serviço, deve-se considerar a possibilidade de colocar em risco a segurança dos funcionários e terceiros e que, em situações de risco, a prioridade é a segurança dos funcionários, clientes, visitantes e fornecedores.

A ABNT ISO/IEC 17799 (ABNT, 2001), que é uma norma de segurança da informação, acrescenta que os procedimentos de emergência – a serem executados após a ocorrência do incidente – devem contemplar ações para preservar as operações do negócio e / ou vidas humanas.

Para Savage (2002), deve-se incluir, no plano de continuidade, procedimentos de saúde e segurança.

Karakasidis (1997), por sua vez, complementa indicando que a continuidade de negócio deve ser usada em conjunto com um programa de gerenciamento de risco mais abrangente.

Na visão de Kumamoto & Henley (1996), a segurança é fundamental para a existência da continuidade da organização.

Apesar desta interação entre o gerenciamento de segurança e de continuidade, alguns autores os consideram distintos. BCI (BCI, 2005), por exemplo, discute algumas diferenças entre gerenciamento de segurança e gerenciamento de continuidade. Dentre outras, o fato de o primeiro fazer uso de parâmetros de impacto e probabilidade e, o segundo, de impacto e tempo (cronologia).

É interessante observar que é comum, na gestão da segurança, agregar outros parâmetros no perfil do risco. Kumamoto & Henley (1996), por exemplo, incorporam a população afetada e o cenário causal no perfil do risco, sendo que este último considera a cronologia dos eventos. Portanto, não se restringindo ao impacto e à probabilidade, que normalmente são tratados como severidade e probabilidade pelos gestores de segurança. De fato, modelos cadeia causal normalmente são cronologicamente estruturados.

Ademais, ao se verificar a necessidade de desenvolver técnicas como FTA dinâmico, ESD dinâmico, entre outras, fica evidente a necessidade de considerar a variável tempo na gestão de segurança, bem como recomenda-se considerar probabilidades na gestão da continuidade, para possibilitar uma análise de custo-risco-benefício dos investimentos a serem feitos pela

organização.

Neste sentido, alguns autores apresentam recomendações que associam os conceitos de segurança e continuidade, tais como:

1. a BIA deve ser conduzida conforme a estratégia de gerenciamento de risco da organização (BCI, 2005);
2. deve-se trabalhar as vulnerabilidades da organização como um todo, para reduzir os danos e perdas por perigos naturais (WEICHSELGARTNER, 2001);
3. se a prevenção completa for aceita como absolutamente inatingível, a abordagem de desastres para a continuidade resulta em uma política de redução de risco a longo prazo (WEICHSELGARTNER, 2001); e
4. um dos requisitos para o BCM deve ser fomentar um programa de redução de riscos, para assegurar que as ameaças da organização serão adequadamente identificadas e avaliadas (KARAKASIDIS, 1997).

No entanto, nenhuma das metodologias apresentadas integra, de maneira estruturada, os conceitos de continuidade e de segurança. No Capítulo 5, está delineada a metodologia desenvolvida – foco deste trabalho de doutorado –, que visa atender a essa necessidade.

É fato que todo sistema técnico tem uma função a desempenhar. Esta função, então, contribui para a operação da organização. Apesar de todo sistema técnico ser portador de perigo, a sociedade está disposta a correr o risco de um incidente para ter o benefício adquirido pela operação da organização.

Desta forma, para a sociedade, a relação custo-risco-benefício se dá pelo aporte que ela faz na organização (seja pela aquisição de seus produtos / serviços, por subsídio, por financiamento, ou qualquer outra forma de favorecimento), pelo risco de dano à sociedade em confronto com os benefícios advindos da manutenção da operação da organização.

A organização, por sua vez, fornece produtos / serviços em troca de remuneração. Desta forma, cria-se um laço de dependência entre as partes: organização e sociedade.

Assim, a sociedade incorre em dois riscos: de um incidente gerar dano a ela ou interromper a operação da organização, isto é, riscos relativos à segurança e à continuidade.

Por fim, destaca-se que ainda não existe um consenso quanto à terminologia utilizada na gestão de risco quanto à segurança, nem na gestão de risco quanto à continuidade, tampouco entre elas – conforme discutido no Capítulo 2.

De fato, os gerenciamentos de risco à segurança e à continuidade abordam situações simi-

lares, mas de forma diferente e com designação distinta. O Quadro 3.2 ilustra este ponto: nele está apresentado um comparativo entre a nomenclatura utilizada no gerenciamento de segurança e no de continuidade para designar as atividades típicas, a serem realizadas no período anterior e posterior a um caso de incidente.

Contudo, observa-se que as metodologias para gerenciamento de riscos destes dois atributos estão convergindo, apesar de ainda não se ter uma que formalmente integre os atributos segurança e continuidade.

Quadro 3.2: Designações relativas à aceitação do risco, utilizadas na gestão de continuidade e de segurança

Continuidade	**Segurança**	**Comentários**
Monitoramento & controle	Prevenção do incidente	Nos dois casos, o objetivo é monitorar os distúrbios que possam causar a falha. Para o gerenciamento de segurança, a preocupação é a integridade das pessoas e do meio ambiente; para o gerenciamento da continuidade, é a manutenção das funções críticas (mas sem comprometer a segurança)
Resposta emergencial	Gestão do incidente	Assim como a resposta emergencial, a gestão do incidente também procura minimizar os danos do incidente. Mais uma vez, a diferença está no foco de cada: a primeira se preocupa em minimizar o impacto às funções críticas (sem comprometer a segurança), e a segunda, em manter a segurança.
Operação alternativa	Gestão do incidente	Não são usuais, em sistemas técnicos industriais, algumas soluções adotadas para sistemas de informações, tais como local redundante (*hot site*). No entanto, a prática de redundância é comum para equipamentos e instalações menores.
Retorno	—	Como a grande preocupação do gerenciamento de segurança é o dano ao homem e ao meio, normalmente não existe um planejamento para retorno às operações normais de operação.

4 *Principais técnicas usadas para dar suporte à metodologia de gerenciamento de risco*

Tanto o gerenciamento de segurança quanto o de continuidade fazem uso de técnicas de suporte às respectivas metodologias, a fim de modelar a realidade e estruturar o conhecimento. Existem inúmeras técnicas de modelagem para gerenciamento de risco – EUROCONTROL (2004) e Everdij & Blom (2008) apresentam uma listagem de centenas delas, indicando a época de origem e as características principais de cada uma.

A seguir, será apresentada uma breve descrição das que foram consideradas mais relevantes para a metodologia de gerenciamento de risco desenvolvida e apresentada no Capítulo 5, que são: IDEF0; redes bayesiana; atualização bayesiana; FTA; ETA; ESD; FHA; FMECA; BTA e CNEA. Isto não significa que outras técnicas não possam ser utilizadas – RBD (*reliability block diagram*) ou HAZOP, por exemplo, podem ser utilizadas para auxiliar na identificação de incidentes. Por fim, na Seção 4.10, destaca-se como as técnicas apresentadas estão associadas à metodologia desenvolvida.

Para uma leitura mais aprofundada, sugere-se a bibliografia referenciada no Quadro 4.1[1].

Quadro 4.1: Referências bibliográficas recomendadas

Técnica de suporte	**Documento NeDIP**	**Outras referências sugeridas**
Atualização bayesiana	NE-RE-06	Droguett & Mosleh (2000); Calil et al. (2005); RAC (2003); Kapur & Lamberson (1977); Gill (2002).
Redes bayesianas	NE-RE-06	Pearl (1988); Jensen (2001); Boerlage (1994).

(continua na próxima página)

[1] Os documentos NeDIP estão disponíveis no sítio do núcleo na internet: <www.nedip.ufsc.br>.

Quadro 4.1: Referências bibliográficas recomendadas

(continuação)

Técnica de suporte	Documento NeDIP	Outras referências sugeridas
Análise por árvore de falha (FTA)	NE-RE-03	Sakurada (2001); USA/NRC (1981); NASA (2002a); Ericson II (2005); Leveson (1995).
Análise por árvore de eventos (ETA)	NE-RE-01	Papazoglou (1998); Kumamoto & Henley (1996); Ericson II (2005); Leveson (1995).
Diagrama sequencial de eventos (ESD)	———	NASA (2002b); Swaminathan & Smidts (1999).
IDEF0	NE-RE-04	NIST (1993); Presley (1997).
Análise / avaliação dos perigos funcionais (FHA)	———	EUROCONTROL (2006), Ericson II (2005); Leveson (1995).
Análise do modo de falha, efeitos e criticidade (FMECA)	NE-RE-02	Sakurada (2001); SAE (2002); USA/DOD (1980); STAMATIS (1995); ECSS (2001).
Análise *bow-tie* (BTA)	———	Lewis & Hurst (2005); GOVERNORS (2005); Ramzan (2006); Trbojevic (2004).
Análise de eventos por rede causal (CNEA)	NE-RE-05	———

4.1 IDEF0

IDEF0 (*integration definition for function modeling*) é uma técnica para dar suporte à modelagem de decisões, ações e atividades (PRESLEY, 1997). A ideia do IDEF0 é representar graficamente o funcionamento do objeto de estudo. Esta técnica é baseada em uma linguagem gráfica consolidada – a *structured analysis and design technique* (SADT), desenvolvida nos anos 70 (PRESLEY, 1997) – e objetiva facilitar a análise e a comunicação das funções estudadas (NIST, 1993).

Como ferramenta de análise, o método auxilia na identificação das funções executadas, o que se necessita para executá-las, o que o sistema atual faz corretamente e o que o sistema atual faz de errado (NIST, 1993). Como ferramenta de comunicação, o método possibilita aprimorar o conhecimento e trazer consenso quanto à função do sistema.

Os componentes da sintaxe do IDEF0 são caixas, setas, regras, diagramas, textos e glossário – como ilustrado na Figura 4.1.

As caixas representam funções – definidas como atividades, processos ou transformações – que podem ser detalhadas em caixas de nível inferior (subfunções). O código da função

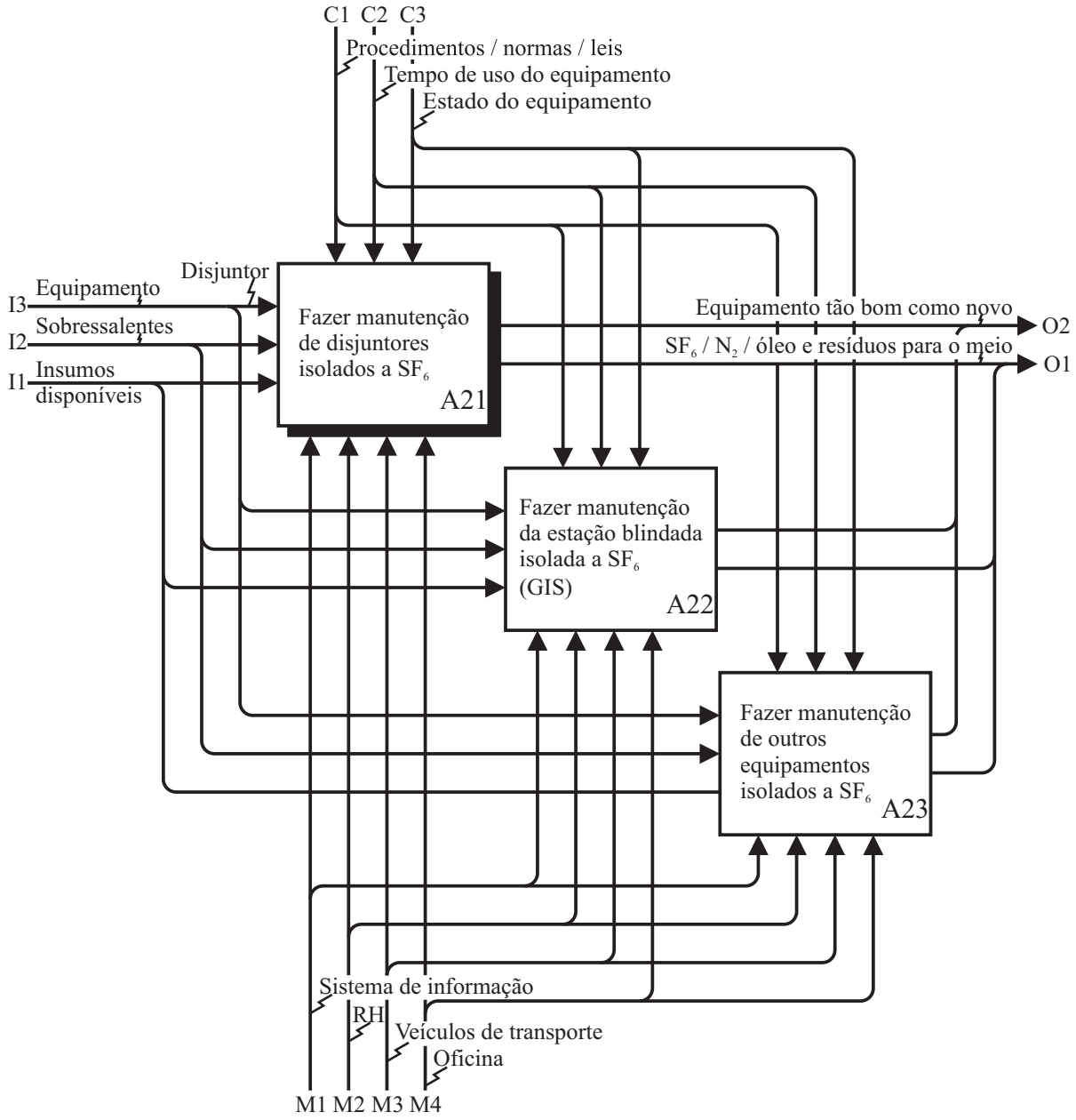


Figura 4.1: Exemplo de IDEF0 da função "Fazer manutenção de equipamentos isolados a SF_6"
Fonte: MT-PR-RT-NE-01 (UFSC/NEDIP, 2008j, Apêndice A, p. 21)

principal deve ser 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.

As setas são dados ou objetos relacionados às funções a serem executadas. As setas de entrada 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 devem ser conectadas no lado de cima de uma caixa. As setas de mecanismo definem os meios ou ferramentas através

dos quais será exercida a função especificada pela caixa, devem apontar para cima e devem ser conectadas no lado de baixo da caixa.

As regras de sintaxe definem como os componentes são utilizados, e os diagramas, que são a principal parte do IDEF0, fornecem o formato para descrever o modelo graficamente. 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. (NIST, 1993).

4.2 Abordagem bayesiana

Reverendo Thomas Bayes nasceu em Londres, em 1702, e era um matemático amador. Faleceu em 1761, em Tunbridge Wells – também na Inglaterra (O'CONNOR; ROBERTSON, 2004).

Seu texto mais ilustre, *Essay Towards Solving a Problem in the Doctrine of Chances*[2], 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. Este, por sua vez, foi apresentado, em 1774, por Pierre-Simon Laplace, no texto "Mémoire sur la Probabilité des Causes par les Événements" (FIENBERG, 2006).

O teorema de Bayes fundamenta-se na teoria de probabilidade condicional e é a base para a atualização bayesiana e para as redes bayesianas.

Para dois dados eventos A e B, pode-se apresentar o teorema pela equação a seguir:

$$P(B|A) = \frac{P(A|B).P(B)}{P(A)} \tag{4.1}$$

Onde,

- $P(A|B)$ é a probabilidade de ocorrer o evento A, dado que ocorreu o evento B;
- $P(B|A)$ é a probabilidade de ocorrer o evento B, dado que ocorreu o evento A;
- $P(A)$ é a probabilidade de ocorrer o evento A; e
- $P(B)$ é a probabilidade de ocorrer o evento B.

[2] A University of York, no Reino Unido, disponibiliza uma cópia do ensaio de Bayes no endereço eletrônico: <http://www.york.ac.uk/depts/maths/histstat/essay.pdf>

4.2.1 Atualização bayesiana

Tradicionalmente, divide-se o "mundo" da estatística em dois campos: a estatística clássica e a estatística bayesiana. Em síntese, o que diferencia estas duas abordagens é o fato de a estatística clássica tratar os parâmetros das distribuições como valores definidos – fixos, enquanto a estatística bayesiana considera os parâmetros do modelo estatístico como variáveis aleatórias, com uma própria distribuição probabilística (RAC, 2003).

A análise estatística clássica procura inferir sobre os dados coletados. No entanto, não leva em consideração, na análise, informações anteriores – exceto para sugerir a escolha de um modelo de população para "ajustar", aos dados, e esta escolha é posteriormente checada contra os dados coletados para verificar se ela foi razoável .

Por outro lado, na abordagem bayesiana, utilizam-se informações anteriores – até mesmo julgamentos subjetivos – para construir um modelo da distribuição *a priori* do parâmetro da distribuição estudada, conforme apresentado na expressão matemática a seguir:

$$f(\theta|x) = \frac{f(x|\theta).f(\theta)}{f(x)} \tag{4.2}$$

Onde,

- $f(\theta|x)$ é a distribuição *a posteriori* do parâmetro θ;
- $f(\theta)$ é a distribuição *a priori* do parâmetro θ; e
- $f(x|\theta)$ é a função verossimilhança.

Que pode ser lida – omitindo o denominador do lado direito da equação, já que ele não depende de "θ" – como: a distribuição "*a posteriori*" é proporcional à "verossimilhança" multiplicada pela função "*a priori*" (EHLERS, 2005).

Este modelo é a avaliação inicial de quão provável são os vários valores do parâmetro. Então, faz-se uso dos dados observados (pela função verossimilhança) para revisar a avaliação inicial, chegando ao chamado modelo de distribuição *a posteriori* para a população do parâmetro modelado (NIST/SEMATECH, 2003). Em outras palavras, o lado esquerdo da equação corresponde à representação matemática da pergunta: o que se pode dizer sobre o parâmetro θ, dadas as informações disponíveis "x", e o lado direito é o mecanismo de inferência para responder a esta questão (DROGUETT; MOSLEH, 2000).

Para obter um valor representativo do parâmetro, pode-se fazer uso de estatísticas e calcular o valor esperado da função *posteriori*, e o "estimador bayesiano" pode ser alcançado por

(KAPUR; LAMBERSON, 1977):

$$\hat{\theta} = E(\theta|x) = \int_{-\infty}^{\infty} \theta . f(\theta|x) . d\theta \tag{4.3}$$

4.2.2 Redes bayesianas

Redes bayesianas são grafos acíclicos direcionados (DAG - *directed acyclic graph*). Grafos direcionados, pois são representações gráficas em que nódulos representam as variáveis, arcos direcionados representam a existência de uma influência direta entre as variáveis, e probabilidades condicionais expressam a intensidade desta influência (PEARL, 1988). Acíclicos, pois não pode existir um caminho $A_1 \rightarrow \cdots \rightarrow A_n$ em que $A_1 = A_n$ (JENSEN, 2001); isto é: não existe um caminho que comece e termine no mesmo nódulo.

As redes bayesianas são modelos que procuram representar a realidade, podendo inferir a probabilidade de um ou mais eventos, dada a observação de alguma evidência.

O exemplo ilustrado pela Figura 4.2 refere-se à probabilidade de um sistema falhar (ou se manter em operação), baseando-se no estado de cinco componentes: A, B, C, D e E[3].

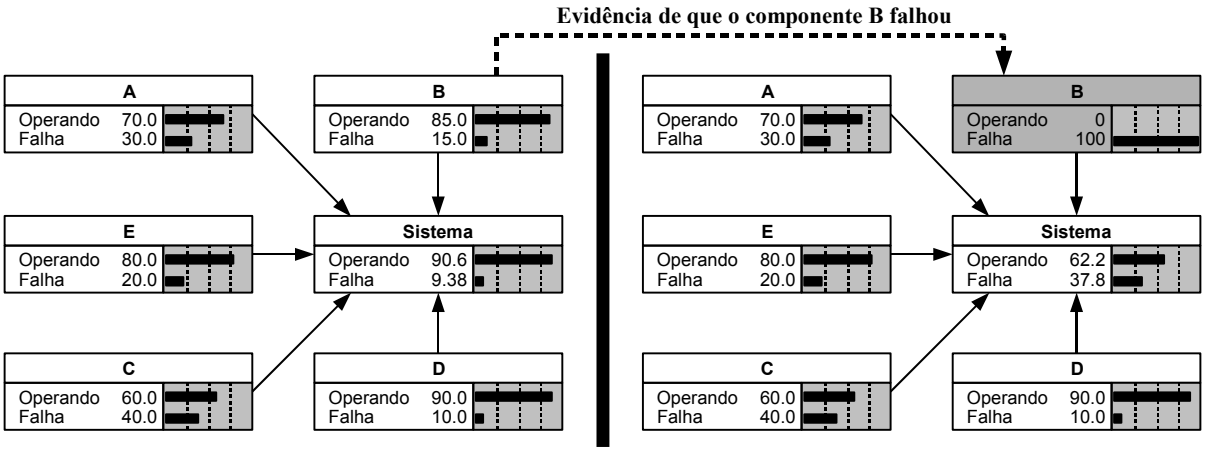


Figura 4.2: Exemplo de rede bayesiana antes e após evidência

Note-se que a probabilidade de falha do sistema alterou de 9,38% para 37,8% após a evidência de que o componente B falhou.

[3]Figura editada a partir da rede elaborada utilizando o *software* Netica©, desenvolvido pela Norsys Software Corp.

4.3 Árvore de falha (FTA)

FTA (*fault tree analysis*) foi elaborada por H. A. Watson, dos Laboratórios Bell, em 1961, em atividade desenvolvida para a força aérea norte-americana, com o fim de estudar o míssil Minuteman. Em 1965, na primeira conferência de sistemas de segurança, patrocinada pela Boeing e pela Universidade de Washington, foram apresentados os primeiros trabalhos utilizando FTA, difundindo a técnica. (ERICSON II, 1999).

FTA, ilustrada na Figura 4.3, é uma técnica dedutiva que elabora o modelo partindo de um evento (evento topo) e, posteriormente, identificando as causas necessárias para sua ocorrência. A diagramação é feita utilizando operadores lógicos – como "e", "ou", etc. –, o que possibilita calcular a probabilidade de ocorrência do evento topo por lógica booleana, atribuindo probabilidades à ocorrência de cada causa.

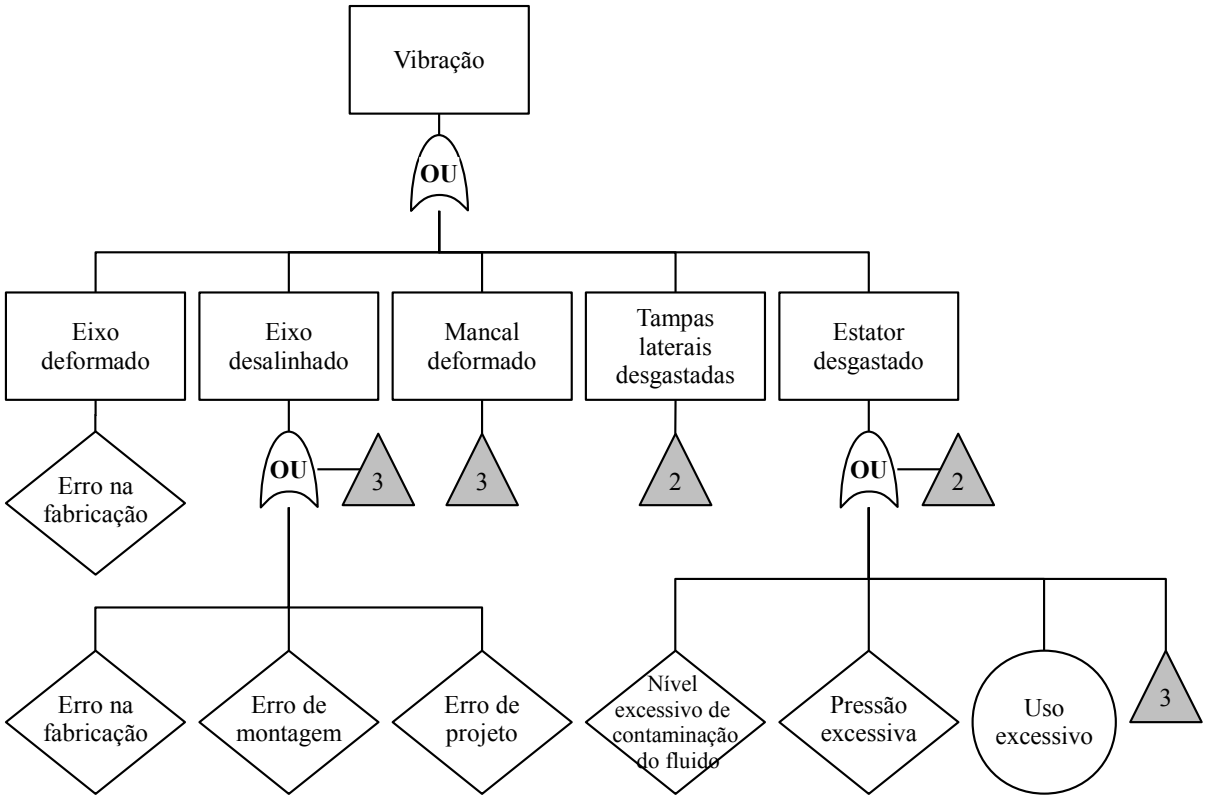


Figura 4.3: Exemplo de árvore de falha para o efeito topo vibrações
Fonte: Sakurada (2001, p. 83)

Na Figura 4.3, por exemplo, o evento "eixo desalinha" ocorre sempre que um dos eventos abaixo – "erro na fabricação", "erro na montagem" ou "erro no projeto" – ocorrer, pois é uma porta "ou". Note-se que as causas que foram desdobradas estão representadas por retângulos, e as que ainda requerem uma futura análise são diagramadas como losangos (círculos representam

as causas raízes). O triângulo, por sua vez, representa o ramo que está abaixo dele – assim, não é necessário repetir o mesmo ramo várias vezes.

É interessante esclarecer que o símbolo do triângulo é utilizado para evitar que se repita a mesma informação várias vezes. Assim, o triângulo de número 3 representa o conjunto abaixo da porta.

FTA pode ser executada em quatro etapas (ALBERTON, 1996): definição do sistema, construção da árvore de falhas, avaliação qualitativa e avaliação quantitativa (quando aplicável).

4.4 Árvore de eventos (ETA)

Aparentemente, ETA (*event tree analysis*) foi desenvolvida no início dos anos 70, durante o WASH-1400, para apoiar a implementação de análises de riscos em centrais nucleares (ERICSON II, 2005), e atualmente é utilizada nas mais diversas áreas.

ETA é um método indutivo que, partindo de um determinado evento inicializador, delineia as combinações de eventos até chegar aos possíveis resultados (cenários). Nestes modelos, usualmente cada evento pode ser instanciado apenas em "aconteceu" ou "não aconteceu", o que resulta em 2^n cenários, onde "n" é o número de eventos da árvore.

Note-se que existem técnicas de otimização da árvore (desbaste dos ramos), que simplificam o diagrama – já que o número de ramos cresce exponencialmente com o número de eventos, podendo resultar em árvores complexas.

A Figura 4.4 ilustra uma árvore de eventos. Nela, o evento A é o inicializador, e a ocorrência (ou não) dos eventos B e C determina qual o cenário esperado. Por exemplo, caso ocorra A, B e não ocorrer C ($A = a$, $B = b$ e $C = \bar{c}$), o estado final resultante é o "2", sendo que a probabilidade de este cenário ocorrer é $P(a).P(b|a).P(\bar{c}|a,b)$.

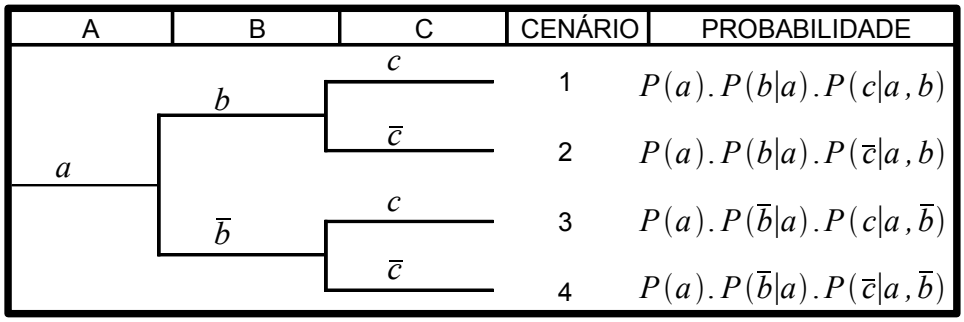


Figura 4.4: ETA de eventos sequenciais, na qual o evento *A* é o evento inicializador

A técnica pode ser utilizada para delinear, barreiras a fim de reduzir consequência ou para organizar, caracterizar e quantificar potenciais incidentes de uma maneira metódica (EUROCONTROL, 2004). Ela pode ser executada em cinco etapas: (i) identificação dos eventos inicializadores; (ii) identificação dos eventos que podem influenciar (incluindo barreira, salvaguardas, etc.); (iii) estruturação da árvore de eventos; (iv) simplificação da árvore de eventos; e (v) cálculo da probabilidade de cada cenário (quando aplicável).

4.5 Diagrama sequencial de eventos (ESD)

Um ESD (*event sequence diagram*), a exemplo do ilustrado na Figura 4.5, é um modelo que procura representar esquematicamente sequências de eventos que levam a diferentes estados finais. Cada "caminho", no diagrama, é um cenário, e cada evento pivotal é identificado como "ocorreu" ou "não ocorreu" (NASA, 2002b).

ESD é mais uma técnica para delinear cenários; no entanto, ela se destaca por ser mais aderente à forma de pensar dos engenheiros, comparada com as árvores de eventos (NASA, 2002b). Assim, ESD também é utilizado como técnica de suporte para elicitar o conhecimento do especialista, para, então, modelar árvores de eventos e fazer análises probabilísticas.

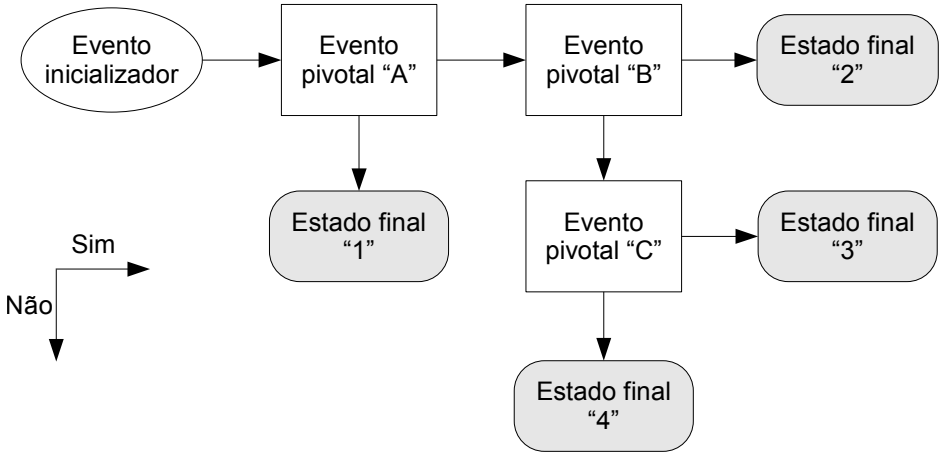


Figura 4.5: ESD ilustrativo

Everdij & Blom (2008, p. 44) consideram ESD como sendo uma "generalização da ETA", pois não se restringe à representação da sequência de eventos, podendo modelar sistemas reparáveis. Ademais, recentemente, Swaminathan & Smidts (1999) propuseram uma extensão da técnica, possibilitando a modelagem de sistemas dinâmicos, bem como sua análise probabilística.

4.6 Análise / avaliação dos perigos funcionais (FHA)

A origem exata da técnica FHA (*functional hazard assessment*) é incerta; no entanto, acredita-se que os estudos iniciais para sua concepção tenham sido feitos na década de 1960 (EUROCONTROL, 2006).

A técnica, no setor aéreo, atualmente é utilizada em metodologias como a EATMP SAM, que originalmente baseou-se na FHA proposta na SAE ARP 4761, mas extrapolou o escopo, contemplando todo o sistema de navegação aérea (EUROCONTROL, 2006). A SAE ARP 4761, por sua vez, é um refinamento e uma extensão da JAA JAR-25 e abrange tanto *hardware* quanto *software* (EVERDIJ; BLOM, 2008).

FHA é uma técnica *top-down* iterativa que procura determinar quão seguro deve ser o sistema, e normalmente é conduzida no início do desenvolvimento ou da modificação do sistema (EUROCONTROL, 2006). É uma análise metódica das funções do sistema, a fim de identificar as possíveis falhas e classificá-las de acordo com uma escala de severidade dos efeitos (SILVA, 2006).

A representação do modelo é feita na forma de tabelas, a exemplo do Quadro 4.2, que ilustra parte da análise / avaliação de um prédio de uma central de controle de tráfego aéreo (ATCC – *air traffic control center*).

Quadro 4.2: Exemplo de parte de FHA de um ATCC

Função	Perigo	Efeito no ATCC	Efeito no ATM	Severidade	Comentários
Construção da sala de ATC	Perda total da sala do controle de tráfego aéreo (ATC – *air traffic control*) devido à colisão (aeronave, meteorito, veículos, etc.), danos severos ao prédio.	Evacuação imediata das pessoas. Inviabiliza a operação.	Inabilidade total de prover ou manter serviço de ATM (*air traffic management*) seguro. Perda do serviço.	1	Evento tão improvável de ocorrer, que foi decidido não se fazer nada para evitar o perigo ou mitigar suas consequências (em alguns casos nada poderia ser feito). Esse risco é classificado como aceitável pela gerência.

Fonte: EUROCONTROL (2006, FHA, Level 3, Appendix D (Core), p. 16, tradução nossa)

No Quadro 4.2, os termos adotados têm os seguintes significados:

- "Função" – as funções que o sistema deve desempenhar;
- "Perigo" – os perigos levantados e avaliados para as falhas funcionais;
- "Efeitos" – os efeitos e consequências caso o incidente ocorra;
- "Classe de severidade" – a classe da máxima probabilidade tolerável de o efeito ocorrer

(classe 1 refere-se ao mais severo, cuja ocorrência não é tolerável, e classe 5 refere-se ao efeito inexistente[4]);

- "Comentários" – incluem-se informações relevantes sobre o perigo estudado.

É possível, então, especificar os objetivos de segurança e apresentá-los em uma tabela – o Quadro 4.3 é um exemplo de parte dos objetivos da FHA ilustrada no Quadro 4.2.

Quadro 4.3: Exemplo de parte dos objetivos de segurança

Função	Perigo	Severidade	Objetivos de segurança
Construção da sala de ATC	Perda total da sala do controle de tráfego aéreo (ATC – *air traffic control*) devido à colisão (aeronave, meteorito, veículos, etc.), danos severos ao prédio.	1	Nenhum objetivo de segurança. Uma vez que este evento é tão improvável de ocorrer, foi decidido não se fazer nada para evitar o perigo ou mitigar suas consequências (em alguns casos nada poderia ser feito). Esse risco é classificado como aceitável pela gerência.

Fonte: EUROCONTROL (2006, FHA, Level 3, Appendix D (Core), p. 30, tradução nossa)

EUROCONTROL (2006) destaca que FHA pode ser aplicada em diferentes níveis, mas, idealmente, deve ser conduzida no sistema mais abrangente (nível macro) – para que os objetivos sejam traçados para este nível, sendo que os requisitos devem ser desdobrados para os subsistemas.

4.7 Análise do modo de falha, efeitos e criticidade (FMECA)

FMECA (*failure modes effects and criticality analysis*)[5] teve sua origem no departamento de defesa dos Estados Unidos (DOD – Department of Defense), em 1949, com a norma militar MIL-P-1629 (*Military procedure* MIL-P-1629: *Procedures for performing a failure mode, effects and criticality analysis*).

A FMECA é uma técnica analítica desenvolvida com base em uma tabela, como a ilustrada no Quadro 4.4, que tem como propósito "estudar os resultados ou efeitos da falha de um item na operação do sistema e classificar cada falha potencial de acordo com sua severidade" (USA/DOD, 1980, p. 101-1, tradução nossa).

Segue uma breve descrição dos elementos da FMECA:

1. **função** – a função estudada;

[4]Note-se que esta classificação de severidade tem escala inversa da adotada em algumas outras técnicas – na FMECA, por exemplo.

[5]A FMECA se distingue da FMEA (*failure modes effects and analysis*) pelo fato de agregar um índice de criticidade que orienta a prioridade nas ações a serem executadas pela organização.

2. **modo de falha** – é a forma em que o sistema deixa de cumprir seu requisito funcional;
3. **efeito potencial** – potenciais efeitos que a falha desta função pode gerar;
4. **causas** – as causas raízes do modo de falha;
5. **controles atuais** – apresentar as barreiras para monitorar e controlar a falha;
6. **NPR** – é o resultado da multiplicação de três índices, referentes à probabilidade de ocorrência (O), à severidade do efeito (S) e à possibilidade de se detectar o modo de falha a partir dos controles atualmente implementados (D);
7. **ações recomendadas** – são as ações preventivas que devem ser executadas diante das variações percebidas da função, a fim de evitar ou mitigar falha;
8. **responsabilidade** – os nomes dos responsáveis pelas ações;
9. **ações executadas** – ações efetivamente executadas; e
10. **reavaliação dos índices** – valor atribuído aos índices após as ações executadas.

Quadro 4.4: Exemplo de tabela para FMECA

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
Porta dianteira L.H H8HX-0000-A ▪ Entrar e sair do veículo ▪ Proteção dos ocupantes contra o tempo, ruído, e impacto lateral	Painel inferior de dentro da porta corroído	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 do 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 (Teste Nº 1481) a especificação para o gume superior subiu 125mm	7	2	2	28
				Especificação da espessura da cera é insuficiente	4	Teste de durabilidade geral do veículo – como acima	7	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 (Teste Nº 1481) mostraram que a espessura especificada é adequada. DOE mostrou que variação de 25% na espessura é aceitável	7	2	2	28

Fonte: SAE (2002, p. 43, tradução nossa)

No entanto, a representação do modelo na forma de tabela é um dos grandes inconvenientes desta técnica (LEE, 2000). Os campos das tabelas são limitados e a definição semântica

é pobre, o que torna difícil a reutilização do conhecimento em outras FMECAs – bem como compartilhar o conhecimento com outras equipes de projeto e de diagnóstico. Adicionalmente, o tempo dispendido em reuniões normalmente é alto, o que impacta fortemente no custo de desenvolvimento da FMECA.

Com o intuito de auxiliar na elaboração da FMECA, o NeDIP – em um projeto inicialmente suportado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) – vem trabalhando na elaboração de uma ferramenta computacional chamada OpenFMECA, apresentada na Seção 5.4, a fim de minimizar estes inconvenientes.

4.8 Análise *bow-tie* (BTA)

Para Everdij & Blom (2008), o diagrama BT (*bow-tie*[6]) é uma evolução dos diagramas causa-consequência dos anos 70 e dos diagramas de barreiras dos anos 80, tendo sido mais intensamente utilizado nas indústrias químicas e petroquímicas.

Lewis & Hurst (2005) corroboram com estes autores e indicam a Royal Dutch / Shell Group como sendo a primeira grande empresa a integrar a BTA (*bow-tie analysis*) às suas práticas, sendo responsável pelo desenvolvimento da técnica e sua disseminação em todo o mundo.

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 et al. (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; FIÉVEZ, 2006; GOWLAND, 2006); entre outras.

BTA é uma alternativa gráfica para tradicionais métodos de análise de risco, como HAZOP (*hazard and operability*) e "*what-if*" (PHILLEY, 2006). Nela, o evento a ser estudado é posicionado no centro do diagrama, suas causas à esquerda, e seus efeitos à direita, permitindo a visualização das relações entre os elementos do sistema modelado.

A Figura 4.6 ilustra uma BTA, de acordo com a sintaxe proposta por Lewis & Hurst (2005), que é similar à adotada por outros autores, como Trbojevic (2004) e Beerens et al. (2006), e pelos *softwares* BowTieXP[7] e BowTie-Pro[8], em que:

[6] O diagrama tem este nome porque sua forma se assemelha a uma gravata-borboleta
[7] Vide: <http://www.bowtiexp.com/>.
[8] Vide: <http://www.bowtiepro.com/>.

- **Ameaça:** causa potencial para dar início ao cenário de risco que leva ao evento central.
- **Barreira:** medidas de proteção para prevenir as ameaças que podem levar ao 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 "medidas de recuperação".
- **Controle do fator de escala:** medidas para evitar a falha da "barreira" ou "medida de recuperação".

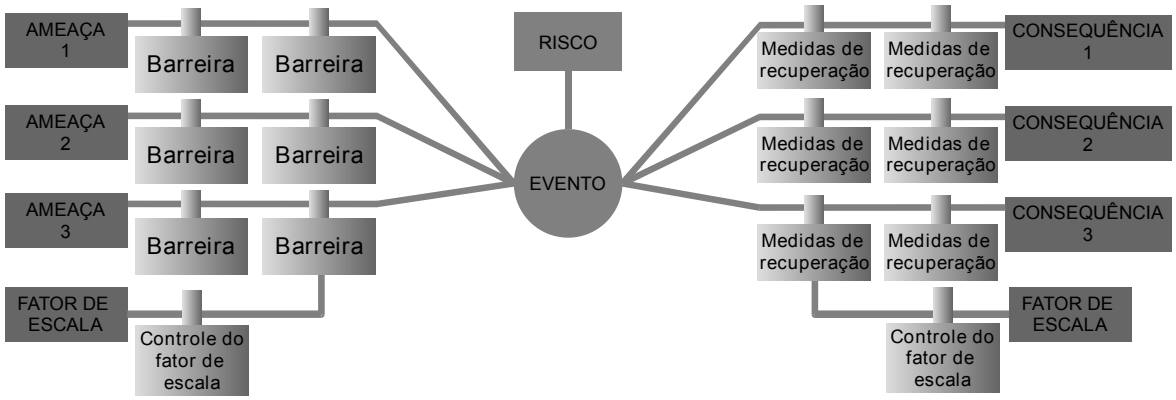


Figura 4.6: Diagrama ilustrativo de uma BTA
Fonte: Lewis & Hurst (2005, p. 2, tradução nossa)

4.9 Análise de eventos por rede causal (CNEA)

A CNEA (*causal network event analysis*), apresentada na Figura 4.7 e no Quadro 4.5, é uma técnica que faz uso de redes causais para analisar a ocorrência de um determinado evento (um incidente ou um modo de falha, por exemplo). Redes causais são grafos acíclicos direcionados (DAG), que, no caso da CNEA, apresentam, no centro do diagrama, o evento a ser analisado. Este formato é análogo ao da BTA, no entanto, na CNEA, podem-se desdobrar as causas e os eventos, i.e.: é possível incluir eventos intermediários.

Outro ponto a se destacar nesta técnica é a possibilidade de considerar que a barreira foi bem sucedida, mas que o resultado disto também deve ser incluído na análise. Em alguns casos, principalmente na mitigação do incidente, uma barreira pode resultar em situações não tão graves quanto se ela não existisse, mas que não podem ser desprezadas.

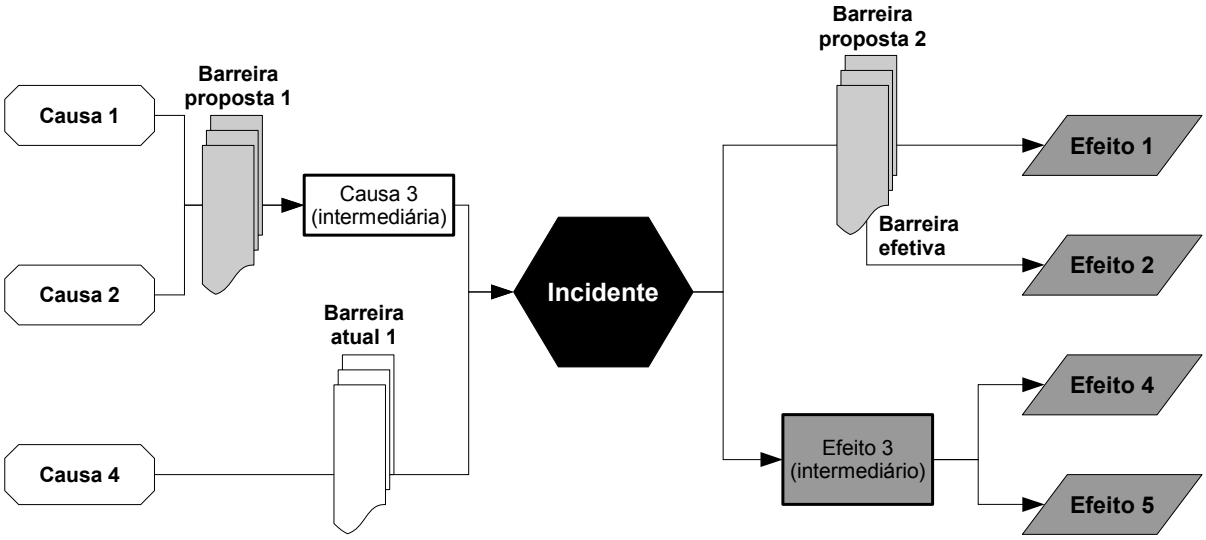
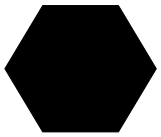
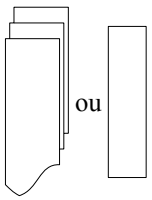
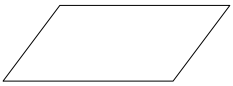
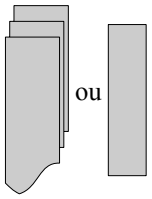


Figura 4.7: Diagrama ilustrativo da técnica CNEA

Quadro 4.5: Elementos utilizados na 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**		

Note-se que é possível, em apenas um diagrama, visualizar as relações das causas (que podem ser modeladas em uma árvore de falhas) e dos efeitos (que podem ser modeladas em uma árvore de eventos). No entanto, a CNEA pode ser modelada sem ter que determinar o tipo de relação existente entre seus elementos – como em uma FTA –, e os efeitos são estados e não eventos, como em uma ETA.

É interessante observar que não existe uma sintaxe consolidada para a BTA, sendo que alguns autores – como GOVERNORS (2005) e Lewis & Hurst (2005) – apresentam apenas uma lista de ameaças (que são as causas), o evento central e uma lista das consequências (efeitos). Outros, como Beerens et al. (2006) e Léger et al. (2006), incluem eventos intermediários, o que

torna a BTA similar a uma CNEA.

De fato, a técnica CNEA foi desenvolvida neste trabalho de doutorado e em projetos de pesquisa e desenvolvimento (P&D) realizados pelo NeDIP / UFSC, a fim de contornar algumas dificuldades identificadas na utilização da estrutura FTA / ETA. A CNEA surgiu da associação da BTA com redes causais e, com a experiência acumulada pela equipe de pesquisadores do núcleo na utilização de técnicas para análise de confiabilidade e segurança, foi possível aprimorar esta associação e propor a técnica como apresentada neste documento.

Por fim, é interessante destacar que a CNEA permite diagramar incidentes modelados pela corrente causal proposta por Mosleh et al. (2004). De fato, em uma rede causal, podem-se modelar várias correntes causais referentes a um determinado incidente, conforme ilustrado na Figura 4.8.

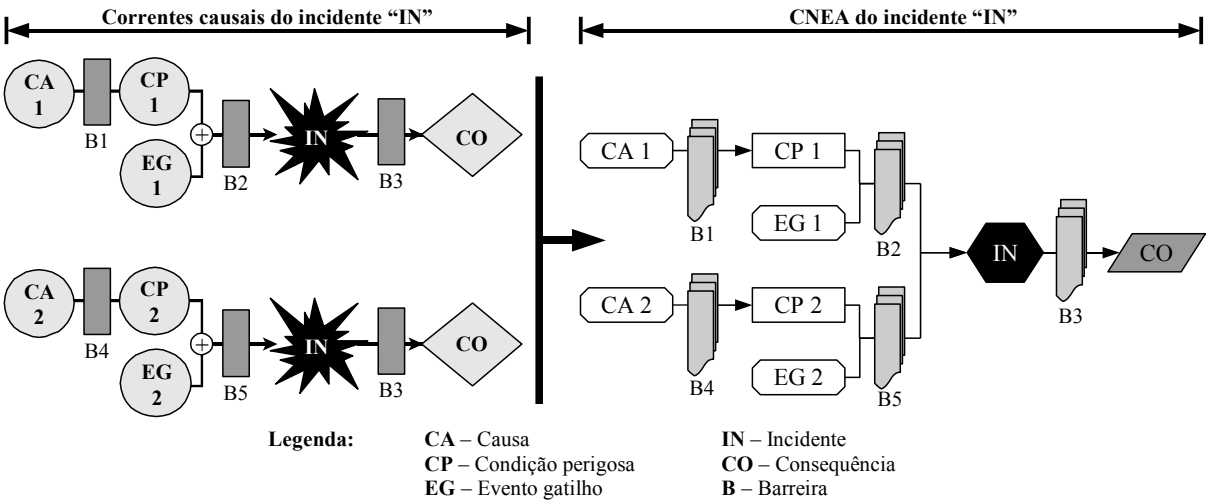


Figura 4.8: Modelagem de correntes causais na CNEA

No entanto, para que se possa agrupar correntes causais, os efeitos decorrentes do incidente devem ser idênticos. Caso exista uma particularidade de um incidente quando deflagrado por uma condição específica, esta 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 de o mesmo evento gatilho deflagrar mais de uma condição perigosa (CP1 e CP2, na Figura 4.8).

4.10 Considerações finais

Foi apresentada, ao longo do Capítulo 4, uma breve revisão sobre algumas técnicas de modelagem utilizadas no gerenciamento de risco. Estas técnicas podem ser aplicadas independentemente; no entanto, foi desenvolvida uma estrutura de trabalhado – detalhada no Capítulo 5 – que associa as técnicas IDEF0, FHA, FMECA, CNEA, FTA, redes bayesianas e atualização bayesiana, a fim de possibilitar uma melhor análise / avaliação dos riscos .

No que se refere à técnica IDEF0, ela será fundamental para o mapeamento funcional da organização. Assim, pode-se identificar quais funções (caixas) são essenciais para o negócio, e quais as restrições (controles) e os recursos (entradas e mecanismos) que são críticos.

A FHA, então, pode ser utilizada para identificar os perigos associados a estas funções e analisar seus efeitos e quão críticos são eles para o sistema, a fim de definir os objetivos de risco.

Pode-se, então, identificar a forma em que ocorre o incidente ou a falha (modo de falha) e a criticidade dela, pela técnica FMECA – que possibilita, ainda, que se avaliem indicadores de controle (sensores) e barreiras para mitigar ou evitar os potenciais cenários.

No entanto, a representação em tabelas dificulta a execução da FMECA, sendo um dos grandes inconvenientes da técnica. A fim de fornecer uma ferramenta gráfica para a análise, associou-se a técnica CNEA à FMECA.

A CNEA possibilita uma modelagem do sistema sem a necessidade de conhecê-lo tão profundamente quanto na FTA. A modelagem dos efeitos também se mostrou mais intuitiva que na ETA, pois não utiliza eventos pivotais – que, na CNEA, estão modelados como barreiras. Outro ponto a se destacar na CNEA é o fato de ela ser mais aderente ao modelo de Mosleh et al. (2004), adotado neste trabalho, para representação de incidentes.

Para fazer o tratamento estatístico dos modelos elaborados com a FMECA /CNEA, podem-se utilizar redes bayesianas – especialmente quando as relações entre as causas e os efeitos não forem determinísticas.

Por fim, para inferir a probabilidade dos eventos, pode-se utilizar a inferência bayesiana (para eventos raros) ou a estatística clássica – quando se tem histórico de falha mais representativo.

Quanto à ETA e à FTA, elas são muito utilizadas em conjunto para delinear possíveis cenários (ETA) e identificar as possíveis causas da ocorrência de cada evento (FTA) e podem ser empregadas como uma alternativa à CNEA. A BTA também pode ser utilizada em substitui-

ção à CNEA, especialmente em situações em que se listem as possíveis causas e efeitos sem a necessidade de compreender todas as correntes causais. Pode-se, ainda, utilizar a ESD para facilitar a elicitação do conhecimento do especialista.

Estas técnicas darão suporte principalmente para a etapa de análise / avaliação de risco da metodologia desenvolvida, mas também serão fundamentais no tratamento e no planejamento dos riscos aceitos.

5 *Metodologia de gerenciamento de risco desenvolvida*

Neste capítulo, apresenta-se a metodologia de gerenciamento de risco desenvolvida neste trabalho, objetivando contemplar as necessidades percebidas durante a pesquisa básica no campo da gestão de risco e consubstanciada nos capítulos de revisão da literatura.

Observou-se que o gerenciamento de risco vem sendo explorado principalmente nos últimos 50 anos (destacadamente nos 15 últimos) e que, a partir do ano 2000, foram efetivamente consolidadas regras e normas. Isto ocorreu em resposta ao aumento de complexidade e de porte dos sistemas – além da redução da tolerância da sociedade quanto à ocorrência de incidentes, tanto com impacto na segurança do homem, do ambiente e do patrimônio quanto com impacto na continuidade da função desempenhada pelo sistema.

Também foram apresentadas algumas evidências da necessidade de se integrar estas duas abordagens. Assim, a metodologia apresentada a seguir procura satisfazer esta necessidade e considera a segurança e a continuidade / disponibilidade como atributos a serem tratados durante a gestão de risco. Nesta ótica, elas deixam de ser abordagens independentes e passam a integrar o mesmo sistema de gestão (SGR) que trabalha os riscos de maneira mais abrangente.

5.1 Estrutura da metodologia de gerenciamento de risco

A Figura 5.1 ilustra as etapas da metodologia de gestão de risco, que serão apresentadas nas próximas seções. Note-se que a metodologia pode ser aplicada aos três níveis da estrutura proposta para o desdobramento da organização apresentada na Seção 2.3, vide Figura 2.7 e Quadro 2.6.

A Figura 5.2 ilustra a aplicação da metodologia nestes três níveis. Neste contexto, no nível da organização, a gestão de risco objetiva garantir a continuidade do negócio e garantir que a operação da organização não incorra em riscos inaceitáveis à segurança de seus colaboradores e da sociedade em geral; no nível da unidade organizacional, o foco é manter as funções críticas

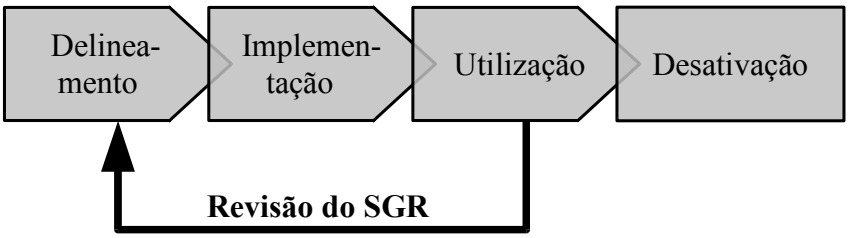


Figura 5.1: Etapas da metodologia de gestão de risco

ativas (continuidade operacional) e garantir a segurança do meio em que está inserida, de seus colaboradores (e outras pessoas afetadas pela sua operação) e dos sistemas técnicos que a compõem; e, no nível do sistema técnico, o foco é manter sua disponibilidade sem comprometer a segurança das pessoas, do meio e outros sistemas técnicos que interagem com ele.

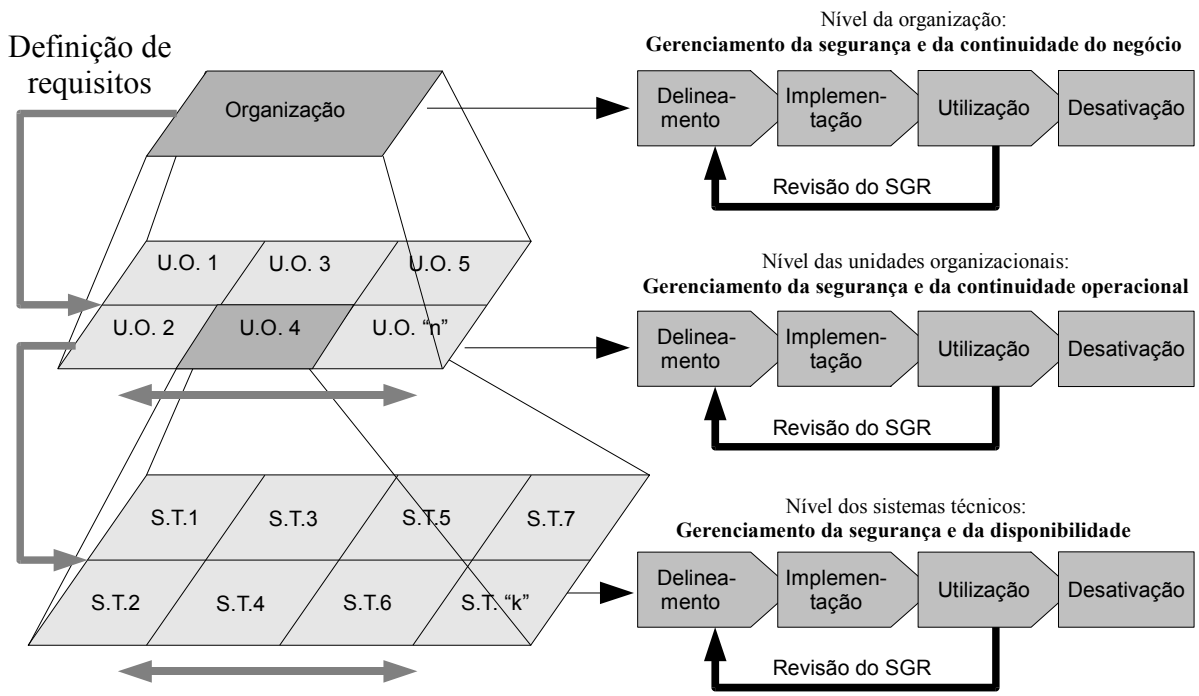


Figura 5.2: Estrutura da metodologia desenvolvida

Idealmente, o sistema de gestão de risco deve ser desenvolvido do nível superior para o inferior. No entanto, os níveis podem ser trabalhados independentemente – por exemplo: a aplicação do sistema de gestão de risco em uma unidade organizacional não é pré-requisito para a aplicação em um sistema técnico.

Note-se que a disponibilidade de um sistema técnico pode ser determinante para a continuidade da unidade organizacional, como apresentado no Quadro 2.6. Assim, é interessante que se delineie o sistema de gestão de risco na unidade, para que se possam definir os objetivos de

risco dos sistemas técnicos que a compõem, conforme apresentado na Seção 5.3.1.1.

Contudo, é importante que a decisão dos níveis em que serão feitas as aplicações da metodologia seja feita no âmbito do planejamento da organização, no primeiro nível da Figura 5.2. O sistema de gerenciamento de risco contribui para que a organização alcance sua missão e, portanto, deve estar inserido em um planejamento mais amplo.

Assim, o primeiro passo para se poder aplicar a metodologia de gerenciamento de risco desenvolvida é a definição da estrutura da organização em unidades organizacionais e em sistemas técnicos. Note-se que a resolução adotada – i.e., até quando será feito o desdobramento – é uma questão gerencial. Por exemplo, uma unidade organizacional pode ser um departamento, um setor, uma divisão, etc., dependendo do desdobramento realizado.

Posteriormente, a organização deve fazer o planejamento de quais os sistemas (sistemas técnicos, unidades organizacionais e a própria organização) que terão o sistema de gestão de risco implementado. Note-se que, ao longo da aplicação da metodologia em um sistema (uma unidade organizacional, por exemplo), pode-se evidenciar a necessidade de implementar o SGR em outro sistema que, inicialmente, tinha sido excluído – ou mesmo alterar o cronograma das implementações.

É interessante destacar que, como todo programa, nesse também existe uma curva de aprendizado e (apesar de o grupo responsável pela implementação em cada nível e em cada unidade organizacional ou sistema técnico não ser exatamente o mesmo) as lições aprendidas por um grupo podem – e devem – ser passadas para os outros. Essa situação é especialmente interessante no caso de existirem similaridades entre as implementações. Assim, recomenda-se que seja feita uma implementação piloto para, posteriormente, replicar a aplicação nas outras unidades organizacionais (ou sistema técnico, se for o caso).

Neste contexto, pode-se trabalhar a aplicação da metodologia como um programa, e cada uma de suas etapas pode, assim, ser gerenciada como um projeto independente. Para tanto, sugere-se que seja adotada uma metodologia de gerenciamento de projetos consolidada, como a PRINCE2 (*projects in controlled environments*) da OGC (Office of Government Commerce / United Kingdom) ou o PMBOK (*project management body of knowledge*) do PMI (Project Management Institute), por exemplo.

De fato, a gestão do projeto para a aplicação da metodologia desenvolvida não difere significativamente da gestão de outros projetos. No entanto, é importante salientar que o apoio da alta gerência é um fator determinante para o sucesso do projeto.

Também, destaca-se a definição do responsável pelo projeto (coordenador) e dos partici-

pantes do grupo de trabalho. A disponibilidade dos recursos humanos é decisiva para o sucesso do programa, e a alocação das horas desses colaboradores deve ser autorizada pelos respectivos setores.

Destaca-se, ainda, a decisão de como captar o conhecimento necessário para a aplicação da metodologia e suas técnicas de suporte – já que muitas delas podem não ser utilizadas cotidianamente pelos colaboradores –, além da aquisição e capacitação quanto ao uso de *softwares* a serem utilizados.

Nas próximas seções, serão apresentadas as etapas da metodologia, indicadas na Figura 5.1. Para tanto, parte-se do pressuposto de que a organização tomou a decisão de implementar um sistema de gestão de risco. Com o intuito de auxiliar a visualização do que está apresentado neste capítulo, apresenta-se primeiramente a metodologia na forma de fluxogramas, que evidenciam como os processos das etapas (ou fases) se correlacionam.

Destaca-se, ainda, que a etapa de delineamento foi dividida em 4 fases, conforme ilustra a Figura 5.3, para facilitar o entendimento e a aplicação.

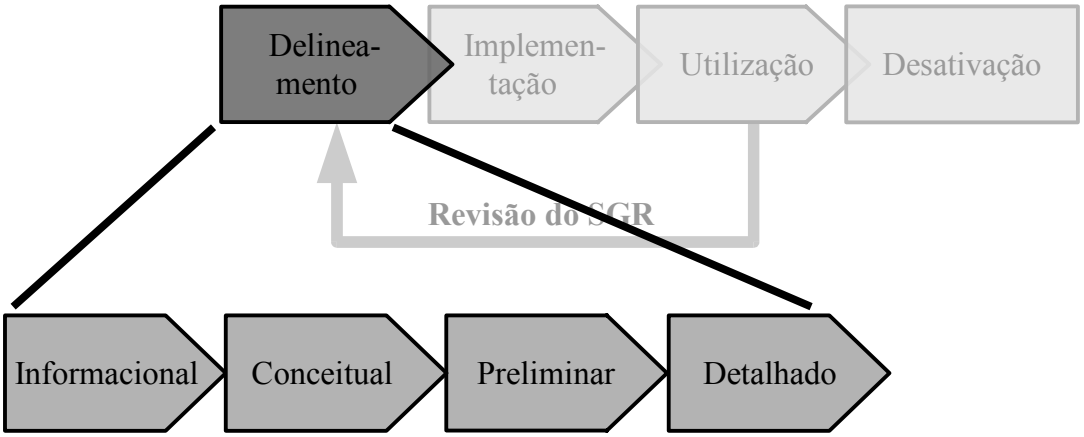


Figura 5.3: Desdobramento da etapa de delineamento do SGR

A estrutura da etapa do delineamento é uma adequação, para a gestão de risco, da adotada pelo NeDIP/UFSC para projeto de produto – apresentada em diversas publicações do núcleo, destacadamente em Back et al. (2008).

Por fim, é importante salientar que, ao longo do texto, indicam-se algumas técnicas de suporte associadas à metodologia. No entanto, outras técnicas podem ser utilizadas em substituição ou complementação das aqui apresentadas.

5.2 Fluxogramas de representação da metodologia desenvolvida

A Figura 5.4 apresenta a notação utilizada nos fluxogramas. Note-se que alguns elementos do diagrama foram destacados, utilizando borda mais grossa, para indicar que eles estão desdobrados em outros diagramas. Também existem elementos no fluxograma que indicam que a continuação da sequencia de processos segue em outro diagrama. Por fim, os processos referentes a uma determinada etapa, fase ou macroprocesso estão delimitados por uma "caixa" com linha tracejada.

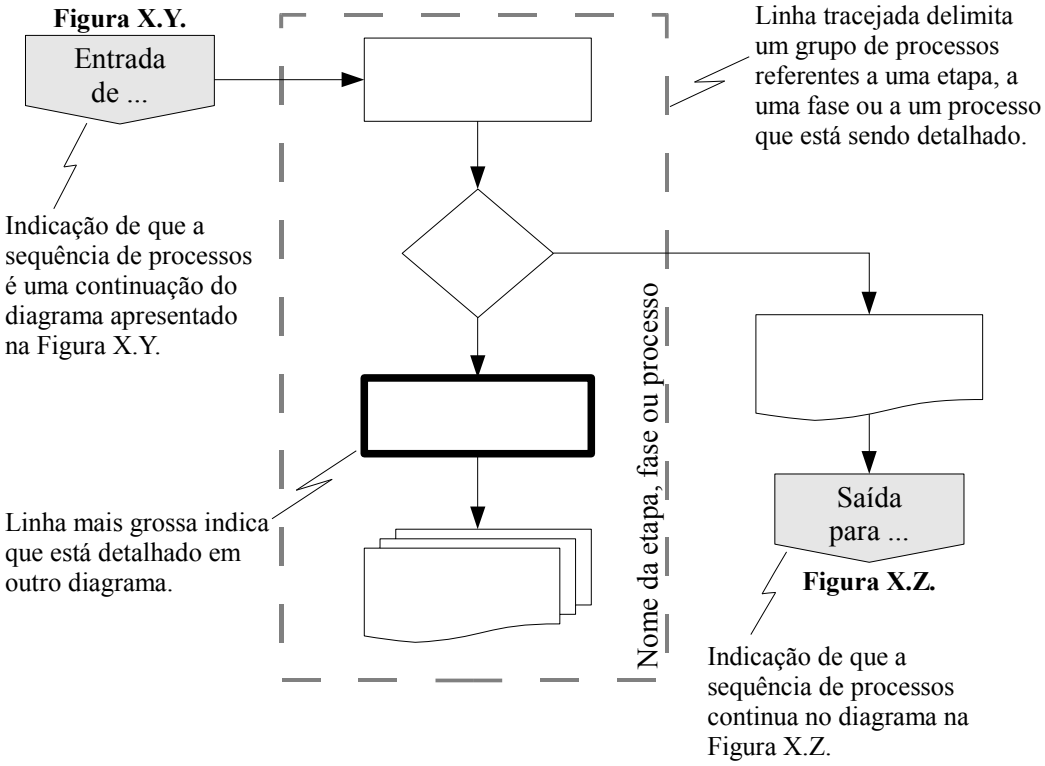


Figura 5.4: Notação utilizada nos fluxogramas

A Figura 5.5 apresenta a visão geral da metodologia desenvolvida. Note-se que elementos do diagrama referentes às fases informacional, conceitual e preliminar foram destacados, utilizando borda mais grossa, para indicar que eles estão desdobrados em outros diagramas – respectivamente: Figura 5.6; Figura 5.7 e Figura 5.8; e Figura 5.11.

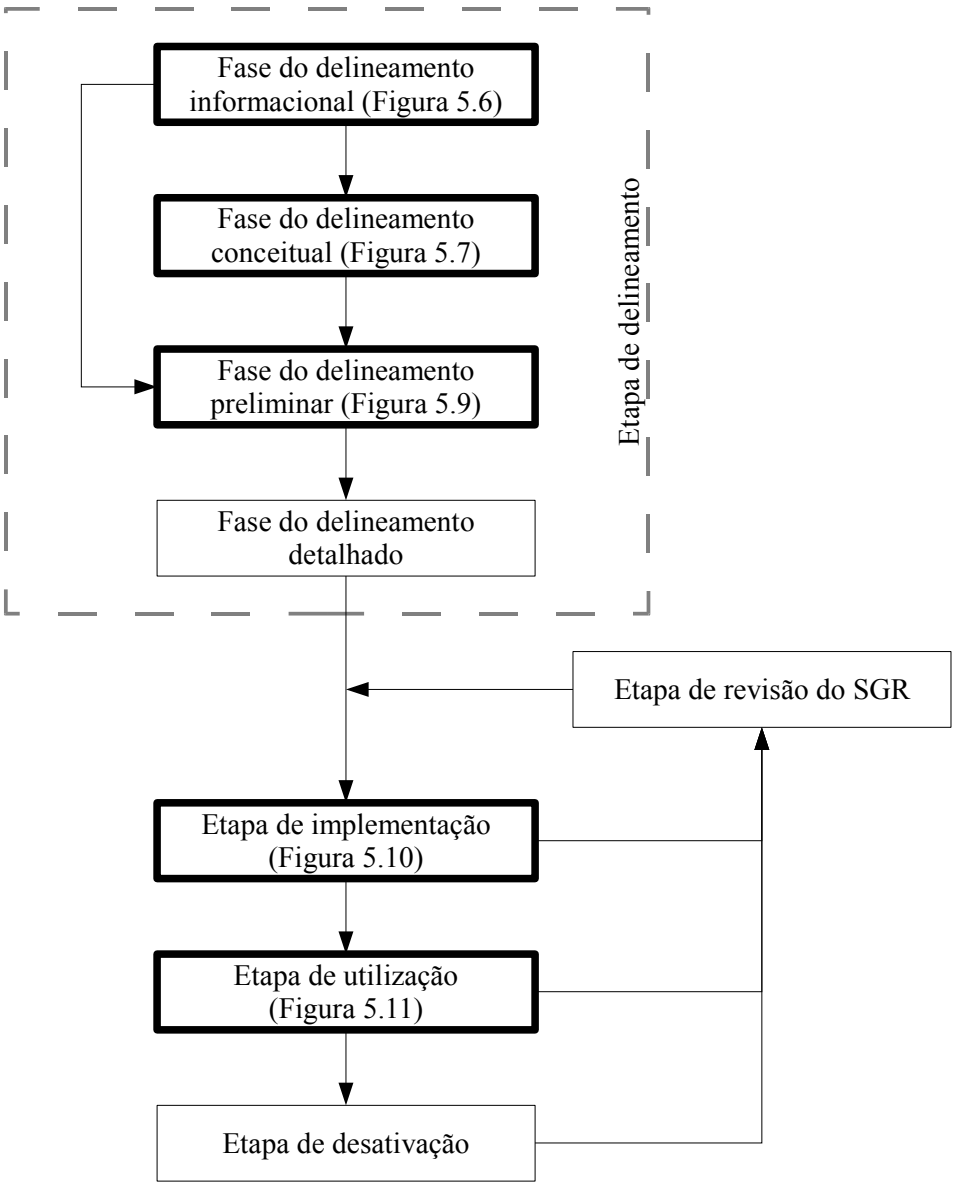


Figura 5.5: Fluxograma geral da metodologia desenvolvida

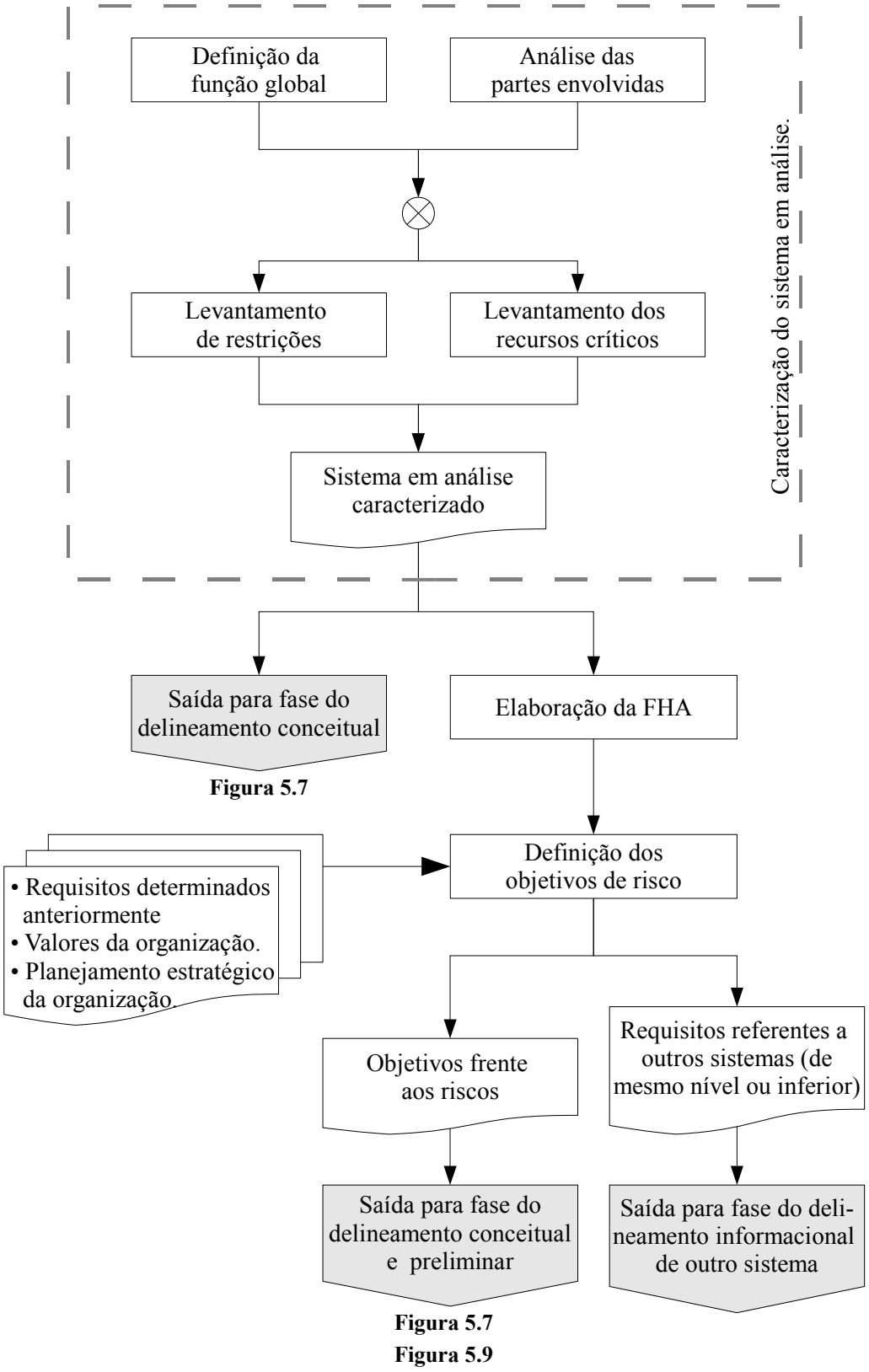


Figura 5.6: Fluxograma da fase do delineamento informacional

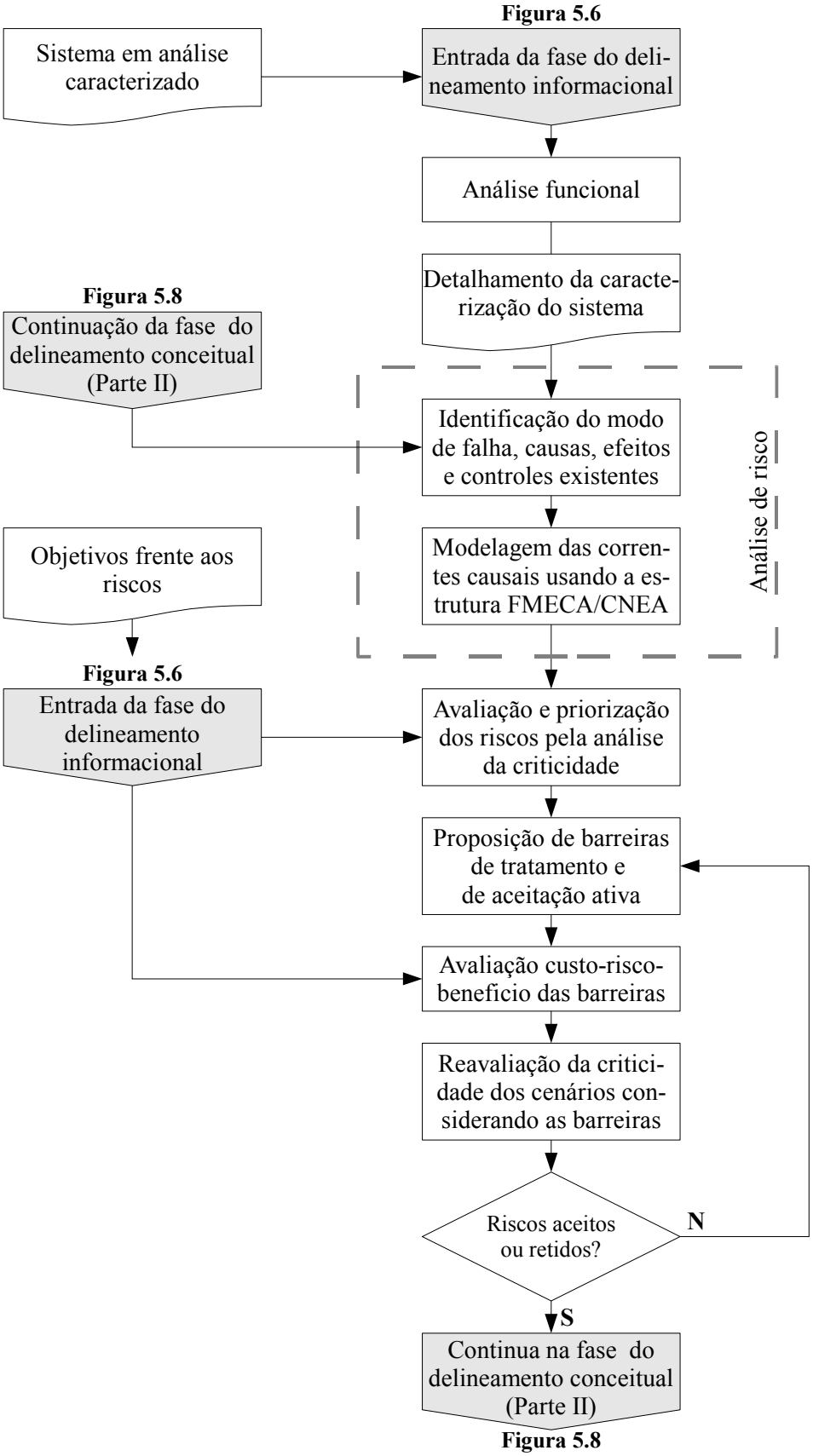


Figura 5.7: Fluxograma da fase do delineamento conceitual (parte 1)

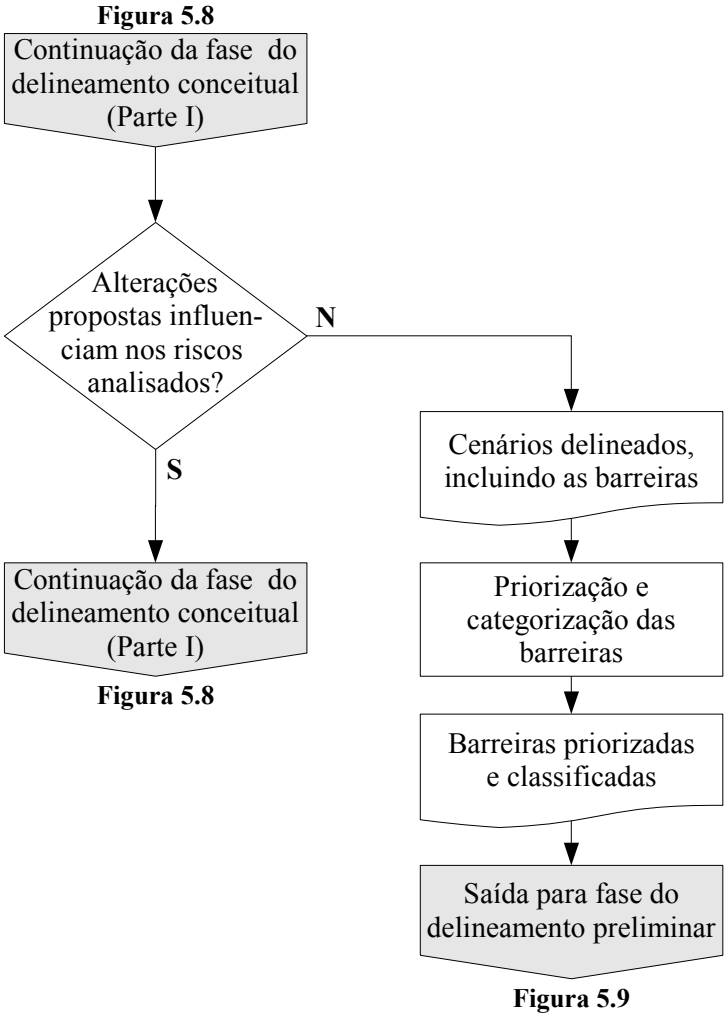


Figura 5.8: Fluxograma da fase do delineamento conceitual (parte 2)

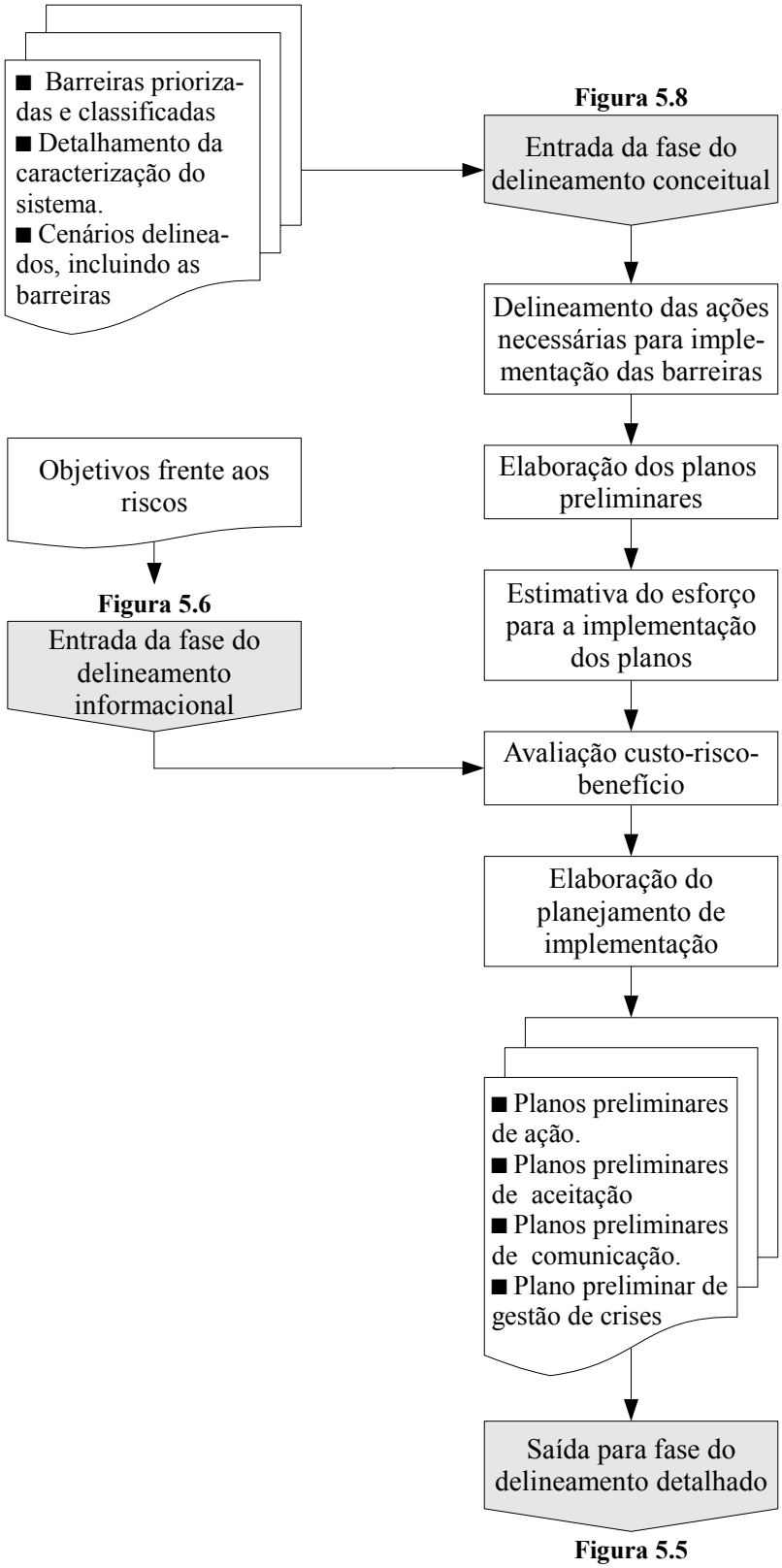


Figura 5.9: Fluxograma da fase do delineamento preliminar

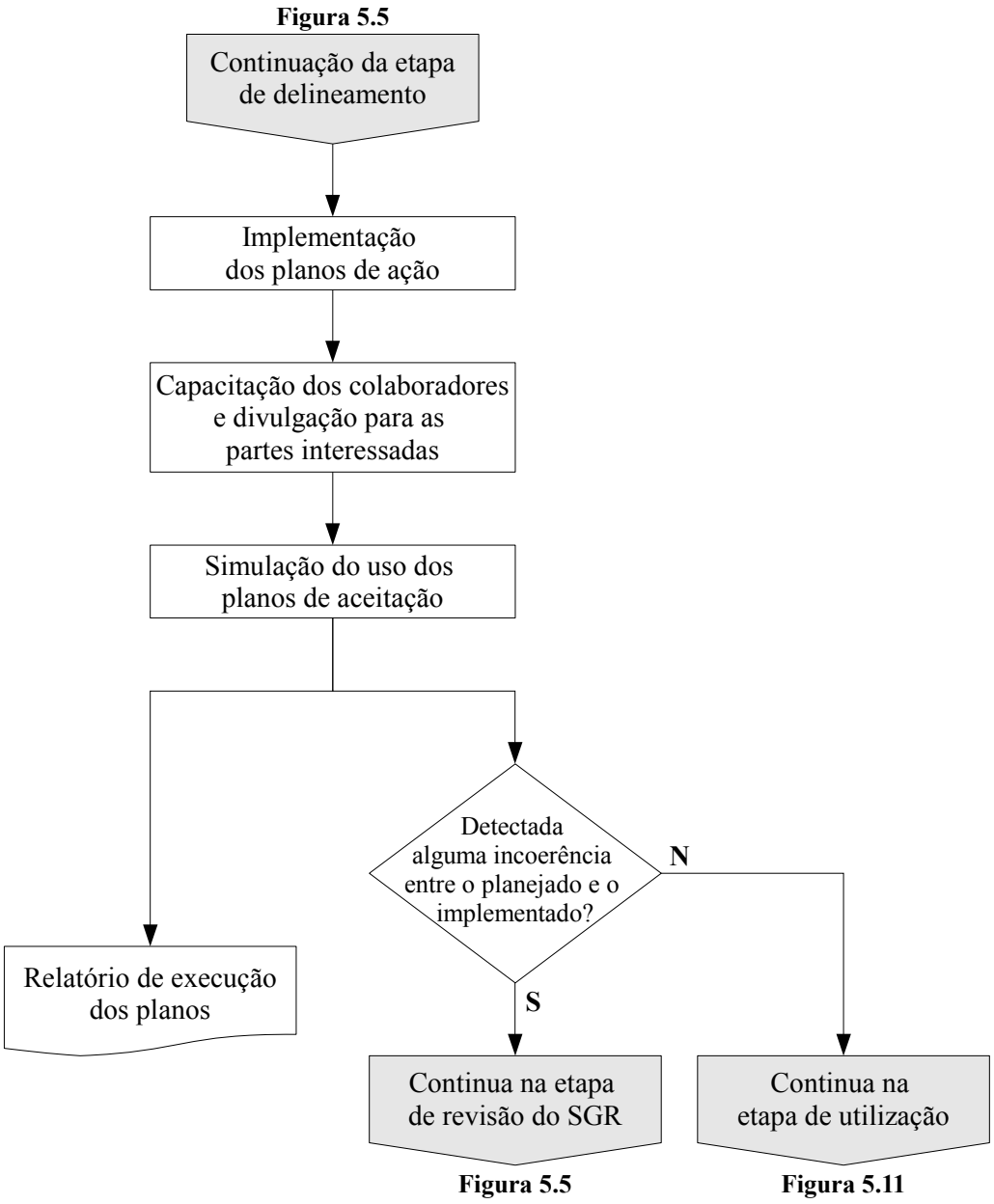


Figura 5.10: Fluxograma da etapa de implementação

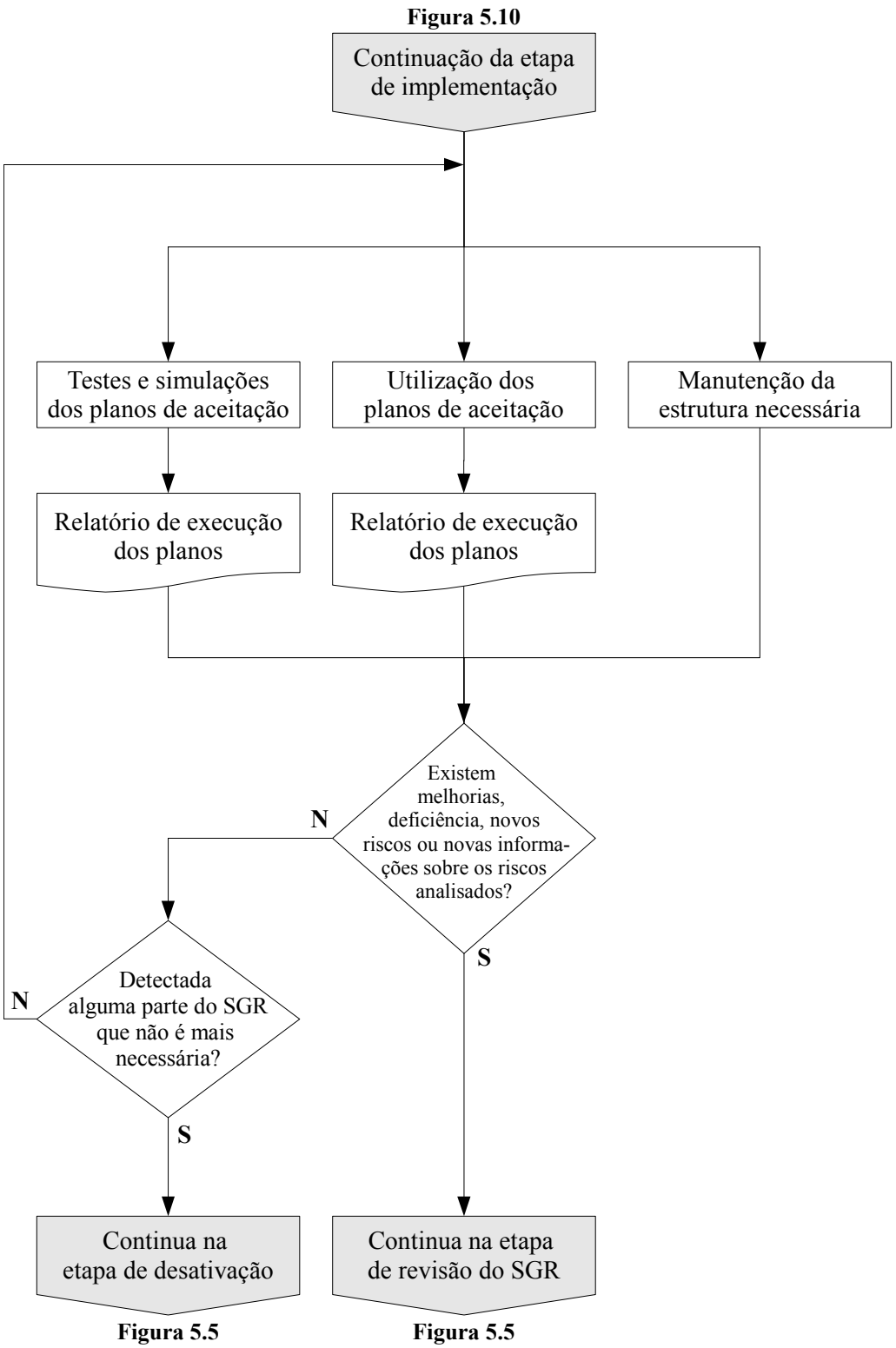


Figura 5.11: Fluxograma da etapa de utilização

5.3 Detalhamento das etapas da metodologia

Nesta seção, apresenta-se o detalhamento da metodologia desenvolvida neste trabalho.

5.3.1 Etapa de delineamento

Nesta etapa, faz-se a análise / avaliação dos riscos, o delineamento das ações para o tratamento, a aceitação e o delineamento da comunicação.

5.3.1.1 Fase do delineamento informacional

A fase do delineamento informacional visa definir os objetivos de aceitação de risco, i.e., os impactos toleráveis e suas respectivas metas relativas à disponibilidade (ou à continuidade), à segurança ambiental e à segurança humana – conforme ilustrado no Quadro 5.1 e Figura 5.6.

Quadro 5.1: Entradas, processos, técnicas & ferramentas e saídas para a fase de delineamento informacional

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Requisitos determinados anteriormente. ■ Valores da organização. ■ Planejamento estratégico da organização.	■ Caracterização do sistema em análise. ◇ Definição da função global. ◇ Análise das partes envolvidas. ◇ Levantamento de restrições. ◇ Levantamento dos recursos críticos. ■ Elaboração da FHA. ■ Definição dos objetivos de aceitação de risco.	■ Questionários. ■ Análise funcional (IDEF0 ou análise funcional de produto). ■ FHA.	■ Sistema em análise caracterizado. ■ Objetivos de aceitação de riscos. ■ Requisitos referentes a outros sistemas (de mesmo nível ou inferior).

Esta etapa, no que se refere ao levantamento dos efeitos possíveis, equivale à BIA (*business impact analysis*) feita na gestão da continuidade. No entanto, recomenda-se que aqui os objetivos sejam obtidos utilizando a técnica FHA. Sendo assim, é conveniente fazer uma análise funcional – que possibilitará a **caracterização do sistema em análise**[1]. Para tanto, 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 –, etc. Também é interessante, nesta fase, que se faça uma análise das partes envolvidas (*stakeholders analysis*), para que se possa captar as necessidades e limitações delas. Esta análise também auxilia na elaboração dos planos de comunicação, descrit na Seção 5.3.1.1.

[1]Para auxiliar a leitura, foram destacados, em negrito (ou sublinhado), os processos apresentados nos quadros com as entradas, processos, técnicas & ferramentas e saídas de cada etapa (ou fase).

Para a definição da função global, na análise funcional, recomenda-se a técnica IDEF0 – pois a técnica permite melhor comunicação e visualização dos sistemas, além de balizar o conhecimento dos membros do grupo de trabalho sobre o sistema técnico. Para sistemas físicos (*hardware*), recomenda-se a análise funcional de produto, na qual é feito o desdobramento do sistema em subsistemas até a resolução desejada, e, posteriormente, analisa-se a função de cada um deles – esta técnica tem benefícios equivalentes a IDEF0, mas é mais indicada quando se tem um desdobramento estrutural (e não funcional). Nesta fase, no entanto, não será necessário o desdobramento – tanto funcional quanto estrutural –, pois a FHA utiliza a função global do sistema (organização, unidade organizacional ou sistema técnico). O desdobramento, por sua vez, faz parte da fase do delineamento conceitual e subsidiará a análise dos modos de falha.

A partir da função global, então, pode-se fazer a **elaboração da FHA**. É interessante destacar que ela é normalmente realizada durante a concepção do sistema; no entanto, o documento RVSM 697 traz uma análise feita em um estágio avançado do programa de redução da distância vertical mínima entre aeronaves em vôo (*reduced vertical separation minimum*),, na perspectiva de que, se algum problema fosse identificado, isto seria levado em consideração pelo programa RVSM (EUROCONTROL, 2006).

De forma análoga, propõe-se que a análise seja feita para sistemas já existentes. Assim, é possível estipular como o sistema deveria ser, para que se possa fazer a tomada de decisão de aceitar ou não um determinado risco – i.e., fazer a **definição dos objetivos de risco**. Para tanto, pode-se utilizar de métricas, como frequência máxima de ocorrência de um evento ou um outro tipo de indicador, tais como:

- 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 expressão 5.1, onde: $\Delta Custo$ é o custo adicional ocasionado pela implementação da barreira; $\Delta Benefícios$ são os benefícios econômicos decorrentes da implementação da barreira; e $\Delta Risco$ é a redução do risco em termos de fatalidades evitadas[2].

[2] Skjong (2002) apresenta algumas considerações e estimativas para NCAF e outros parâmetros para avaliação de custo-risco-benefício.

$$NCAF = \frac{\Delta Custo - \Delta Beneficios}{\Delta Risco} \tag{5.1}$$

Quanto às métricas de frequência, Kumamoto & Henley (1996) propõem alguns critérios para a aceitação do risco, ilustrado na Figura 5.12:

- 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. Caso justifique, o risco pode ser retido e, caso não justifique, a frequência deve ser reduzida até se justificar ou para nível inferior a "L". A justificativa deve ser feita com base no que é razoavelmente praticável em termos de redução do risco (ALARP).

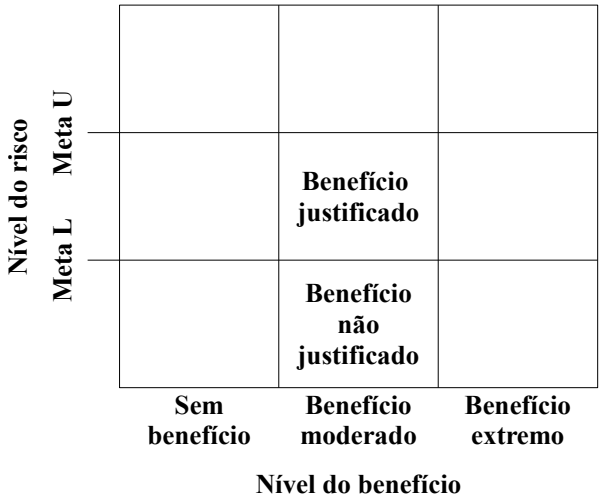


Figura 5.12: Critérios de aceitação de risco
Fonte: Kumamoto & Henley (1996, p. 38, tradução nossa)

O conceito de benefício está relacionado com a utilidade do risco. Em uma guerra, por exemplo, a probabilidade de se ter vítimas é extremamente alta (certamente acima de "U"); no entanto, alguns consideram de "benefício extremo"[3]. Assim, o risco é relutantemente aceito por

[3]Este exemplo foi colocado no texto porque deixa claro o conceito de utilidade do risco. No entanto, destaca-se que o autor não corrobora esta opinião.

eles (KUMAMOTO; HENLEY, 1996, p. 37).

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. Como limites, Kumamoto & Henley (1996) sugerem que se adote $L = 10^{-6}/[ano, individuo]$ e $U = 10^{-3}/[ano, individuo]$; no entanto, estes limites variam de autor para autor e de área de aplicação.

Caso tenha sido definido algum objetivo na análise do nível superior, ele deve ser considerado na FHA e incluído nos objetivos de aceitação de risco do sistema – por exemplo, na análise da unidade organizacional foi definido um MTO para um determinado sistema técnico.

É importante destacar que 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.

Por fim, destaca-se que a análise da função global permite identificar a dependência de algum outro sistema. Assim, ao definir os objetivos de risco, deve-se considerar esta dependência. Por exemplo: pode-se concluir que é necessário que alguns sistemas técnicos tenham uma determinada disponibilidade, para que a unidade organizacional que se está analisando atinja a continuidade operacional desejada. Desta forma, um dos resultados desta fase pode ser a definição de requisitos para outros sistemas (de mesmo nível ou inferior). Portanto, ao iniciar a análise de um determinado sistema, deve-se - primeiramente - verificar se foi determinado algum requisito anteriormente.

5.3.1.2 Fase do delineamento conceitual

Esta fase – ilustrada no Quadro 5.2, na Figura5.7 e na Figura5.8 – tem como objetivo definir os conceitos das soluções para o risco, i.e., se ele deve ser aceito ou tratado e como fazer isso.

Na **análise funcional**, nesta fase – que é a continuação da anterior –, é feito o desdobramento até a resolução desejada, a fim de obter o detalhamento da caracterização do sistema. Como resultado da IDEF0, podem-se levantar os processos (funções) e recursos (mecanismos e controles) críticos para que o sistema cumpra seus objetivos. No caso da análise funcional de produto, tem-se como resultado uma lista contendo a identificação dos componentes e as respectivas funções que cada um deve desempenhar.

Para executar a **análise de risco**, recomenda-se o uso da estrutura FMECA / CNEA[4]. Substituindo o evento central da CNEA pelo modo de falha e fazendo algumas adaptações, o diagrama da CNEA permite uma visualização gráfica da FMECA. Os modos de falha podem,

[4]Ou FMEA, caso não se avalie a criticidade.

Quadro 5.2: Entradas, processos, técnicas & ferramentas e saídas para a fase de delineamento conceitual

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Sistema em análise caracterizado. ■ Objetivos frente aos riscos.	■ Análise funcional. ■ Análise dos riscos. ◇ Identificação do modo de falha, causas, efeitos e controles existentes. ◇ Modelagem das correntes causais usando a estrutura FMECA/CNEA. ■ Avaliação e priorização dos riscos pela análise da criticidade. ■ Proposição de barreiras de tratamento e de aceitação ativa. ■ Avaliação custo-risco-beneficio das barreiras. ■ Reavaliação da criticidade dos cenários considerando as barreiras. ■ Priorização e categorização das barreiras.	■ Banco de dados. ■ *Brainstorming*. ■ Questionários. ■ Análise funcional (IDEF0 ou análise funcional de produto). ■ Modelo da corrente causal proposto por Mosleh et al. (2004). ■ FMEA / FMECA. ■ CNEA. ■ FTA. ■ Redes bayesianas. ■ Atualização bayesiana.	■ Conhecimento estruturado: ◇ Detalhamento da caracterização do sistema. ◇ Delineados dos cenários dos riscos ■ Barreiras priorizadas e classificadas.

então, ser modelados em correntes causais e diagramados na CNEA.

Destaca-se que se podem diagramar as várias correntes causais relacionadas a um determinado incidente em uma única CNEA, conforme apresentado na Seção 4.9.

Adicionalmente, para a adequação do diagrama CNEA à tabela FMECA, foram feitas as seguintes adaptações: diferenciação da cor das barreiras "controle atual" e "ação proposta" e inclusão dos índices da FMECA (S, O, D e NPR), conforme ilustrado na Figura 5.13.

Note-se que o índice de severidade "S" refere-se a todos os efeitos e, portanto, está representado no nódulo de origem deles: o modo de falha. Os índices de ocorrência "O", de dificuldade de detecção "D" e o número de prioridade de risco "NPR" estão representados junto às causas, pois é onde inicia cada cenário[5]. Assim, a dificuldade de detecção, por exemplo, se refere a todos os controles existentes, desde as causas até os efeitos.

É interessante destacar que a representação gráfica permite uma melhor contextualização que a tabela e se mostra mais interessante, tanto por proporcionar uma análise mais eficaz quanto por gerenciar melhor o conhecimento gerado – facilitando sua institucionalização.

Destacam-se os seguintes benefícios na utilização do diagrama da CNEA:

- melhora a comunicação entre o analista e outros colaboradores, auxiliando no envolvi-

[5]Entende-se por cenário a cadeia de eventos desde a causa até o efeito. No caso da FMECA, como os efeitos são tratados como um único bloco, cada cenário engloba uma causa, o modo de falha e seus efeitos.

mento 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 intermediários – não apenas causas-raiz e efeitos-finais;
- permite identificar onde um controle atual está atuando na corrente causal – ou uma ação proposta irá atuar;
- apresenta a relação entre as causas e entre os efeitos; e
- melhora a formalização do conhecimento e, consequentemente, o reaproveitamento das informações da análise.

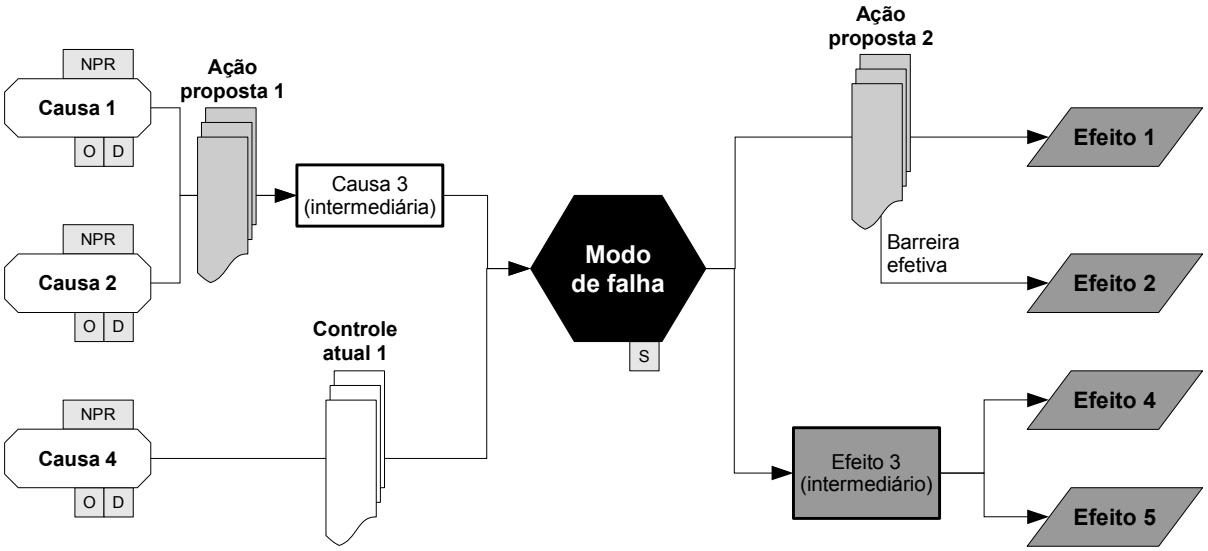


Figura 5.13: Diagrama CNEA adaptado para representar FMECA

Da mesma forma que é feito nas FMECAs, pode-se, também na CNEA, incluir uma FTA (*fault tree analysis*) das causas, para refinar a análise em relação a este fator. Adicionalmente, pode-se, também, fazer FTAs de barreiras – o que possibilita uma melhor compreensão dos "furos" que permitem o desencadeamento do cenário causal.

O primeiro passo na análise de risco é a identificação dos incidentes e dos eventos envolvidos na corrente causal, que usualmente compreende a combinação de técnicas criativas e analíticas, objetivando identificar as situações de risco que já ocorreram no sistema, as que já ocorreram em outros sistemas e as de que não se tem conhecimento de ter ocorrido. Para tanto, podem-se utilizar listas pré-elaboradas, base de dados de risco e técnicas de criatividade – como tempestade de ideias (*brainstorm*). O Quadro 5.3 traz uma lista de alguns perigos com potencial

impacto à segurança e à continuidade / disponibilidade que podem ser considerados na identificação. Uma outra solução para a identificação dos possíveis incidentes é levantar e classificar os perigos relacionados ao sistema em análise, e identificar os incidentes que cada perigo pode desencadear – a exemplo da metodologia para identificação, classificação e análise de perigos em sistemas de aviação elaborado para a FAA (Federal Aviation Administration / United States of America), por Mosleh & Dias (2004).

Quadro 5.3: Lista de perigos com potencial impacto à segurança e à continuidade / disponibilidade

Humanas	
■ acesso indevido aos sistemas/dados	■ greve de funcionários
■ acesso indevido às instalações	■ manuseio indevido de dados críticos
■ ameaça de bomba	■ paralisação de transporte
■ ataque terrorista	■ proximidade à zona de alta criminalidade
■ balão (fogo)	■ proximidade de presídio/delegacia
■ desvio fraudulento de recursos	■ roubo de dados
■ distúrbio civil	■ roubo e/ou furto de patrimônio
■ falha humana (dano não intencional)	■ sabotagem (instalações e dados)
■ greve em prestador de serviço	■ sequestro de funcionário vital
Tecnológicas	
■ acidente aéreo, rodoviário, ferroviário	■ falta de água
■ acidente nuclear	■ pressão (alta, baixa ou descargas rápidas de pressão)
■ acidente químico	
■ oxidação	■ choque mecânico
■ corrosão	■ aceleração
■ explosão	■ energia elétrica (choque, ativação inadvertida, falha da fonte de força, radiação eletromagnética)
■ fogo	
■ radiação (térmica, eletromagnética ionizada, ultravioleta)	■ problema estrutural da instalação
	■ proximidade de instalação militar (com paiol), de gás, de posto de gasolina, de armazenamento de óleo, de central elétrica
■ dissociação química	
■ calor e temperatura (alta ou baixa)	
■ falha de *software* aplicativo	■ falha em *hardware*
■ falha de *software* operacional	■ falha em instalação elétrica
■ falha do sistema de refrigeração	■ falha em rede local
■ falha e/ou rompimento de tubulação (água, gás, vapor)	■ falha em telecomunicação
	■ falha na entrada de dados
■ vazamento (tubulação, o-*ring*, tanques, etc.)	■ vírus
Naturais	
■ avalanche/deslizamento de terra	■ tornado, vendaval
■ chuva de granizo	■ tremor de terra
■ incêndio	■ vazamento em represa
■ inundação, enchente	■ calor e temperatura (alta ou baixa)
■ perda de acesso físico às instalações	■ umidade (alta ou baixa)
■ raio	

Fonte: adaptado de Saldanha (2000) e Kumamoto & Henley (1996)

Caso o incidente já tenha ocorrido, pode-se fazer uso de histórico e da experiência de especialistas, por meio do diagnóstico do incidente – para tanto, recomenda-se o uso de modelos da

literatura, como o de Maurino et al. (1995), por exemplo.

O processo seguinte, então, é a modelagem das correntes causais utilizando a estrutura FMECA / CNEA, já que a CNEA é aderente ao modelo de Mosleh et al. (2004), adotado neste trabalho, para representação de incidentes – vide Seção 4.9.

É interessante destacar que a modelagem do incidente no diagrama da CNEA facilita a tarefa da identificação dos eventos e estados envolvidos – pois permite visualizar a corrente causal. Assim, adicionalmente, o diagrama também facilita a elicitação do conhecimento do especialista, pois atua como uma ferramenta de comunicação.

Note-se que a CNEA modela tanto as causas, que podem ser representadas por uma FT (*fault tree*), quanto as consequências, que podem ser representadas por uma ET (*event tree*) ou ESD (*event sequence diagram*).

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.

A Figura 5.14 apresenta a rede bayesiana[6] equivalente ao diagrama CNEA ilustrado na Figura 5.13, 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[7].

Note-se que as barreiras – ações propostas e controles atuais –, nessa modelagem, entram como nódulos no mesmo nível dos eventos que se pretendem salvaguardar, exemplificado no Quadro 5.4, que ilustra uma tabela de relações para o nódulo “CA3”.

É interessante observar que a estrutura FTA/ETA baseia-se em relações determinísticas (lógica booleana), enquanto que as redes bayesianas podem tratar incertezas nestas relações.

Note-se que o Quadro 5.4 ilustra relações determinísticas; por exemplo: não ocorrendo “CA1”, ocorrendo “CA2” e “PA1” não sendo eficaz, certamente ocorrerá “CA3”.

Nas redes bayesianas, pode-se introduzir incerteza nesta relação e modelar a ocorrência de “CA3”, dada a combinação anterior como: 80% de probabilidade de ocorrer e 20% de não ocor-

[6]Rede editada a partir do *software* JavaBayes, atualmente mantido pelo Prof. Fábio Gagliardi Cozman (Escola Politécnica da USP).

[7]Para melhor entendimento da análise de d-separadores, recomenda-se a leitura de Jensen (2001), Pearl (1988) e UFSC/NeDIP (2008o).

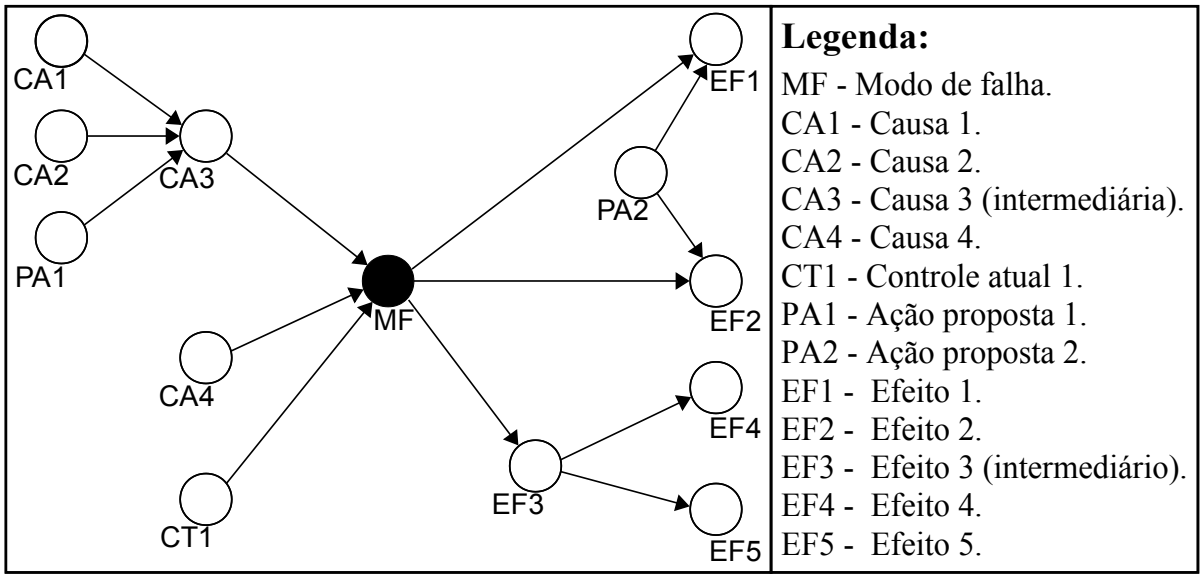


Figura 5.14: Rede bayesiana para o diagrama da Figura 5.13

Quadro 5.4: Tabela de relações do nódulo "CA3" da rede bayesiana da Figura 5.14

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

rer, por exemplo. Com isso, podem-se elaborar modelos com menor incerteza epistemológica[8].

Este recurso é bastante útil na modelagem dos efeitos. Isto porque a ocorrência do EF3, por exemplo, não implica necessariamente a ocorrência do EF4. Neste caso, pode-se modelar a cadeia causal de forma não determinística.

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 5.15, contemplando, assim, os tipos de relações possíveis em uma CNEA.

[8]É importante destacar que o uso de redes bayesianas na modelagem de CNEAs tem uma limitação, apresentada no final da Seção 5.3.3.

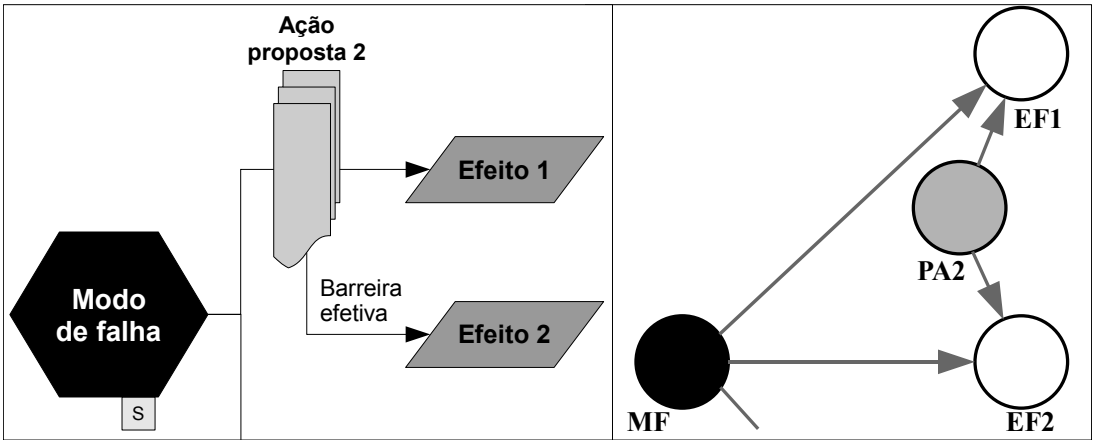


Figura 5.15: Detalhe da barreira com derivação, no diagrama CNEA, e sua modelagem em rede bayesiana

Destaca-se, ainda, que uma das dificuldades de se implementar uma rede bayesiana – e de qualquer análise quantitativa – é a obtenção de estatísticas. Para tanto, pode-se fazer uso de base de dados, simulações ou outro tipo de técnica reconhecida, baseada no conhecimento dos especialistas. Uma técnica que pode auxiliar na obtenção de estimativas para as probabilidades de ocorrência (e para as relações dos eventos / estados) é a atualização bayesiana, apresentada na Seção 4.2.1, na qual se podem conciliar informações subjetivas com os dados de campo.

Na análise dos riscos, faz-se o modelamento de toda a corrente causal, considerando os possíveis resultados de cada incidente – portanto, delineando os cenários de risco. Isso implica trabalhar todo o modelo de ocorrência do risco, desde as causas da condição perigosa e do evento gatilho até as consequências do incidente. Estas consequências (ou efeitos) podem ser, então, classificadas (quanto à segurança, continuidade / disponibilidade, e/ou econômicas / financeiras) e avaliadas no que se refere a sua severidade.

Note-se que não é possível 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.

Essa priorização dos modos de falha, de acordo com a norma SAE-J1739, pode ser feita pela análise do NPR (número de prioridade de risco), que é a multiplicação dos índices de severidade (S), ocorrência (O) e dificuldade de detecção (D). No entanto, esta abordagem tem alguns inconvenientes, tais como:

- A escala não é homogênea – i.e., idêntica no seu todo – pois não permite números primos (não existe uma combinação de índices que resulte no NPR igual a 113, por exemplo), e

um NPR igual a 200 não é necessariamente duas vezes mais crítico que um igual a 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 também – no entanto, a primeira combinação se mostra mais crítica.
- É possível obter NPR relativamente baixo com índices de severidade altos – por exemplo, na combinação S=10, O=3 e D=1.

A fim de minimizar estes inconvenientes, é usual que se leve em consideração não apenas o NPR, mas também o valor do índice de severidade. No entanto, esta análise normalmente é feita de forma subjetiva, sem uma regra clara, e o resultado dependerá da aversão / propensão ao risco do analista.

Propõe-se, então, uma abordagem para categorização da criticidade baseada em relações determinísticas[9], de forma atributiva em substituição à quantitativa. Para possibilitar uma melhor visualização destas regras, pode-se utilizar uma matriz – equivalente à tradicional matriz de criticidade – para cada índice de dificuldade de detecção.

A Figura 5.16 e o Quadro 5.5 ilustram um exemplo dessa abordagem, onde estão respectivamente apresentadas as regras para definição do tratamento a ser dado para cada combinação de índices e as escalas de valores para cada índice.

Note-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.

Quadro 5.5: 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

Uma vez modelados e priorizados os potenciais riscos, podem-se **propor barreiras**, a fim de tratá-los ou de se planejar ativamente para sua ocorrência. Podem-se adotar três estratégias

[9]Para categorização da criticidade considerando variáveis linguísticas, recomenda-se a leitura de Xu et al. (2002) e Garcia (2006), que apresentam abordagens utilizando lógica difusa (*fuzzy*).

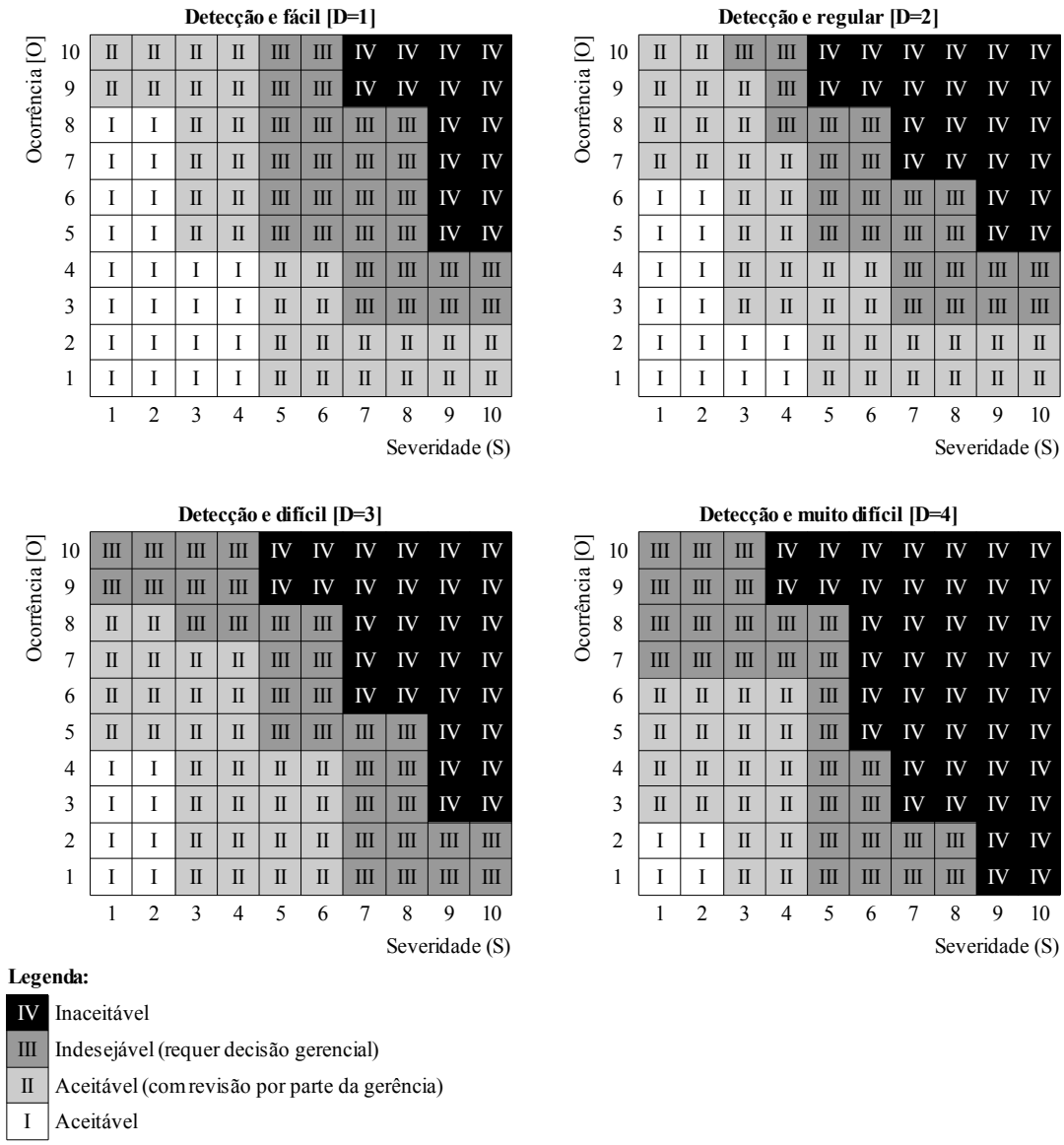


Figura 5.16: Relações determinísticas (regras) para definição do tratamento de cada combinação de índices

de tratamento – não excludentes: (a) evitar o risco; (b) transferir o risco; e (c) reduzir o risco, conforme apresentado no Capítulo 2.

É importante, para a aceitação do risco, considerar a contratação de seguro (transferir o risco) para cobrir os danos causados pelo incidente e, se possível, o lucro cessante decorrente de uma interrupção prolongada.

As barreiras podem, então, ser diagramadas nas CNEAs e inseridas no campo das "ações" nas FMEAs. É interessante que, juntamente com a proposição da barreira, seja feita uma estimativa inicial do seu custo e da disponibilidade de recursos (humanos e materiais) necessários para executá-la. Estas informações serão úteis para a primeira **avaliação custo-risco-benefício** das

barreiras propostas. Assim, com base na comparação das barreiras (na potencial redução dos riscos, nos custos para implementar e nos eventuais benefícios que ela possa gerar) é possível identificar as alternativas mais atraentes.

É importante destacar que, nesta fase, ainda não se tem um levantamento confiável dos custos das barreiras, portanto esta avaliação permitirá identificar apenas as barreiras mais discrepantes.

Caso a modelagem tenha sido feita utilizando-se redes bayesianas, a análise pode ser complementada fazendo-se simulações da implementação das barreiras, a fim de avaliar o impacto da implementação de cada uma delas. Neste caso, pode-se analisar a probabilidade de ocorrência do modo de falha e seus efeitos, considerando a existência da barreira, e comparar com as probabilidades calculadas, atribuindo a evidência de falha ao nódulo que representa a barreira a ser estudada (o que corresponde a ela não existir).

Pode-se, então, avaliar se a redução da probabilidade de ocorrência do modo de falha compensa o esforço necessário para implementação das barreiras. Da mesma forma, procede-se com as barreiras com potencial para mitigar os efeitos.

O passo seguinte é a **reavaliação da criticidade dos cenários considerando as barreiras**, para que se possa verificar se os riscos se tornaram aceitáveis – caso contrário, deve-se retornar à proposição de novas barreiras ou simplesmente reter o risco, mesmo acima do considerado aceitável.

Destaca-se que, após a definição das barreiras, é importante verificar se alterações nas instalações e no *modus operandi* influenciam nos riscos analisados (positiva ou negativamente) ou, ainda, se deflagram novos riscos. Caso isto ocorra, deve-se retornar à analise dos riscos; no entanto, considerando a existência das barreiras.

Uma vez que os cenários dos riscos estão delineados (incluindo as barreiras), é possível verificar as barreiras mais interessantes, tanto no que se refere à segurança quanto à continuidade – fazendo a **priorização delas e posterior classificação**.

Usualmente, a organização não tem 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.

Adicionalmente, é interessante que se adote o aprimoramento contínuo do programa, o que é descrito por Paradies & Unger (2000, p. 15, tradução nossa) como: “Monitorar as estatísticas de desempenho e procurar por áreas potenciais para analisar as razões para as tendências ou problemas de desempenho e, então, corrigi-los.”

Quanto à classificação, ela deve ser feita para orientar a elaboração dos planos preliminares. Assim, as barreiras podem ser classificadas como referentes aos planos de ações; aos planos de monitoramento & controle; aos planos de ações emergenciais; aos planos de operações alternativas; aos planos de retorno; aos planos de comunicação; ou a uma combinação destes.

Observe-se que é sistematizado – ou gerado – um volume considerável de conhecimento, ao final desta fase. Assim, é importante que se tenham recursos para gerenciar este conhecimento, para que ele esteja sempre disponível. Para tanto, destaca-se o uso de *softwares* para dar suporte às técnicas utilizadas. Existe uma diversidade grande de ferramentas computacionais que procuram atender a esta necessidade – algumas delas foram listadas ao final dos textos elaborados pelo NeDIP, listados no (vide Quadro 4.1). Destaca-se, ainda, que o *software* OpenFMECA, que atualmente auxilia na elaboração da FMECA, está sendo restruturado para, no futuro, dar suporte a toda a estrutura de trabalho apresentada nesta seção – o que inclui: IDEF0, FMECA, CNEA e FTA.

5.3.1.3 Fase do delineamento preliminar

Nesta fase, primeiramente, delineiam-se as **ações necessárias para implementar as barreiras**. As ações, juntamente com as barreiras, que resultarem em mudanças nas instalações e na estrutura organizacional devem estar discriminadas nos planos de ação, enquanto as que implicarem a implementação de procedimentos devem ser consideradas na elaboração dos planos de aceitação (monitoramento & controle; resposta emergencial; operação alternativa; e retorno). Por fim, as relativas à capacitação dos colaboradores e à divulgação para as partes envolvidas devem estar apresentadas no plano de comunicação. Assim, tem-se, como saída da fase preliminar, os planos de ação, de aceitação, de comunicação e de crise, como ilustrado no Quadro 5.6 e Figura 5.11.

No delineamento preliminar, faz-se um esboço dos planos (que é a **elaboração dos planos preliminares**). Detalha-se o suficiente para evidenciar o que será necessário para colocá-los em operação. A Figura 2.6 ilustra os quatro planos de aceitação ao longo dos estados de operação de um sistema, para o caso de ativação do plano de operação alternativa.

No plano de monitoramento & controle, incluem-se as barreiras para manter a condição perigosa dentro de limites aceitáveis, além de monitorar a situação a fim de prever a ocorrência do incidente.

O conceito de controle está relacionado com a execução de quatro fases (LEME, 1967): considerar o que foi planejado (condição esperada); considerar o que ocorreu (condição avaliada); confrontar o planejado com o ocorrido; e tomar providências quando necessário (ações para

Quadro 5.6: Entradas, processos, técnicas & ferramentas e saídas para a fase de delineamento preliminar

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Conhecimento estruturado: ◇ Detalhamento da caracterização do sistema. ◇ Delineados dos cenários dos riscos ■ Barreiras priorizadas e classificadas. ■ Objetivos frente aos riscos	■ Delineamento das ações necessárias para implementação das barreiras. ■ Elaboração dos planos preliminares. ■ Estimativa do esforço necessário para a implementação dos planos. ■ Análise custo-risco-benefício. ■ Elaboração do planejamento de implementação.	■ Fluxogramas. ■ Mapas de processo. ■ Mapas mentais. ■ Questionários. ■ FMEA / FMECA. ■ CNEA. ■ Redes bayesianas.	■ Planos preliminares de ação. ■ Planos preliminares de aceitação: ◇ Planos de monitoramento & controle. ◇ Planos de ações emergenciais. ◇ Planos de operações alternativas. ◇ Planos de retorno. ■ Planos preliminares de comunicação. ■ Plano preliminar de gestão de crises.

prevenir que se desencadeie o incidente).

Assim, o plano de monitoramento & 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, a fim de retornar à condição de normalidade.

Infelizmente a ação corretiva nem sempre será possível – ou, quando possível, nem sempre será eficaz –; assim, cabe especificar no plano quando considerar que a situação é emergencial.

Fazem parte de um plano de monitoramento & controle as 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. Por isso, é também denominado plano de mitigação (SALDANHA, 2000).

O plano é um conjunto de ações que tem como objetivo minimizar o impacto nas pessoas, no meio ambiente, no patrimônio e nas funções vitais de uma organização ocasionado por um incidente previsto.

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, por exemplo: condições para o seu acionamento; 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.

O plano de retorno traz as atividades relativas ao restabelecimento das condições normais de operação.

Assim como o plano de operação alternativa, ele deve ser elaborado para cada incidente e, de maneira análoga, definir: condições para o retorno à operação normal; definição da equipe e responsabilidades; transporte e logística; etc.

No que se refere ao plano de ação, é importante que se especifiquem os produtos e serviços a serem adquiridos – isto inclui consultorias e apólice de seguros. Assim, podem-se levantar os custos envolvidos em cada ação.

É importante destacar que o plano de ações deve contemplar a inclusão do sistema de gerenciamento de riscos na organização – uma vez implementado, o sistema permeia a estrutura organizacional. Assim, devem-se atualizar as atribuições dos colaboradores, além de revisar a estrutura organizacional, por exemplo, no caso de se optar por implementar funções dedicadas ao gerenciamento dos riscos.

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

Assim os planos de comunicação devem abranger tanto treinamento teórico como prático – 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 comum existir um relacionamento das ações dos planos de aceitação com outras instituições, como Defesa Civil, Corpo de Bombeiros, assistências técnicas, etc. Assim, 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 contactar, as informações e documentos necessários, etc.

Fazem parte dos planos de comunicação informações como, por exemplo, 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; quem deve ser submetido à capacitação; etc.

Por fim, destaca-se a elaboração do plano de gerenciamento de crise para a organização. Este plano visa fornecer, aos gestores, um conjunto de informações e recursos que podem ser úteis no momento da crise, além de um planejamento de como tratar a mídia.

Ele contempla todo tipo de crises, tais como:

- crises resultantes de incidentes que não foram previstos;
- crises com proporções além do escopo do sistema de gerenciamento de risco;
- uma exposição negativa na mídia causada por um incidente.

O passo seguinte é **estimar qual o esforço necessário para implementação dos planos**. Para tanto, deve-se levar em consideração não apenas o custo, mas também o tempo necessário; a disponibilidade de recursos internos da organização e que devam ser adquiridos; etc. Destaca-se, ainda, que se devem avaliar os esforços referentes à manutenção da estrutura e à capacitação referente aos riscos.

Nesta fase, é necessário fazer um orçamento pormenorizado, pois será com base nestes valores que será planejada a implementação. De fato, deve-se fazer uma **avaliação de custo-risco-benefício**, a fim de priorizar as medidas de tratamento a serem implementadas, e, eventualmente, descartar as não justificadas.

Essa avaliação deve ser baseada nos critérios de aceitação definidos na fase informacional. A ideia é confrontar os benefícios e a redução do risco com os custos das medidas – a fim de verificar se elas são justificáveis e priorizá-las. Por exemplo, uma possível medida para alcançar o MTO 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, esta 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, pode-se fazer 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.

5.3.1.4 Fase do delineamento detalhado

O Quadro 5.7 ilustra o processo do delineamento detalhado. Nesta fase, é feito o detalhamento dos planos preliminares obtidos na fase anterior.

Quadro 5.7: Entradas, processos, técnicas & ferramentas e saídas para a fase de delineamento detalhado

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Planos preliminares de ação. ■ Planos preliminares de aceitação: ◇ Planos de monitoramento & controle. ◇ Planos de ações emergenciais. ◇ Planos de operações alternativas. ◇ Planos de retorno. ■ Planos preliminares de comunicação. ■ Plano preliminar de gestão de crises.	■ Detalhamento dos planos. ■ Testes dos planos.	■ Fluxogramas. ■ Mapas de processo. ■ Mapas mentais. ■ Questionários. ■ Painéis de apresentação. ■ Fichas de atribuições. ■ DMS (*document management system*).	■ Planos de ação. ■ Planos de aceitação: ◇ Planos de monitoramento & controle. ◇ Planos de ações emergenciais. ◇ Planos de operações alternativas. ◇ Planos de retorno. ■ Planos de comunicação. ■ Plano de gestão de crises.

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 deles.

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 muito 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. Neste último caso, recomenda-se que este 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. Neste 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 *softwares* específicos, chamados de DMS (*document management system*)[10]. Saldanha (2000) recomenda, ainda, que a documentação seja reunida e apresenta uma sugestão de estrutura para isto, indicada para organizações de médio porte – vide Quadro 5.8[11]. A publicação em questão se refere a planos de continuidade, mas pode ser uma orientação para a elaboração de planos considerando também a segurança. Adicionalmente, no Anexo A, apresenta-se o plano de aceitação desenvolvido na aplicação da metodologia na empresa Celesc – melhor descrito na Seção 6.3 –, que também pode ser utilizado como referência para a elaboração de novos planos.

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 se faça **teste dos planos** por meio de lista de verificações (*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 eles serem executados.

5.3.2 Etapa de implementação

Nesta etapa, ilustrada no Quadro 5.9, implementam-se os planos elaborados e socializam-se as informações com todas as partes envolvidas, seguindo o planejamento de implementação especificado no plano de ações.

A **implementação dos planos de ação** instala a estrutura necessária para os planos aceitação, tais como: instrumentos para fazer o controle; alterações no organograma; estruturas alternativas que serão utilizadas em uma contingência; etc.

Para uma efetiva implementação do programa, deve-se fazer a devida **capacitação dos colaboradores e a divulgação para as partes interessadas**, conforme determinado no plano de comunicação.

É interessante salientar que se deve evitar o "efeito serrote", no qual os colaboradores são

[10] OpenKM <http://www.openkm.com/> ou KnowledgeTree <http://www.knowledgetree.com/>, por exemplo.

[11] Saldanha (2000) não inclui o plano de retorno nos planos de aceitação.

Quadro 5.8: Sugestão de estrutura para planos de continuidade de uma organização de médio porte

1. Introdução
- 1.1. Objetivo
- 1.2. Premissas utilizadas no plano
- 1.3. Resumo do plano e estrutura do documento
- 1.4. Instalações alternativas

2. Anteprojeto
- 2.1. Avaliação do impacto de um desastre
- 2.2. Avaliação do grau de exposição
- 2.3. Estratégia de continuidade

3. Estruturação dos planos
- 3.1. Plano de monitoramento e controle
- 3.2. Plano de resposta emergencial
- 3.3. Plano de contingência
  - 3.3.1. Definição dos requisitos do ambiente alternativo
  - 3.3.2. Definição de alterações nas instalações usuais
  - 3.3.3. Definição dos recursos de telecomunicações adicionais
  - 3.3.4. Definição dos procedimentos operacionais adicionais no dia a dia
  - 3.3.5. Procedimentos da equipe da contingência
    - Procedimentos da equipe de suporte técnico
    - Procedimentos da equipe de apoio
    - Equipe de operações
  - 3.3.6. Procedimentos de operação em regime de contingência
    - Procedimentos da equipe de suporte técnico
    - Procedimentos da equipe de apoio
    - Equipe de operações

4. Planos de implantação
- 4.1. Contratos com prestadores de serviço
- 4.2. Obtenção e implementação de recursos
- 4.3. Montagem e treinamento das equipes

5. Anexos
- 5.1. Relação de pessoal de contingência
- 5.2. Relação de fornecedores
- 5.3. Relação de equipamentos padrão
- 5.4. Relação de mobiliário padrão
- 5.5. Relação de telefones úteis

Fonte: Saldanha (2000, p. 219)

motivados, mas não se implementa o programa adequadamente – resultando em desmotivação. Então, faz-se uma nova investida na capacitação e assim por diante.

Também deve ser construído um contexto para se desenvolver a cultura do gerenciamento de risco – a ser integrada ao *modus operandi* da organização.

Uma vez que se tenha instalada a estrutura necessária para execução dos planos, é necessário fazer **simulações do uso dos planos de aceitação**. A execução do plano possibilitará que as pessoas envolvidas estejam melhor preparadas e aumentará a conscientização de todos os colaboradores, além de evidenciar deficiências e possíveis melhorias. Podem-se fazer es-

Quadro 5.9: Entradas, processos, técnicas & ferramentas e saídas para a etapa de implementação

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Planos de ação. ■ Planos de aceitação: ◇ Planos de monitoramento & controle. ◇ Planos de ações emergenciais. ◇ Planos de operações alternativas. ◇ Planos de retorno. ■ Planos de comunicação. ■ Plano de gestão de crises.	■ Implementação dos planos de ação. ■ Capacitação dos colaboradores e divulgação para as partes interessadas. ■ Simulações do uso dos planos de aceitação.	■ Painéis de apresentação. ■ Fichas de atribuições. ■ DMS (*document management system*).	■ Reestruturação conforme previsto no plano de ação. ■ Rotinas de monitoramento & controle implementadas. ■ Colaboradores capacitados. ■ Partes envolvidas conscientizadas. ■ Relatório dos testes dos planos de aceitação.

ses testes 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; devem-se exercitar os participantes, idealmente, a ponto de os procedimentos serem executados de maneira automática e intuitiva.

É importante observar que é possível chegar à conclusão, após a execução das 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. Neste caso, deve-se deflagar uma revisão do SGR (Seção 5.3.4), para verificar se a situação real, após a implementação das barreiras, é aceitável ou se serão necessárias novas barreiras.

5.3.3 Etapa de utilização

Nesta etapa, além da utilização dos planos de aceitação (monitoramento & controle, resposta emergencial, operação interina e retorno à operação normal), também deve-se fazer: a manutenção da estrutura necessária para executá-los e os testes e simulações do uso dos planos de aceitação – conforme apresentado no Quadro 5.10.

No que se refere à **utilização dos planos de aceitação**, prevê-se a execução do plano de monitoramento & controle durante a operação normal – idealmente, estas ações devem estar nas atribuições cotidianas dos colaboradores, conforme ilustrado na Figura 5.17.

Quadro 5.10: Entradas, processos, técnicas & ferramentas e saídas para a etapa de utilização

Entradas	Processos	Técnicas e ferramentas	Saídas
■ Reestruturação da organização, conforme previsto no plano de ação. ■ Planos de aceitação e de crise testados. ■ Rotinas de monitoramento &controle implementadas. ■ Colaboradores capacitados. ■ Partes envolvidas conscientizadas.	■ Utilização dos planos de aceitação. ■ Testes e simulações do uso dos planos de aceitação. ■ Manutenção da estrutura necessária para a execução dos planos.	■ Fluxogramas. ■ Mapas de processo. ■ Mapas mentais. ■ Questionários. ■ Painéis de apresentação. ■ Fichas de atribuições. ■ DMS (*document management system*). ■ Redes bayesianas.	■ Colaboradores capacitados. ■ Partes envolvidas conscientizadas. ■ Identificação de deficiências ou melhorias nos planos. ■ Identificação de novos riscos ou novas informações sobre os riscos já analisados. ■ Relatórios de execução dos planos.

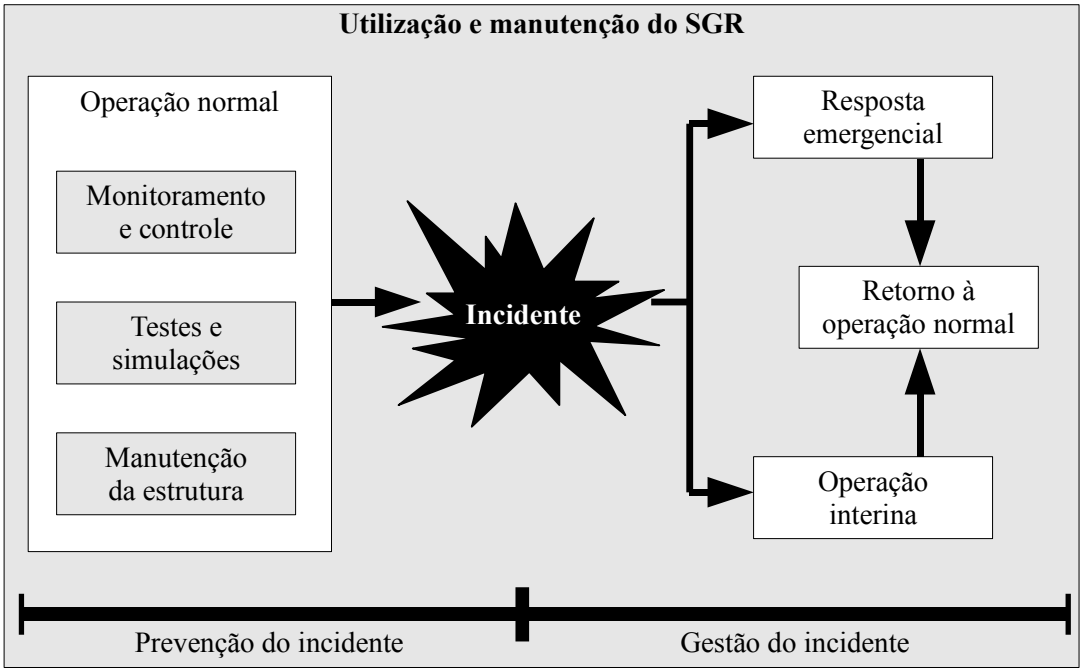


Figura 5.17: Utilização e manutenção do sistema de gerenciamento de riscos

No caso de o incidente ser desencadeado, podem-se executar os planos de resposta emergencial ou operação interina (alternativa) e, ao final, pode-se retornar à condição normal de operação.

Note-se que não foi representada a execução do plano de gerenciamento de crises, pois este contempla situações fora das previstas nos planos de aceitação elaborados.

Os **testes e simulações** e a **manutenção da estrutura** visam manter a capacidade de res-

posta 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 resposta emergencial, de operação interina e de retorno devem ser exercitados conforme previsto nos planos de comunicação. Estes exercícios possibilitam: avaliar a capacitação dos colaboradores e manter a execução das ações de forma automática; identificar problemas de transferência de informações ou outra deficiência de comunicação; destacar pressuposições que precisem ser questionadas; manter o nível de conscientização da organização e das partes envolvidas; etc.

É importante monitorar as mudanças culturais, a fim de avaliar a qualidade e a eficácia da capacitação e da conscientização das partes afetadas. Caso se constate alguma deficiência, os planos de capacitação também devem ser revistos.

Note-se que, além de evidenciar deficiências, a utilização dos planos também permite identificar possíveis melhorias. Estas também devem desencadear a revisão do SGR.

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

Destaca-se, ainda, que é possível utilizar as redes bayesianas elaboradas para fazer diagnóstico – encadeamento reverso, contrário ao sentido das setas. A rede ilustrada na Figura 5.14 é bastante simples, mas permite verificar quais as causas mais prováveis para a ocorrência do "modo de falha", por exemplo. Para isso, entra-se com a evidência de que ocorreu o "modo de falha" e avalia-se a probabilidade de ocorrência das causas.

Estas simulações utilizando as redes bayesianas podem ser feitas nesta etapa para aumentar o conhecimento dos colaboradores sobre os riscos modelados ou como ferramenta para diagnóstico.

É importante destacar que a modelagem de CNEAs em redes bayesianas traz uma limitação: não se pode utilizar a rede para fazer diagnóstico dos efeitos. Esta limitação existe, pois, no modelo apresentado na Figura 5.14, o único nódulo que pode desencadear a ocorrência do "EF1 – Efeito 1", por exemplo, é o "modo de falha". Assim, caso se entre com a evidência de que

ocorreu EF1, obrigatoriamente deve ocorrer o "modo de falha" – o que não é necessariamente verdade, pois outros modos de falha também podem acarretar o mesmo efeito.

Para que o modelo representasse a realidade neste aspecto, devem-se incluir todos os modos de falha que podem levar àquele efeito, o que oneraria muito a elaboração do modelo. Desta forma, neste trabalho, optou-se por limitar o uso do modelo, não analisando encadeamento reverso para os efeitos.

Salienta-se que esta restrição cabe apenas aos efeitos, sendo possível fazer encadeamento reverso para causas e modo de falha.

5.3.4 Etapa de revisão do SGR

Consiste no redelineamento do sistema de gerenciamento de risco e na implementação das alterações que devem ser feitas para seu aprimoramento e atualização – o Quadro 5.11 ilustra este processo.

Quadro 5.11: Entradas, processos, técnicas & ferramentas e saídas para a etapa de revisão do SGR

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Identificação de deficiências ou melhorias nos planos. ■ Identificação de novos riscos ou novas informações sobre os riscos já analisados. ■ Documentação do sistema de gerenciamento de risco.	■ Os mesmos executados durante a etapa de delineamento e implementação (não necessariamente todos).	■ Equivalentes às utilizadas durante a etapa de delineamento e implementação.	■ Sistema de gestão de risco revisado. ■ Identificação de parte do SGR a ser desativada.

As atualizações devem ser feitas sempre que houver alteração significativa na organização ou que 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, novos riscos identificados, etc.

O aprimoramento deve ser feito para corrigir deficiências identificadas e para alcançar a melhoria contínua (sempre que for identificada alguma possível melhoria ou periodicamente), visando aperfeiçoar os planos, ampliar o escopo (identificando novos riscos), revisar as tomadas de decisões anteriores, etc.

O objetivo da revisão do 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, que não é mais necessária.

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 que sejam repetidos todos os processos do delineamento e implementação, pois se pode concentrar nos pontos que podem ser influenciados pelo fato 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. Por exemplo, em uma revisão, opta-se pelo uso da estrutura FTA / ETA em substituição à CNEA.

Destaca-se, ainda, que 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. Neste sentido, deve haver um comprometimento dos colaboradores na busca do aprimoramento contínuo.

5.3.5 Etapa de desativação

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 considerado desprezável. O Quadro 5.12 ilustra o processo de desativação.

Quadro 5.12: Entradas, processos, técnicas & ferramentas e saídas para a etapa de desativação

Entradas	Processos	Técnicas & ferramentas	Saídas
■ Risco eliminado ou risco considerado desprezável. ■ Sistema de gestão de risco revisado.	■ Arquivamento das informações e "lições aprendidas".	■ DMS (*document management system*).	■ Documentação disponível para consulta.

Note-se que a desativação de uma parte do sistema de gestão de risco somente é razoável como um resultado da revisão do SGR, pois neste processo pode-se concluir que certos procedimentos – ou estruturas – não são mais necessários.

Assim, o processo de desativação em si compreende o arquivamento das informações e "lições aprendidas", para que elas possam ser reaproveitadas no futuro, uma vez que a recapaci-

tação dos colaboradores, divulgação para as partes envolvidas e outras ações para readequação do SGR fazem parte da etapa de revisão.

5.4 Ferramenta computacional OpenFMECA

Está sendo elaborado, no NeDIP / UFSC, desde outubro de 2006, um *software* chamado OpenFMECA, a fim de auxiliar no uso da técnica FMECA. Esta ferramenta – melhor descrita no Apêndice A – tem código fonte aberto (*open source*), o que possibilita que outras instituições e usuários possam livremente utilizá-la e / ou aprimorá-la.

O *software* foi concebido para ser instalado em um servidor e utilizado via navegador de internet de qualquer local (desde que tenha conexão com a internet) ou em qualquer sistema computacional (PCs, *palmtops*, etc.). Com isto, pode-se elaborar a FMECA de forma distribuída, na qual mais de uma pessoa pode trabalhar na mesma FMECA, em postos de trabalho diferentes. Nesta condição, o OpenFMECA passa a ser utilizada como uma ferramenta colaborativa, permitindo que se faça a análise de maneira não presencial, eliminando – ou, pelo menos, minimizando – a necessidade das reuniões.

As duas primeiras versões do *software* foram feitas com o objetivo de dar suporte, exclusivamente, à utilização da técnica FMECA[12]. Nestas versões, pode-se estruturar melhor a análise – pois usa uma hierarquia na forma de árvore – e, adicionalmente, é possível incluir uma descrição mais detalhada de cada elemento da FMECA[13], atenuando um dos inconvenientes relacionados com a representação em tabelas.

Atualmente, está sendo desenvolvida a terceira versão do *software* (versão α.3), que objetiva dar suporte á estrutura de trabalho (*framework*) proposta neste doutorado, apresentada na Seção 5.3.1, que associa a FMECA a outras técnicas – a saber: CNEA, IDEF0, redes bayesianas e FTA.

Esta integração das técnicas permitirá que o *software* reúna as informações referentes ao gerenciamento de risco em um único sistema, atuando como uma ferramenta de gestão do conhecimento. Ademais, pelo fato de o OpenFMECA atuar também como ferramenta colaborativa, podem-se incluir na análise pessoas que tenham dificuldade de participar das reuniões – como um especialista de fora da organização, por exemplo. Usualmente a técnica FMECA requer um trabalho de equipe contendo vários especialistas, de diferentes formações e setores de trabalho, de modo que cada membro contribua com diferentes experiências e conhecimentos.

[12] A segunda versão do *software* foi uma reimplementação, objetivando melhorar a rapidez e o projeto gráfico.

[13] Pretende-se, em uma próxima versão, implementar a possibilidade de anexar arquivos a cada elemento, por exemplo, fotografias, árvores de falha, etc.

As reuniões, que normalmente são longas (em muitos casos enfadonhas), exigem a presença de todos os envolvidos em horários pré-determinados, concorrentes com as atividades diárias – o que pode tornar-se um entrave para o desenvolvimento da técnica, pois exige que se concilie a agenda de todos os participantes. Esse tempo despendido nas reuniões potencializa um outro inconveniente: gerar ansiedade na equipe, o que pode resultar em uma análise superficial e comprometer os resultados. Assim, o uso do OpenFMECA pode ser uma alternativa para atenuar este inconveniente da técnica – a Seção A.2.2 traz alguns outros aspectos relevantes do *software*.

É interessante destacar que o desenvolvimento do OpenFMECA foi deflagrado por este trabalho de doutorado; no entanto, o *software* passou a ser utilizado em outras pesquisas e, hoje, tornou-se um projeto à parte dentro do NeDIP / UFSC, integrando outros colaboradores[14].

5.5 Considerações finais

No Capítulo 5, apresentou-se a metodologia para gerenciamento de risco considerando os atributos segurança e continuidade / disponibilidade. Uma vez que o sistema de gerenciamento de risco (SGR) pode ser entendido como um produto a se desenvolver, a metodologia apresentada foi elaborada seguindo a estrutura do PDP (processo de desenvolvimento de produto), destacadamente a etapa de delineamento, que foi baseada no modelo PRODIP[15].

A metodologia, então, está estruturada em 5 etapas: etapa de delineamento, etapa de implementação, etapa de utilização, etapa de revisão do SGR e etapa de desativação, sendo a etapa de delineamento subdividida em 4 fases: fase do delineamento informacional, fase do delineamento conceitual, fase do delineamento preliminar e fase do delineamento detalhado. Na etapa de delineamento, elaboram-se os planos: plano de ação, que define as alterações necessárias para a adequação da organização (incluindo o planejamento para a implementação delas); os planos de aceitação (planos de monitoramento & controle, de resposta emergencial, de operações alternativas e de retorno); os planos de comunicação; e o plano de gestão de crises. Na etapa seguinte, implementam-se os planos elaborados e socializam-se as informações com todas as partes envolvidas, seguindo o planejamento de implementação especificado no plano de ações. Na utilização, os planos são colocados em prática – quer pela ocorrência do incidente, quer pela execução de simulações –, e é feita a manutenção da estrutura do SGR. Na etapa de

[14] A equipe do projeto OpenFMECA é atualmente coordenada pelo Professor Acires Dias e composta por: Luís Fernando Peres Calil; Eduardo Yuji Sakurada; Heitor Azuma Kagueiama; Leonardo Mecabô; Gleber Estefani Diniz; Daniel Koudi Nakano; e Glauco Vinicius Gil Peron. Também fizeram parte do desenvolvimento do *software*: André Ogliari (como coordenador); Emerson Rigoni; e Thiago Nass de Holanda.

[15] Para detalhes sobre o modelo PRODIP, recomenda-se a leitura de Back et al. (2008).

revisão, por sua vez, faz-se a atualização e o aprimoramento do sistema de gerenciamento de risco, o que pode levar à conclusão de que parte dele não é mais necessária. Assim, na etapa de desativação, é feito o arquivamento das informações e das "lições aprendidas", para que elas possam ser reaproveitadas no futuro.

Note-se que a norma ABNT/ISO/IEC Guia 73 (ABNT, 2005) indica que o gerenciamento de risco contempla a análise / avaliação, o tratamento, a aceitação e a comunicação do risco. Estes quatro pontos são contemplados na metodologia desenvolvida; no entanto, não estão claramente definidos na estrutura. A aceitação, por exemplo, é feita na fase do delineamento conceitual, mas é revista no preliminar, quando se tem condição de estimar melhor os custos das medidas de redução e planejamento dos riscos – permitindo fazer uma avaliação de custo-risco-benefício, e, eventualmente, descartar uma ação (que extrapole o NetCAF, por exemplo). Já os parâmetros para a aceitação são delineados na fase informacional.

De forma análoga, é possível observar que os processos das metodologias apresentadas no Capítulo 3 – tanto no que se refere à gestão da segurança quanto à gestão da continuidade – estão, de certa forma, contemplados ao longo da metodologia desenvolvida, já que esta foi baseada nas metodologias estudadas.

É importante observar que a integração das questões relacionadas à segurança e à continuidade / disponibilidade, em um único sistema de gerenciamento de riscos, possibilita gerenciar melhor os recursos da organização, pois, no planejamento da implementação, podem-se priorizar as medidas de maneira geral, tornando a alocação de recursos mais clara e menos subjetiva, tanto nos casos em que a continuidade / disponibilidade de um item favorece a segurança quanto quando estes atributos são antagônicos.

Uma das reclamações na implementação de sistemas de gerenciamento de continuidade está exatamente na questão de quanto se deve direcionar para ele. Cifras consideráveis são injetadas para garantir a continuidade. No entanto, fora de um gerenciamento mais amplo, não é possível analisar com clareza se este investimento teria sido melhor alocado na redução da probabilidade de ocorrer um incidente com repercussão na segurança, por exemplo. É importante salientar que as questões relativas à segurança devem ter prioridade à continuidade / disponibilidade.

Por fim, destaca-se o desenvolvimento da estrutura de trabalho apresentada na Seção 5.3.1, que reúne as seguintes técnicas e ferramentas:

- Análise funcional IDEF0 (*integration definition for function modeling*) ou análise funcional de produto para a caracterização do sistema.
- FHA (*functional hazard assessment*) para o levantamento dos objetivos de risco.

- Modelo da corrente causal (MOSLEH et al., 2004) e CNEA (*causal network event analysis*) para a análise do incidente.
- FTA (*fault tree analysis*) como uma alternativa para a análise de causas que se necessitem detalhar e de falhas em barreiras.
- Categorias de risco por relações determinísticas para análise da criticidade.
- Redes bayesianas para fazer o tratamento estatístico das CNEAs.
- Atualização bayesiana para estimar o valor da probabilidade de ocorrência dos eventos nas CNEAs e nas FTAs.
- FMECA (*failure modes effects and criticality analysis*) como integração dos incidentes (ou modos de falha) identificados; da listagem de causas e efeitos; da indicação das barreiras existentes (controles atuais); da análise de criticidade; e da proposição de barreiras (ações propostas) para reduzir o risco ou mitigar as consequências – bem como a reavaliação da criticidade após a implementação das barreiras propostas.

Esta estrutura de trabalho, então, poderá ser suportada pelo *software* OpenFMECA que, no futuro, prevê a integração de todos estes pontos.

6 *Aplicação da metodologia de gerenciamento de risco desenvolvida*

As aplicações da metodologia foram realizadas ao longo de sua elaboração, em dois estudos de caso: o primeiro realizado em um projeto com a Celesc (Centrais Elétricas de Santa Catarina S.A.), em 2005, e o segundo em um projeto com a Eletrosul Centrais Elétricas S.A., em 2007 e 2008.

Note-se que, no projeto com a Eletrosul, a metodologia já estava bem desenvolvida e pode-se fazer uma aplicação fiel à estrutura e às recomendações apresentadas no Capítulo 5.

Na Celesc, entretanto, o projeto foi realizado na forma de uma pesquisa qualitativa tipo pesquisa-ação, e um dos resultados foi uma primeira estruturação para a metodologia. Assim, a estrutura apresentada no Capítulo 5 não foi integralmente aplicada, principalmente no que se refere ao delineamento informacional e conceitual. No entanto, é importante destacar que os processos referentes à elaboração dos planos já estavam definidos, pois foram baseados na pesquisa bibliográfica realizada. Desta forma, o projeto com a Celesc ilustra o delineamento dos planos preliminares e detalhados, conforme apresentado no capítulo anterior, e evidencia considerações importantes.

O objetivo do projeto com a Celesc era montar uma estrutura que permitisse à empresa restabelecer o fornecimento de energia mais eficientemente, na ocorrência de uma tempestade severa. Esta estrutura foi implementada e está sendo utilizada com bons resultados pela empresa.

O projeto com a Eletrosul, por sua vez, objetivou levantar barreiras na perspectiva de mitigar a emissão de SF_6 (hexafluoreto de enxofre) para a atmosfera. Observe-se que este levantamento está inserido na fase do delineamento conceitual do sistema de gerenciamento de risco. De fato, neste projeto, a metodologia foi aplicada até o início da fase do delineamento preliminar. Portanto, não se chegou a elaborar os planos, mas foram indicadas as ações e recomendações que deveriam constar nos planos preliminares – à exceção dos procedimentos de operação de um equipamento de tratamento de SF_6, em que foram elaborados procedimentos de operação

com o devido detalhamento.

É importante observar que, na Celesc, a aplicação ocorreu no nível da unidade organizacional, no caso nos CODs (centros de operação da distribuição), e, na Eletrosul, ocorreu nos níveis da unidade organizacional e do sistema técnico, no DMS (Departamento de Manutenção do Sistema) e em um modelo de disjuntor, respectivamente – conforme ilustrado na Figura 6.1.

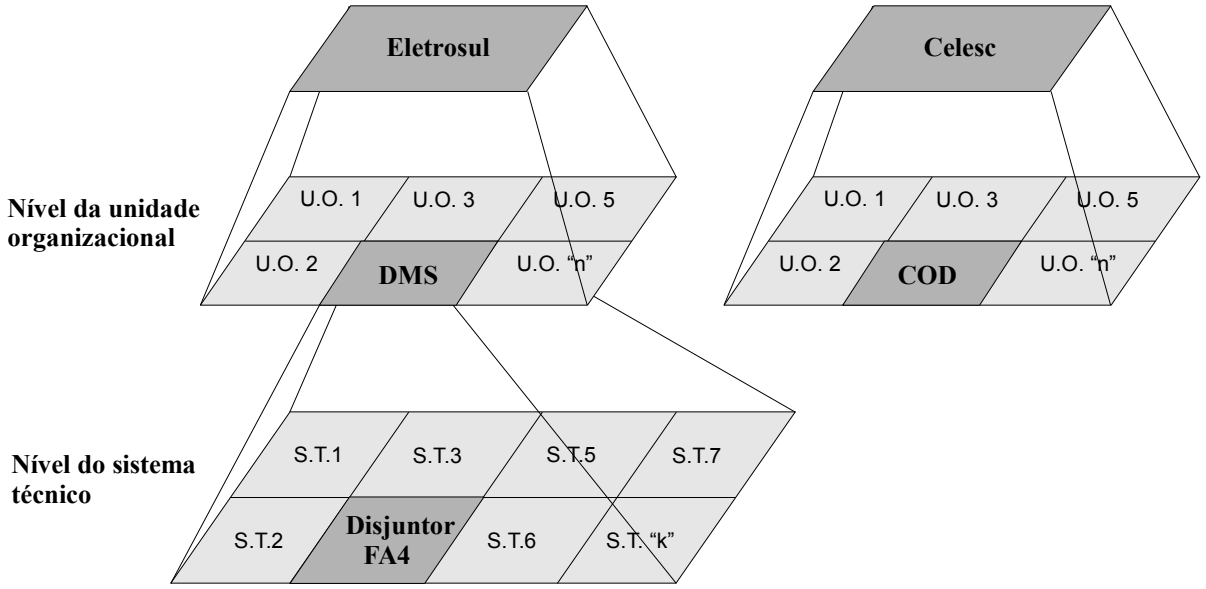


Figura 6.1: Contextualização das aplicações nas empresas Eletrosul e Celesc

Desta forma, não foi feita uma aplicação no nível da organização. No entanto, a metodologia desenvolvida pode ser adaptada a esta realidade, o que possibilitaria uma gestão do negócio mais estruturada.

Por fim, destaca-se que, na medida do possível, os textos das aplicações foram elaborados seguindo a sequência indicada nos fluxogramas apresentados no Apêndice 5.2.

6.1 Aplicação na Eletrosul, no âmbito da unidade organizacional

A aplicação na Eletrosul ocorreu em 2007 e 2008, com o projeto ANEEL intitulado MitiSF6. Este projeto teve como objeto de estudo identificar os pontos de perda de SF_6 e propor soluções para mitigá-la; portanto as análises se concentram nas questões relativas ao gás.

Neste sentido, o projeto foi dividido em duas frentes: uma para estudar as perdas durante a operação dos equipamentos elétricos isolados a SF_6, e outra para estudar as perdas durante a

manipulação do gás e manutenção dos equipamentos. A primeira está apresentada na Seção 6.2, pois se refere ao sistema técnico, e a segunda, que se refere a questões organizacionais, será apresentada a seguir.

É interessante enfatizar que a aplicação da metodologia foi feita até a fase do delineamento preliminar – conforme Figura 6.2 –; desta forma, a fase do delineamento detalhado e as outras etapas serão omitidas nesta seção.

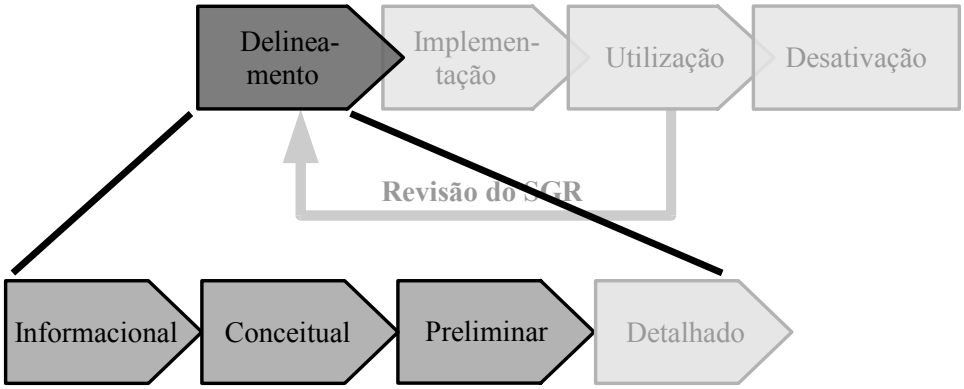


Figura 6.2: Fases da metodologia abordadas na aplicação no DMS da Eletrosul

6.1.1 Contextualização do problema

O SF_6 é utilizado como dielétrico em equipamentos de transmissão e distribuição de energia elétrica. Desta forma, a continuidade da transmissão e distribuição depende deste gás.

Para a Agência de Proteção Ambiental norte-americana (EPA – Environmental Protection Agency), propriedades como: estrutura molecular extremamente estável, alta resistência dielétrica, grande habilidade extintora, excelente capacidade isolante, etc. fazem do SF_6 o dielétrico preferido nos equipamentos de alta-voltagem –; com isso, perto de 80% da produção de SF_6 é destinada ao setor elétrico (EPA, 2003). No entanto, nesta mesma publicação, ela alerta para o fato de o gás ser 23900 vezes mais efetivo que o CO_2 para o efeito-estufa (considerando um período de 100 anos), conforme ilustrado no Quadro 6.1[1] , sendo que sua vida na atmosfera é de aproximadamente 3200 anos.

Apesar de a contribuição atual para o efeito estufa ser baixa – em 2002, estima-se que a emissão de SF_6 pelo setor elétrico foi responsável por 11% do total da emissão de gases de alto potencial efeito-estufa[2] proveniente de processos industriais (EPA, 2003) –, o SF_6 é o gás

[1] Foi publicada uma errata em 31 julho de 2008 com a inclusão de alguns valores e tipos de gases, mas o conteúdo apresentado no Quadro 6.1 – que foi extraído da "Table 2.14" – não sofreu alterações.

[2] *Global warming potential* (GWP).

Quadro 6.1: GWP de alguns gases para 100 anos de horizonte de tempo

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	$CC_{l2}FCC_lF_2$	4.800
HFC-23	CHF_3	11.700
HFC-32	CH_2F_2	650
HFC-125	CHF_2CF_3	2.800
HFC-134a	CH_2FCF_3	1.300
HFC-143a	CH_3CF_3	3.800
HFC-152a	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

Fonte: UNO/IPCC (2007, p. 212 e 213, tradução nossa)

com maior potencial de dano no que se refere ao efeito-estufa, o que levou a sua inclusão no Protocolo de Kyoto (UNO/UNFCCC, 1998). O Brasil é signatário deste protocolo e, no Decreto n° 5.445, de 12/05/2005, estipula que ele "[...] será executado e cumprido tão inteiramente como nele se contém." (BRASIL, 1998a).

Destaca-se que alguns países já possuem regulamentação própria para o 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 (UNIÃO EUROPEIA, 2006); 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 de estufa em comutadores de alta tensão" (UNIÃO EUROPEIA, 2008, p. 17), i.e., o gás SF_6.

No Brasil, ainda não existe nenhuma publicação neste sentido, mas um dos resultados finais deste projeto foi a recomendação, para a ANEEL, de se regulamentar o controle do uso e a qualificação do pessoal que manipula o gás.

Outra questão a ser considerada é o custo da perda de SF_6. O gás é importado, e o preço sofreu aumentos significativos – próximo de 600% em 2 anos, até 2004 (ENERVAC, 2004) –,

constituindo-se aí uma motivação a mais para mitigar sua emissão.

Por fim, destaca-se que a redução da emissão de SF_6 pode viabilizar crédito de carbono.

Diante deste cenário, foi proposto um projeto com o objetivo de mitigar a perda de SF_6 na Eletrosul. Como o projeto foi realizado dentro do programa de pesquisa e desenvolvimento (P&D) da ANEEL, os resultados podem ser utilizados por todo o setor elétrico brasileiro.

No que se refere à manipulação do gás, observou-se, em outros estudos, que este é o ponto com maior potencial de redução de perdas. O programa norte-americano de redução de perdas de SF_6, por exemplo, obteve uma redução na taxa de emissão próxima de 50% em 8 anos – vide Figura 6.3 –, majoritariamente pela redução de perdas na manipulação (EPA, 2006).

Especificamente na Eletrosul, a manipulação é feita pelo Departamento de Manutenção do Sistema (DMS). Assim, optou-se por aplicar a metodologia nesta unidade organizacional. Note-se que, paralelamente, também foi feita a aplicação no âmbito do sistema técnico, em um disjuntor (apresentada na Seção 6.2).

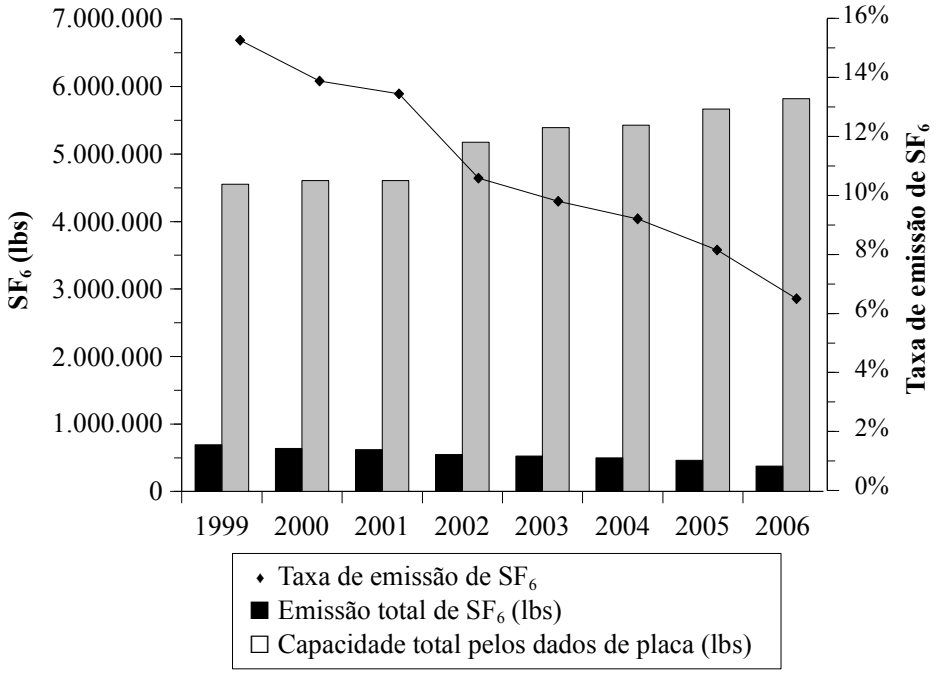


Figura 6.3: Emissão de SF_6 pelos parceiros do programa de redução de emissão de SF_6 no setor elétrico da agência de proteção ambiental norte-americana
Fonte: EPA (2006, p. 2, tradução nossa)

6.1.2 Gerenciamento do projeto MitiSF6

Apesar de não ser uma etapa formal da metodologia, optou-se por destacar algumas considerações sobre a gestão do projeto MitiSF6, a fim de enfatizar alguns pontos destacados na Seção 5.1. 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*[3]) detalhada com o respectivo cronograma; matriz de responsabilidade; alocação de recursos humanos; planejamento de aquisições; etc. A Figura 6.4 ilustra algumas das técnicas e ferramentas utilizadas nesta etapa.

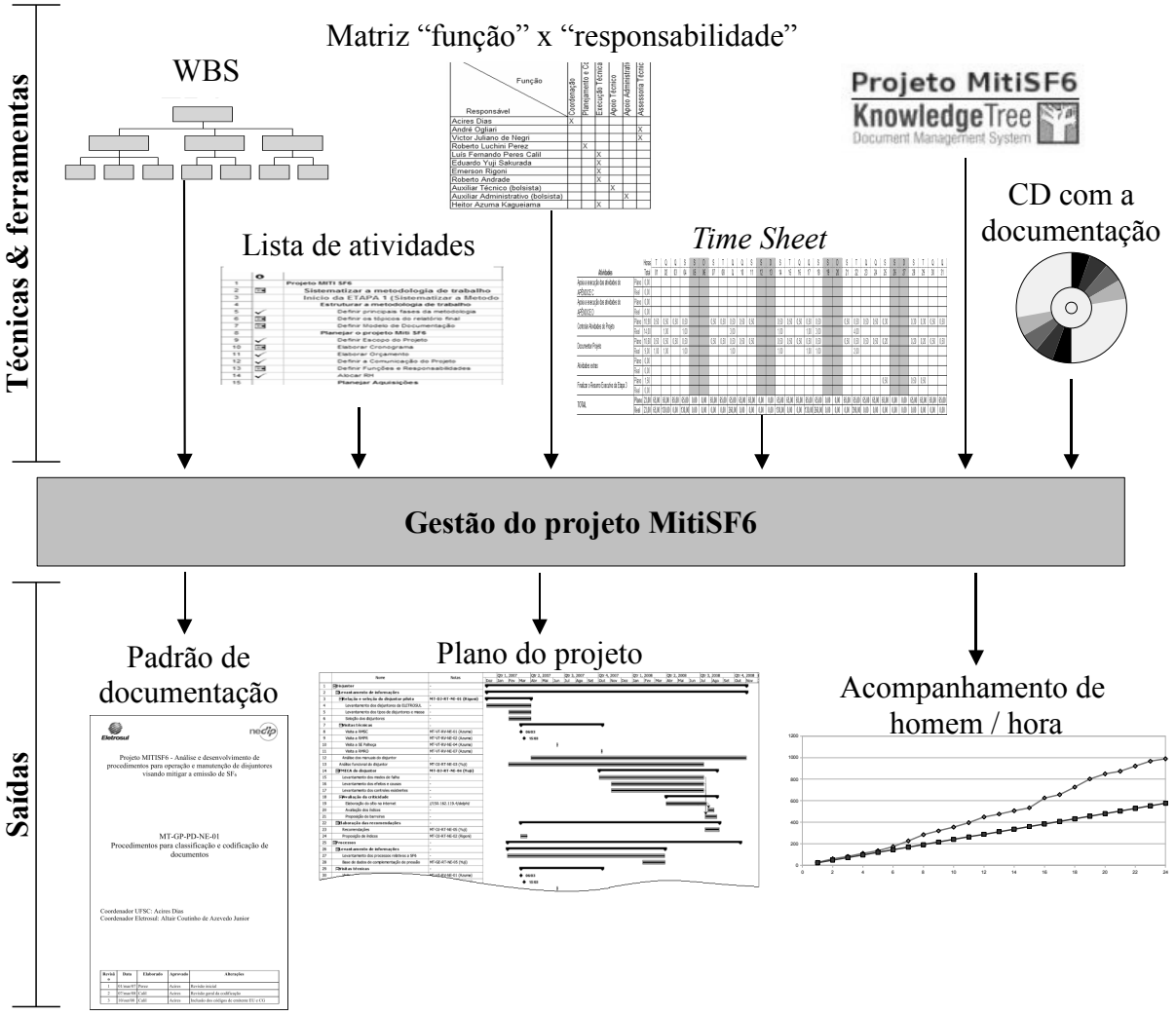


Figura 6.4: Algumas das técnicas e ferramentas utilizadas na gestão do projeto MITISF6
Fonte: UFSC/NeDIP (2008e)

Também foi definido um padrão de numeração dos documentos vinculados ao projeto, fa-

[3]Para detalhes sobre WBS, recomenda-se a leitura no MIL-HDBK-881 (USA/DOD, 1998).

cilitando a gestão e referência deles[4], e, para evidenciar os produtos das tarefas da WBS, foi associado o número do documento resultante daquela ação (quando aplicável).

No intuito de avaliar o tempo que os recursos humanos dedicaram ao projeto, foi implementada uma folha de acompanhamento de homem/hora (*time sheet*). Estes dados possibilitam um melhor controle do uso dos recursos no projeto atual e melhor estimativa para os projetos futuros.

A fim de viabilizar o acompanhamento do projeto pelos colaboradores da Eletrosul, optou-se por elaborar relatórios bimestrais das atividades realizadas. A disseminação do conhecimento gerado ao longo do projeto ocorreu pela documentação gerada e na forma de *workshops*, visitas técnicas e seminários – além dos trabalhos acadêmicos associados ao projeto, como esta tese de doutorado. Adicionalmente, foram disponibilizados, aos participantes da Eletrosul no projeto, os respectivos cadastros no sistema de gerenciamento de documentos utilizado, no caso o KTDMS (Knowledge Tree Document Management System[5]). Para tanto, foi instalado um servido no NeDIP/UFSC com o *software*, possibilitando acessar a documentação remotamente, via internet. É interessante destacar que, na parte final do projeto, a documentação passou a ser entregue à Eletrosul em CD (*compact disc*), juntamente com o relatório bimestral.

Note-se que, na fase final do projeto, verificou-se a importância de se elaborar um livro que compile o conhecimento gerado, nos dois anos de projeto, de tal sorte que o leitor possa ter acesso aos textos necessários e suficientes para o entendimento da teoria envolvida na mitigação das perdas de SF_6, bem como para sua aplicação – tanto pela emissão do gás para a atmosfera quanto pela contaminação do gás, num patamar que acarrete seu descarte. Este fator superveniente levou à extensão do projeto, que contará, ainda, com a adequação do *software* OpenFMECA para as situações do projeto.

Por fim, destaca-se que o projeto, por fazer parte do programa ANEEL, contou com a aprovação da alta gerência da empresa – cujo apoio foi determinante para o seu sucesso.

6.1.3 Etapa de delineamento

A seguir, apresenta-se a aplicação da metodologia no Departamento de Manutenção do Sistema da Eletrosul (DMS), no que se refere às fases do delineamento informacional, conceitual e preliminar.

[4] A documentação do projeto foi gerenciada utilizando o *software* KTDMS.
[5] Disponível em: <http://www.knowledgetree.com/>.

6.1.3.1 Fase do delineamento informacional

O projeto focou exclusivamente nas questões relacionadas ao gás SF_6; assim a análise e a elaboração dos objetivos de risco se restringiram a elas. A Figura 6.5 ilustra algumas técnicas e ferramentas utilizadas nesta fase.

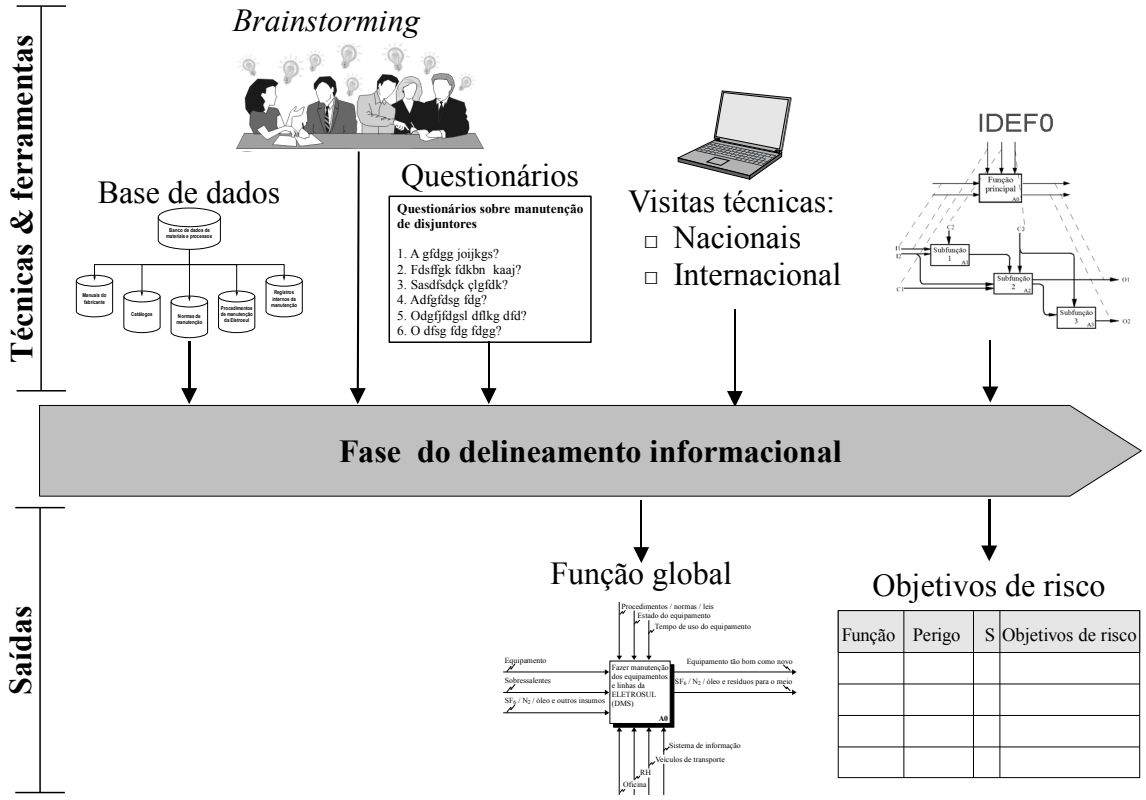


Figura 6.5: Algumas das técnicas e ferramentas utilizadas na fase do delineamento informacional do projeto MITISF6

Para a caracterização do Departamento de Manutenção do Sistema da Eletrosul, optou-se por fazer a definição da função global utilizando a técnica IDEF0, ilustrada na Figura 6.6[6].

A fim de detalhar o 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 (UFSC/NEDIP, 2008f). Destaca-se que, na técnica IDEF0, controles são as restrições da função e mecanismos são os recursos necessários para se executar a função.

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.

[6] A Figura 6.6 e a Figura 6.8 foram obtidas a partir do *software* AI0Win©, desenvolvido pela Knowledge Based Systems, Inc.

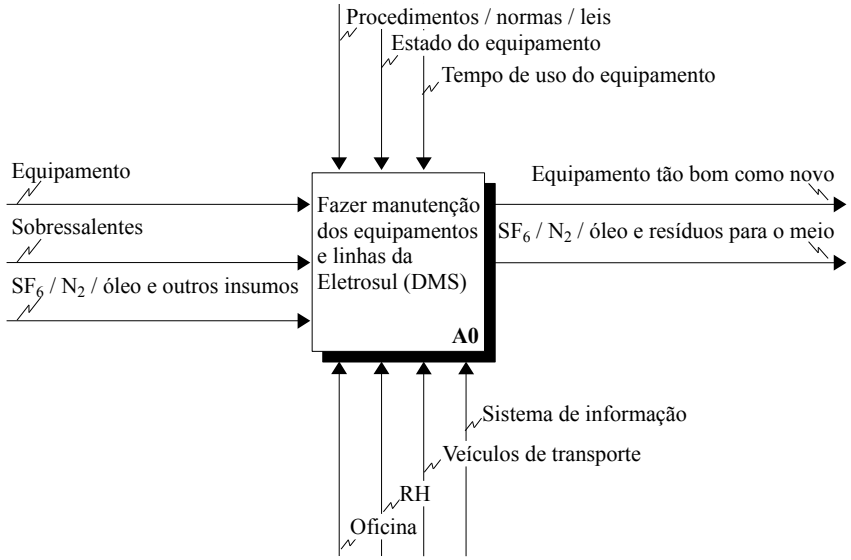


Figura 6.6: Diagrama raiz da IDEF0 dos processos relacionados à manipulação do SF_6
Fonte: MT-PR-RT-NE-01 (UFSC/NEDIP, 2008j, Apêndice A, p. 12)

Destaca-se, ainda, que o número ONU do SF_6 é o 1080, que traz a indicação dos seguintes riscos: explosão do reservatório em caso de aquecimento; queimaduras pelo frio no contacto com o líquido ao vaporizar-se; e asfixia por falta de oxigênio em caso de fuga importante (IGEO/RISE, 2000).

Com base nestas análises, podem-se estipular os objetivos[7] de perda de SF_6 que, posteriormente, balizaram a decisão de aceitar o risco ou não.

6.1.3.2 Fase do delineamento conceitual

A Figura 6.7 ilustra algumas técnicas e ferramentas utilizadas nesta fase.

Uma vez definida a função global no diagrama IDEF0, na análise funcional, fez-se o desdobramento das funções pertinentes ao projeto até a resolução desejada. Observe-se, na Figura 6.8, que as caixas A1 e A2 estão sombreadas, o que indica que estas funções foram desdobradas – pois estão relacionadas ao SF_6.

Para detalhar melhor o modelo, foram incluídas as descrições de cada elemento do diagrama. O Quadro 6.2 ilustra a descrição da função "gerenciar insumos", nódulo A1 do diagrama IDEF0. De forma análoga, foram descritas as outras funções, os controles, os mecanismos, as entradas e as saídas.

[7] Não foi utilizada a técnica FHA; no entanto, entende-se que ela irá contribuir para uma análise mais estruturada, quando esta não for tão específica como a apresentada.

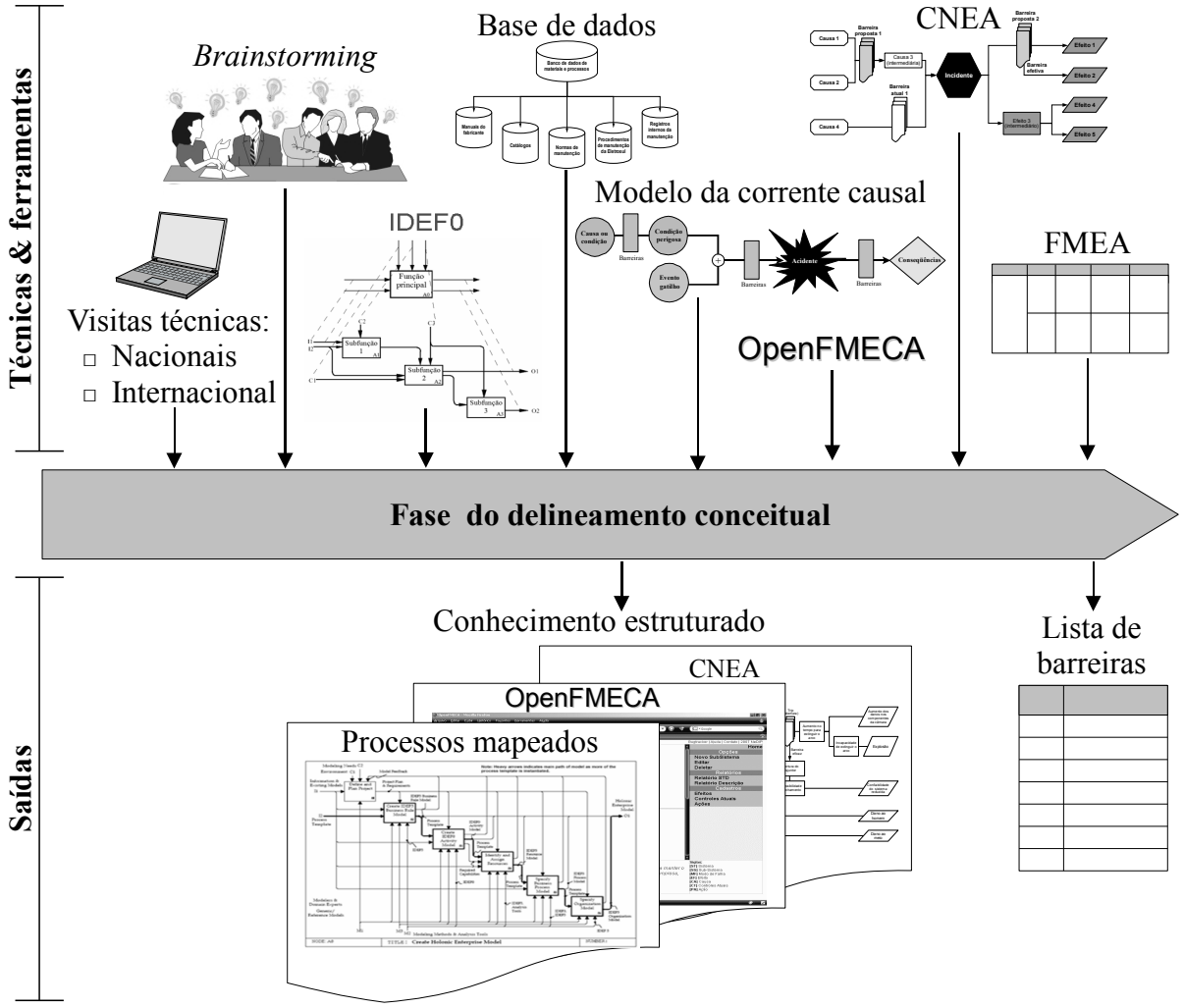


Figura 6.7: Algumas das técnicas e ferramentas utilizadas na fase do delineamento conceitual do projeto MITISF6

Quadro 6.2: Descrição da função "gerenciar insumos" [A1]

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 SF_6 será tratado.

O modelo diagramado pela técnica IDEF0, então, serviu de base para a FMEA dos processos, pois ele evidencia o que é necessário para que as funções sejam adequadamente realizadas.

Primeiramente, foram levantados os possíveis modos de falha para cada função, no último nível de desdobramento do IDEF0, conforme ilustrado na Figura 6.9. Para tanto, foram utilizadas técnicas de criatividade (como *brainstorm* e *brainwriting*) e listas de modos de falhas de

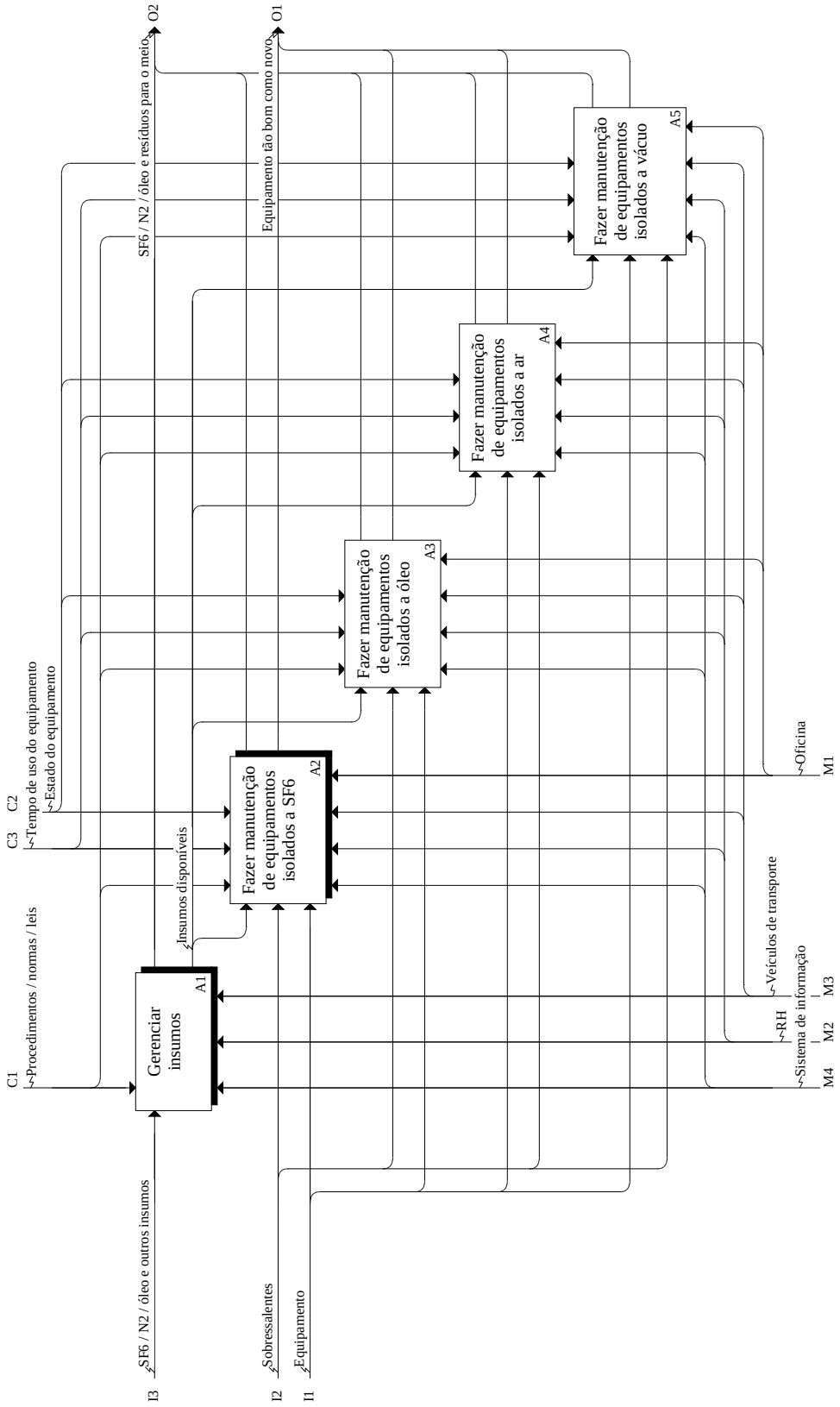


Figura 6.8: Diagrama A0 da IDEF0 dos processos relacionados à manipulação do SF_6
Fonte: MT-PR-RT-NE-01 (UFSC/NEDIP, 2008j, Apêndice A, p. 14)

outras FMEAs, utilizadas como referência.

A análise dos modos de falha foi feita, então, utilizando a estrutura CNEA/FMEA, conforme descrito na Seção 5.3.1.2 e ilustrado na Figura 6.10 e Quadro 6.3.

Para dar suporte à elaboração da FMEA dos processos, foi utilizada a ferramenta computacional OpenFMECA. A Figura 6.9 mostra uma imagem da tela do *software* OpenFMECA, versão *Alpha* 1, que foi a utilizada no projeto. O Apêndice A traz uma descrição mais detalhada do *software*. É interessante destacar que o *software* está sendo restruturado e estará brevemente disponibilizado no sítio SorceForge [8], como versão *Alpha*.

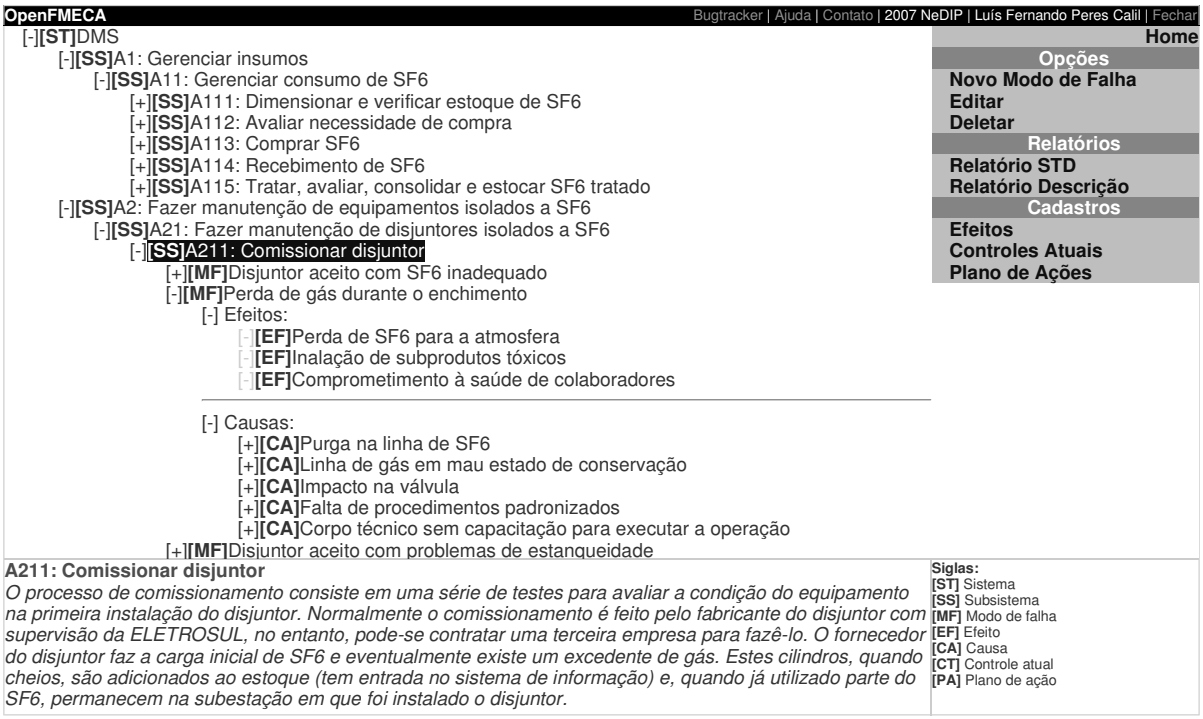


Figura 6.9: Imagem da tela do *software* OpenFMECA, versão Alpha 0.1

Esta ferramenta permite representar, na forma de árvore, a estrutura hierárquica das funções do diagrama IDEF0 e, então, desenvolver uma FMECA para as funções relacionadas ao gás SF_6. O OpenFMECA também permite que se inclua uma descrição mais detalhada de cada elemento da FMECA / CNEA, melhorando a representação do modelo e a gestão do conhecimento.

De fato, a análise foi feita utilizando os diagramas CNEA e, posteriormente, os elementos do diagrama foram passados para o OpenFMECA – que, por sua vez, permite exportar relatórios na forma das tradicionais tabelas FMEA.

O diagrama na Figura 6.10 ilustra uma CNEA, no caso a do segundo modo de falha poten-

[8] <http://sourceforge.net/>

cial identificado para a função "perda de SF_6 durante o enchimento", nódulo A212 do diagrama IDEF0, e o Quadro 6.3 apresenta a tabela FMEA para este diagrama.

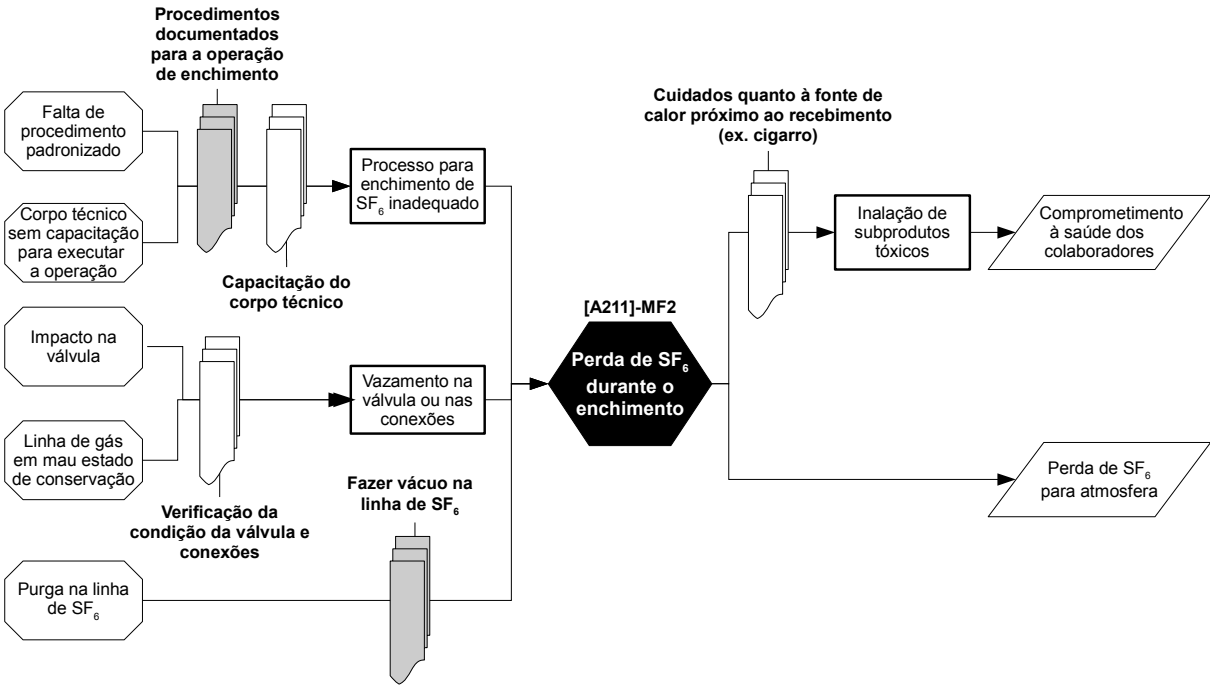


Figura 6.10: CNEA do modo de falha "Perda de SF_6 durante o enchimento", em [A211]
Fonte: adaptado de MT-PR-RT-NE-03 "FMEA dos processos de manipulação de SF_6 na Eletrosul" (UFSC/NEDIP, 2008l, p. 57)

Uma vez modelados os potenciais riscos, podem-se levantar possíveis barreiras, a fim de reduzir o risco ou mitigar suas consequências. Essas barreiras foram diagramadas nas CNEAs e detalhadas no campo das "ações" nas FMEAs – vide Figura 6.10 e Quadro 6.3. Essas barreiras foram, então, analisadas, para verificar se elas não introduziriam novos riscos ou potencializariam existentes, e posteriormente classificadas.

Destaca-se que todas estas análises foram submetidas a especialistas da empresa – em reuniões e visitas técnicas – para serem validadas.

Note-se que se optou por não fazer a análise de criticidade dos cenários. Assim, foram levantadas possíveis barreiras para todas as correntes causais. A seleção de quais barreiras serão implementadas e a priorização delas fica a critério da empresa, que fará esta análise posteriormente. Desta forma, não foi realizada a avaliação custo-risco-benefício para justificar as barreiras.

Também não foi avaliada a possibilidade de contratação de seguro, estratégia já considerada pela empresa.

Quadro 6.3: 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 a 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 a 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 a 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

Fonte: adaptado de MT-PR-RT-NE-03 "FMEA dos processos de manipulação de SF_6 na Eletrosul" (UFSC/NEDIP, 2008l, p. 49 e 50)

6.1.3.3 Fase do delineamento preliminar

No projeto MitiSF6, optou-se por transpor as barreiras identificadas em recomendações. Estas recomendações, por sua vez, subsidiarão o delineamento das ações necessárias para implementação das barreiras e a elaboração dos planos preliminares, conforme ilustrado na Figura 6.11. Em alguns casos, essas recomendações foram detalhadas, como na sugestão de procedimento para controle do uso e solicitação de SF_6 – ilustrada na Figura 6.12 – que pode fazer parte dos planos preliminares, caso a empresa a acate.

De forma geral, as recomendações para a empresa podem ser divididas em três linhas:

- referentes à política de atualização da estrutura de manipulação do gás;
- referentes à política de atualização dos procedimentos; e
- referentes à política de capacitação.

Também foram elencadas algumas recomendações de responsabilidade da ANEEL (Agência Nacional de Energia Elétrica):

- referentes à política regulatória.

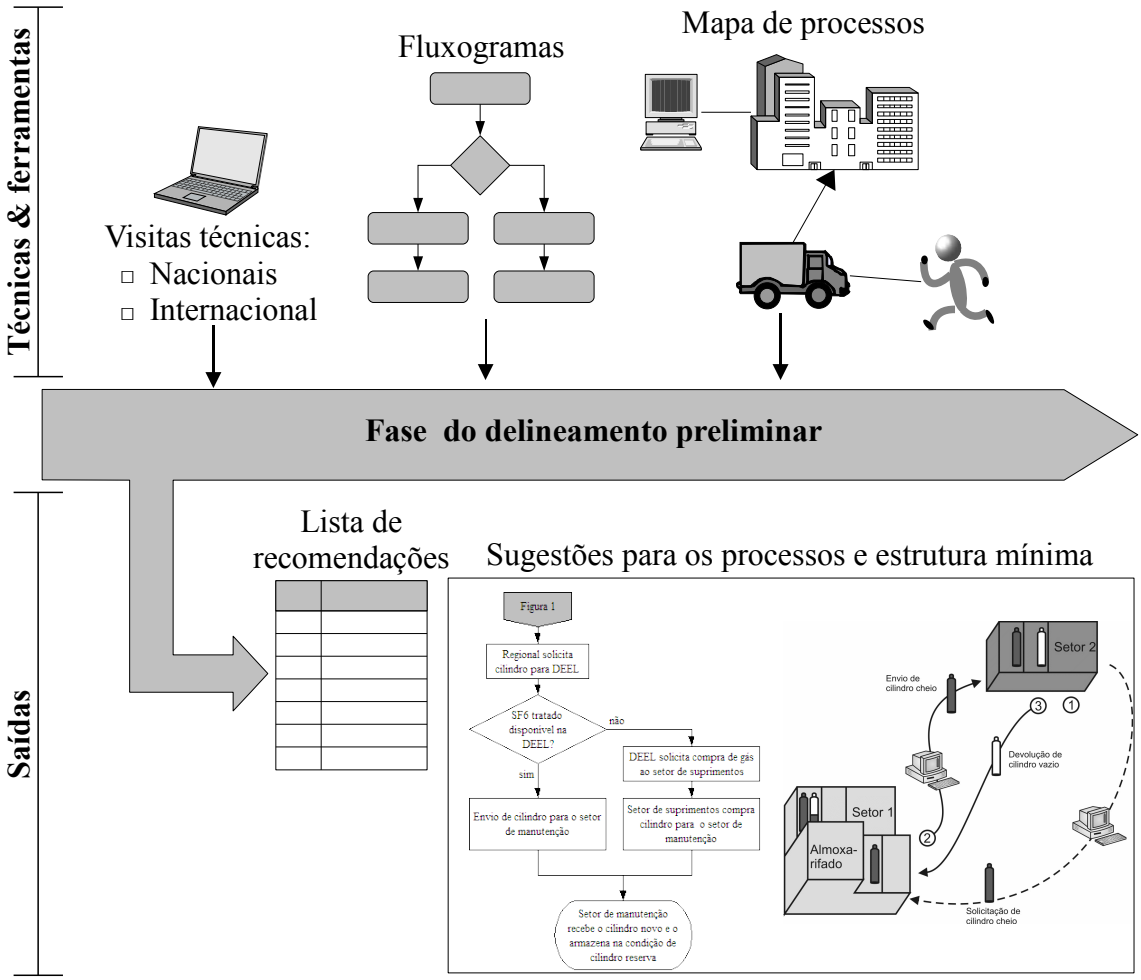


Figura 6.11: Algumas das técnicas e ferramentas utilizadas na fase do delineamento preliminar do projeto MITISF6

No que diz respeito ao plano de ações preliminar, este poderá ser elaborado com base nas recomendações referentes à estrutura mínima sugerida, i.e., equipamentos, instalações, etc., que se considerou necessário para dar suporte aos processos relativos à manipulação do SF_6 – conforme apresentado no documento MT-PR-RT-NE-04 (UFSC/NEDIP, 2008m).

Assim, foi delineada uma estrutura desejável para a regional de manutenção, os setores de manutenção e a central da divisão de manutenção, no sentido de se dispor dos recursos mínimos e suficientes para a adequada gestão do gás, a fim de garantir o tratamento e consolidação de cilindros [9], a detecção de vazamento e de pureza do gás, a disponibilidade de SF_6, a disponibilidade dos dispositivos necessários para executar as operações, etc. Também foram elaboradas recomendações para as especificações técnicas de compra de equipamentos e insumos. Como resultado da implementação destas recomendações, espera-se que a empresa obtenha, além da

[9] Consolidação é o processo em que se completa um cilindro com o gás existente em outros.

redução da perda de SF_6, uma melhor gestão dos recursos existentes – como a redução do número de cilindros de armazenagem do gás, redução de gastos com transporte de equipamentos e insumos, etc.

As recomendações referentes aos planos de aceitação e comunicação estão apresentadas principalmente no documento MT-PR-RT-NE-05 (UFSC/NEDIP, 2008n). Este documento apresenta as recomendações quanto à forma de executar os processos relativos à manipulação do SF_6. Assim, nele foram consideradas desde as alterações referentes à operação normal (pertinentes ao plano de monitoramento & controle) até as recomendações para o caso de um incidente (no caso: os modos de falha trabalhados na estrutura FMECA / CNEA).

É importante ressaltar que a perda de SF_6 é, muitas vezes, intrínseca do processo. Por exemplo: para se fazer a desmontagem do disjuntor, é feita, primeiramente, a retirada do gás; no entanto, existe uma pressão residual que inevitavelmente será emitida.

O documento, então, traz recomendações para segurança; para tratar, avaliar, consolidar e estocar SF_6 tratado; para retirada e transporte dos disjuntores; para manutenção dos disjuntores; para instalação dos disjuntores; para enchimento e complementação de pressão dos disjuntores; para avaliação da condição em campo dos disjuntores; e para controle do uso e solicitação de SF_6, tais como:

- controle do uso dos cilindros de SF_6;
- manutenção dos equipamentos de manipulação de SF_6;
- solicitação de SF_6 pelo setor de manutenção;
- solicitação de SF_6 pela regional de manutenção;
- avaliação da necessidade de compra de SF_6;
- aquisição de SF_6 de fornecedor;
- solicitação e envio de SF_6 tratado;
- recebimento de SF_6 no almoxarifado da regional ou nos setores de manutenção;
- estocagem dos cilindros de SF_6; e
- utilização dos cilindros da reserva de contingência.

Note-se que as análises contemplaram não apenas as falhas referentes à perda de SF_6 para a atmosfera, mas também as questões relacionadas à operação da empresa e à saúde dos colaboradores. Por exemplo, a Figura 6.9 apresenta modos de falha, como “estoque mínimo mal dimensionado” – o que influenciará na disponibilidade de SF_6 e, por consequência, poderá atrasar a manutenção de disjuntores.

É interessante destacar que os planos preliminares não foram elaborados, mas as recomendações muitas vezes traziam uma sugestão de como se deveria operar, que é escopo dos planos de aceitação preliminar – a Figura 6.12 ilustra um fluxograma do processo de solicitação de SF_6.

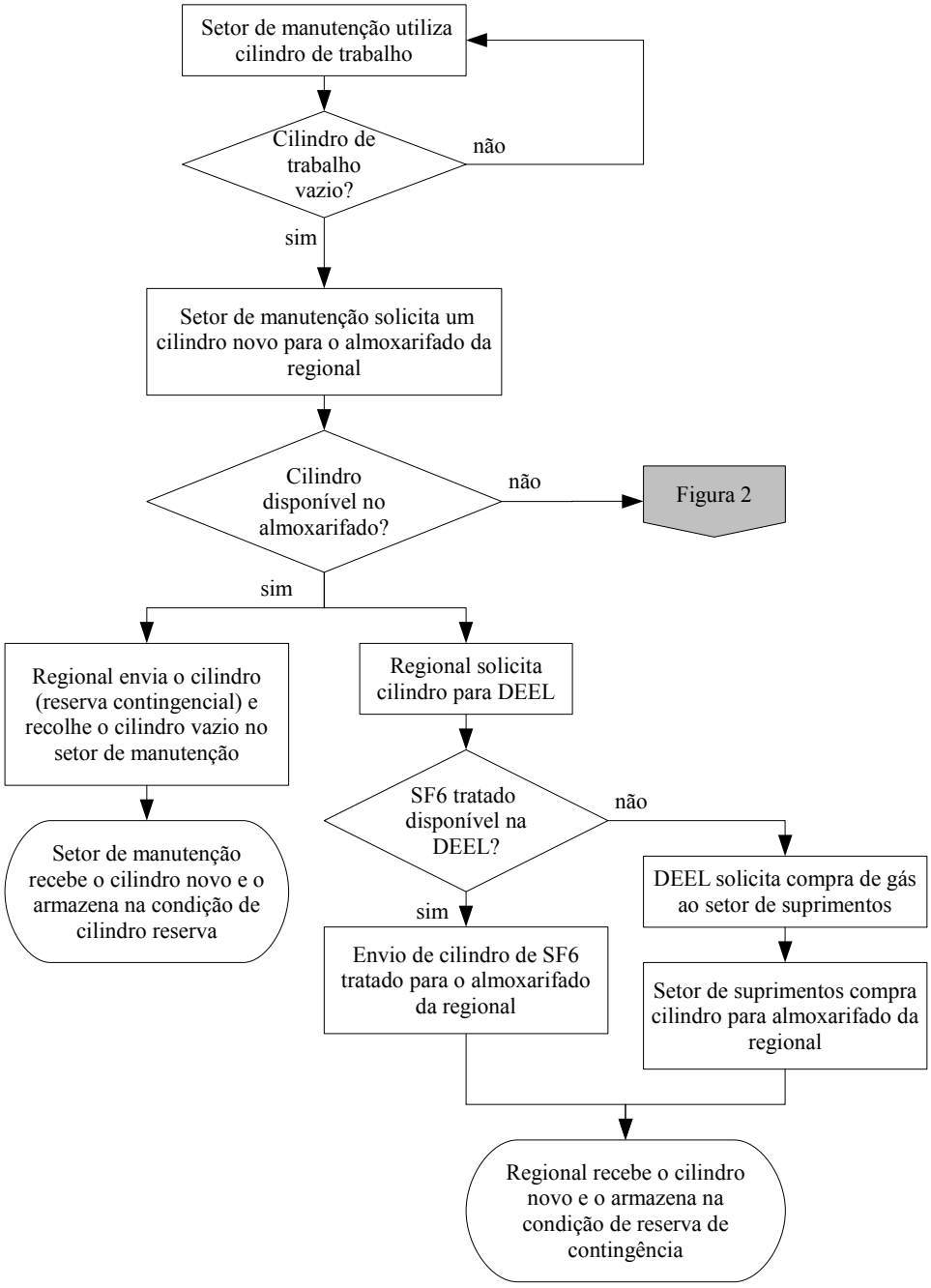


Figura 6.12: Fluxograma para controle do uso e solicitação de SF_6 – parte 1
Fonte: MT-PR-RT-NE-05 "Recomendações para os processos relativos à manipulação do SF_6" (UFSC/NEDIP, 2008n, p. 4)

De fato, houve um procedimento que chegou a ser detalhado: o procedimento de operação

de uma máquina de tratamento de SF_6 – documento MT-PR-RT-NE-02 (UFSC/NEDIP, 2008k) –, o que seria feito apenas na fase do delineamento detalhado.

Quanto ao monitoramento & controle, também foi feito um estudo para propor índices que possibilitassem avaliar a quantidade de SF_6 consumida pela empresa e identificar as áreas com maior potencial para redução – vide documento MT-GE-RT-NE-04 (UFSC/NEDIP, 2008g).

Adicionalmente, foram feitas recomendações para alterar a base de dados de manutenção dos disjuntores, apresentadas no documento MT-GE-RT-NE-05 (UFSC/NEDIP, 2008h). Estas alterações possibilitarão cruzar as informações obtidas na base de dados com as obtidas no acompanhamento do uso do gás – além de fornecer, para o setor de manutenção, informações mais direcionadas às questões do gás.

Por exemplo, pode-se obter da base de dados a massa de gás introduzida em um disjuntor (em função do modelo, da pressão antes e depois do enchimento e da temperatura ambiente). Das fichas de acompanhamento do uso do gás, ilustrada na Figura 6.13, pode-se obter a massa de gás utilizada nesta operação e, com isso, avaliar a eficiência do processo – quanto ao consumo de SF_6.

SF6 novo ou tratado

Data do próximo teste hidrostático: Out/2012
Número de série do cilindro: 053678 **Tara:** 66,1kg

SF_6

Qualidade do SF6
☒ Novo ☐ Tratado

Data	Massa restante	Responsável	Equipamentos relacionados	Operação que consumiu SF6
05/03/08	50,0kg	Fornecedor	-	☐ Complementação em operação ☐ Complementação após manutenção ☒ Outro: Aquisição do cilindro
10/05/08	46,8kg	Colaborador X	DJ0000000	☐ Complementação em operação ☒ Complementação após manutenção ☐ Outro:
				☐ Complementação em operação ☐ Complementação após manutenção ☐ Outro:
				☐ Complementação em operação ☐ Complementação após manutenção ☐ Outro:
				☐ Complementação em operação ☐ Complementação após manutenção ☐ Outro:
				☐ Complementação em operação ☐ Complementação após manutenção ☐ Outro:

Figura 6.13: Sugestão de etiqueta de identificação dos cilindros de SF_6
Fonte: adaptado de UFSC/NeDIP (2008n, p. 7)

No que se refere à capacitação do corpo técnico, foi evidenciado que ela é uma das respon-

sáveis pelo sucesso de um programa de mitigação de perda de SF_6. Assim, a todo procedimento novo – ou alteração nos já existentes – destacou-se a recapacitação dos colaboradores envolvidos.

Por fim, foram feitas algumas recomendações referentes à política regulatória, para que o Brasil – a exemplo da Europa – controle o uso do gás SF_6.

A curto prazo, foram destacadas as seguintes recomendações:

- solicitar aos fornecedores de SF_6, que reportem anualmente a quantidade de SF_6 a ser adquirida e a quantidade 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; e
- solicitar que as empresas do setor elétrico avaliem a quantidade de SF_6 contida em seus equipamentos.
- solicitar que a ANEEL estabeleça uma medida de emissão de gás para o Brasil, para servir como padrão para as empresas do setor elétrico;
- solicitar que a ANEEL sugira à Secretaria de Meio ambiente que seja feito um acompanhamento do consumo de SF_6, semelhante ao que é feito no setor elétrico, para se dispor de uma medida de consumo de SF_6 para o país.

6.2 Aplicação na Eletrosul, no âmbito do sistema técnico

A aplicação no nível do sistema técnico, na Eletrosul, aconteceu em paralelo à da unidade organizacional e seguiu a gestão do projeto MitiSF6 apresentada na Seção 6.1.2.

Da mesa forma que na aplicação no DMS, a aplicação no sistema técnico também contemplou as fases do delineamento informacional, conceitual e o início do preliminar – ilustrado na Figura 6.14.

6.2.1 Contextualização do problema

Existem inúmeros equipamentos de transmissão e distribuição de energia elétrica que utilizam SF_6 como dielétricos. No caso da Eletrosul, seu parque inclui disjuntores de tanque vivo e uma subestação blindada (GIS – *gas insulated substation*). No entanto, estes equipamentos não são totalmente estanques e, ao longo de sua operação, perdem gás para a atmosfera.

Normalmente esta perda é muito pequena e não afeta o desempenho do equipamento, mas,

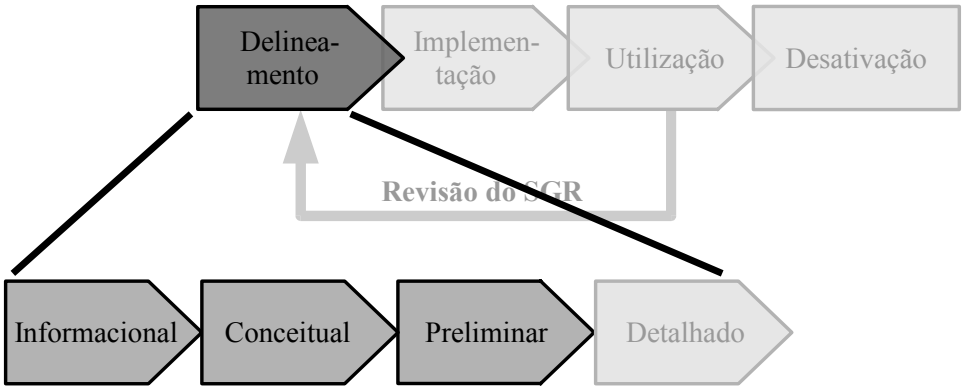


Figura 6.14: Fases da metodologia abordadas na aplicação no nível do sistema técnico, na Eletrosul

em alguns casos, esta redução de pressão pode alcançar valores significativos – as causas para isto foram exploradas no projeto MitiSF6. A fabricante de disjuntor ABB, por exemplo, considera que a perda de SF_6, em seus novos disjuntores de tanque vivo, não supera a marca de 0,5% da massa de gás por ano (ABB, 2008).

Para evitar que o disjuntor fique disponível para operação com baixa pressão de SF_6, existem dois níveis de alarme: um de advertência e outro que abre o disjuntor em "*trip*".

O disjuntor Merlin Gerin, modelo FA4, por exemplo, trabalha com 6,0bar de pressão nominal (na temperatura de referência de 20°C) e tem alarme de advertência com 5,2bar e de *trip* com 5,0bar, sendo que a expectativa é que se perca anualmente menos de 1% da massa de SF_6 (ELETROSUL, 2006).

Além da perda de SF_6, também existe o problema da entrada de contaminantes. 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 (RODRIGUES FILHO; BARZ, 2005). 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 não apenas na operação do equipamento, mas também quando este sofrer manutenção. Isto pode ocorrer não apenas pela introdução de ar e umidade durante o enchimento de SF_6, mas também pela exposição dos componentes do equipamento à atmosfera – por adsorção, por exemplo.

Por fim, destaca-se que o SF_6 é um gás atóxico, no entanto, durante a operação do disjuntor, podem ser gerados subprodutos tóxicos – na forma de pó. Assim, a redução da contaminação

do gás irá reduzir a produção destes subprodutos e, por consequência, reduzir a chance de dano à saúde dos colaboradores em contato com o equipamento (e ao meio ambiente).

6.2.2 Etapa de delineamento

A seguir, apresenta-se a aplicação das fases do delineamento informacional, conceitual e preliminar no âmbito do sistema técnico, no caso um disjuntor.

6.2.2.1 Fase do delineamento informacional

Os sistemas técnicos de interesse neste projeto são os que utilizam SF_6 como dielétrico. Assim, foi feita a caracterização das instalações da empresa, buscando identificar estes equipamentos – o relatório deste estudo está apresentado no documento MT-DJ-RT-NE-01 (UFSC/NEDIP, 2008b).

Destes sistemas, optou-se por estudar, primeiramente, os disjuntores e – como caso piloto – optou-se pelo disjuntor Merlin Gerin FA4. Os seguintes critérios foram utilizados para a seleção do modelo de disjuntor para estudo piloto (UFSC/NEDIP, 2008b):

1. Modelo e/ou fabricante com a maior massa de SF_6 e cujo disjuntor está em operação.
2. Modelo e/ou fabricante no nível de tensão de maior concentração de disjuntores.
3. Modelo e/ou fabricante mais antigo no sistema da Eletrosul.
4. Modelo e/ou fabricante com menor Índice de Eficiência de Extinção com relação à tensão de isolação e massa de SF_6 necessária (IEEMassa)[10].
5. 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).
6. Modelo e/ou fabricante com estudo consolidado na literatura nacional e/ou internacional.
7. Modelo e/ou fabricante utilizado em outras concessionárias.
8. Modelo e/ou fabricante com maior potência manobrada pelo disjuntor.
9. Modelo e/ou fabricante com posição operacional estratégica dentro do sistema Eletrosul.
10. Modelo e/ou fabricante com maior dificuldade de manutenção em função de sua localização em campo.
11. Modelo e/ou fabricante que tenha manutenção programada dentro do tempo do projeto.

[10] IEEMassa e IEEDensidade são índices elaborados ao longo do projeto MitiSF6 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.

É interessante destacar que o projeto MitiSF6 não tinha como objetivo fazer alterações de projeto nos equipamentos, mas estudar os possíveis cenários associados à perda de SF_6 para a atmosfera.

Assim, foi definida como função do disjuntor "conter SF_6". Neste caso, as restrições são as normas e regulamentos no que se refere à perda de gás nos equipamentos. Os recursos críticos, por sua vez, estão relacionados a integridade dos invólucros e das vedações. Com base nestes pontos, fez-se a análise funcional de produto e puderam-se estipular os objetivos de perda de SF_6 na operação do equipamento.

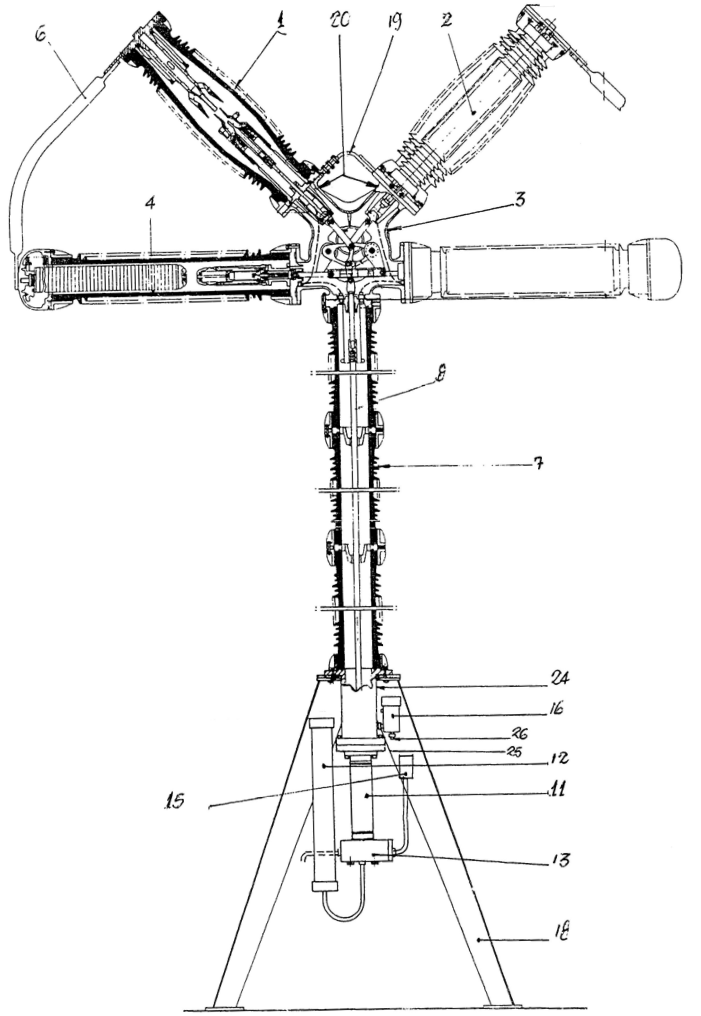
6.2.2.2 Fase do delineamento conceitual

Foi feita, então, a análise funcional do disjuntor Merlin Gerin FA4, ilustrado na Figura 6.15, que está apresentada no documento MT-DJ-RT-NE-03 (UFSC/NEDIP, 2008c).

Figura 6.15: Fotografia de disjuntores Merlin Gerin FA4 (550kV)
Fonte: UFSC/NeDIP (2008c, p. 3)

A Figura 6.16 é um desenho esquemático de um módulo do disjuntor. Cada uma das 3 fases é composta por 2 módulos, portanto, totalizando 6 módulos por disjuntor, como pode ser observado na Figura 6.15.

Observe-se que a câmara de extinção, o cárter, o resistor de pré-inserção e coluna de isoladores de porcelana – itens 1, 3, 4 e 7, respectivamente – são preenchidos com SF_6. No caso



Legenda:

1 – Câmara de extinção
2 – Capacitor equalizador de potencial
3 – Cárter
4 – Resistor de pré-inserção
6 – Conexão elétrica (Câmara-resistor)
7 – Coluna suporte (isoladores de porcelana)
8 – Haste isolante
11 – Cilindro hidráulico principal
12 – Acumulador de energia
13 – Relé hidráulico
15 – Tanque de expansão (baixa pressão)
16 – Manostato de gás
18 – Chassis galvanizado (estrutura)
19 – Conexão elétrica entre câmaras
20 – Plugue do dreno do cárter
24 – Caixa de molas
25 – Parafusos e porcas do acoplador do manostato
26 – Tampão do manostato

Figura 6.16: Módulo de um disjuntor FA4
Fonte: UFSC/NeDIP (2008c, p. 6)

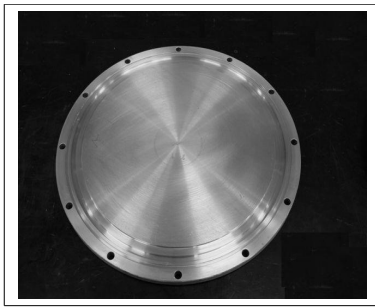
do disjuntor Merlin Gerin FA4, estes subsistemas estão interligados – exceto o cárter, que fica isolado.

Após o desdobramento do disjuntor em subsistemas, foi feita uma análise em cada um dos componentes constituintes de cada subsistema, ilustrada no Quadro 6.4 (UFSC/NEDIP, 2008c).

Também foram identificadas 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.

A análise funcional, então, serviu de base para a FMEA do disjuntor, que teve como modo de falha estudado "não conter SF_6".

Quadro 6.4: Análise funcional da placa de fechamento



ITEM 5 – Placas de fechamento

Função:
- Vedar o SF_6.
- Impedir a entrada de umidade.
- Alojar os anéis de vedação (*O-rings*)

Fonte: UFSC/NeDIP (2008c, p. 16)

Assim como na FMEA dos processos, a análise dos modos de falha foi feita utilizando a estrutura CNEA/FMEA, apresentada no documento MT-DJ-RT-NE-04 (UFSC/NEDIP, 2008a), e também foi utilizado a ferramenta computacional OpenFMECA.

Também foram feitas análises por árvore de falha (FTA) de algumas causas, que se mostraram mais relevantes. A Figura 6.17 ilustra uma das FTAs elaboradas, no caso, para a causa "Anel de vedação com deformação permanente".

Uma vez modelados os potenciais cenários, puderam-se levantar possíveis barreiras, a fim de reduzir o risco ou mitigar suas consequências. Essas barreiras foram diagramadas nas CNEAs e detalhadas no campo das "ações" nas FMEAs.

Note-se que, da mesma forma que se procedeu nas FMEAs dos processos, todas as análises eram submetidas a especialistas da empresa para serem validadas.

Na análise dos disjuntores, também se optou por não fazer a análise de criticidade dos cenários, e foram identificadas as possíveis barreiras para todas as correntes causais – para, posteriormente, a empresa decidir sobre quais devem ser implementadas (fazendo uma avaliação custo-risco-benefício) e qual a prioridade de cada uma delas.

6.2.2.3 Fase do delineamento preliminar

Assim como na unidade organizacional, optou-se por transpor as possíveis barreiras identificadas na FMEA/CNEA/FTA do disjuntor em recomendações e deixar a decisão de sua implementação e priorização para uma análise posterior, a ser realizada pela Eletrosul.

As recomendações referentes ao disjuntor estão apresentadas no documento MT-DJ-RT-NE-05 (UFSC/NEDIP, 2008d). Elas abordam basicamente as questões relacionadas à manutenção e à compra de novos disjuntores. Questões construtivas, que seriam tratadas em um reprojeto do equipamento, ficaram fora do escopo do projeto MitiSF6. No entanto, nas recomendações

para aquisição de novos equipamentos, foram consideradas características construtivas, como o tipo de conexão da linha de SF_6. Também foi enfatizada a importância de se ter um ponto de enchimento do gás ao alcance do operador (sem a necessidade de subir até o painel). Em alguns modelos de disjuntor, o ponto de enchimento fica elevado, diminuindo a distância do operador para a linha viva, quando do enchimento – portanto, aumentando a periculosidade da operação. A Eletrosul já vinha fazendo esta modificação de projeto, e a análise de risco destacou a relevância desta ação.

Quanto à manutenção, destacaram-se, principalmente, as questões relacionadas às vedações e a política de manutenção dos equipamentos.

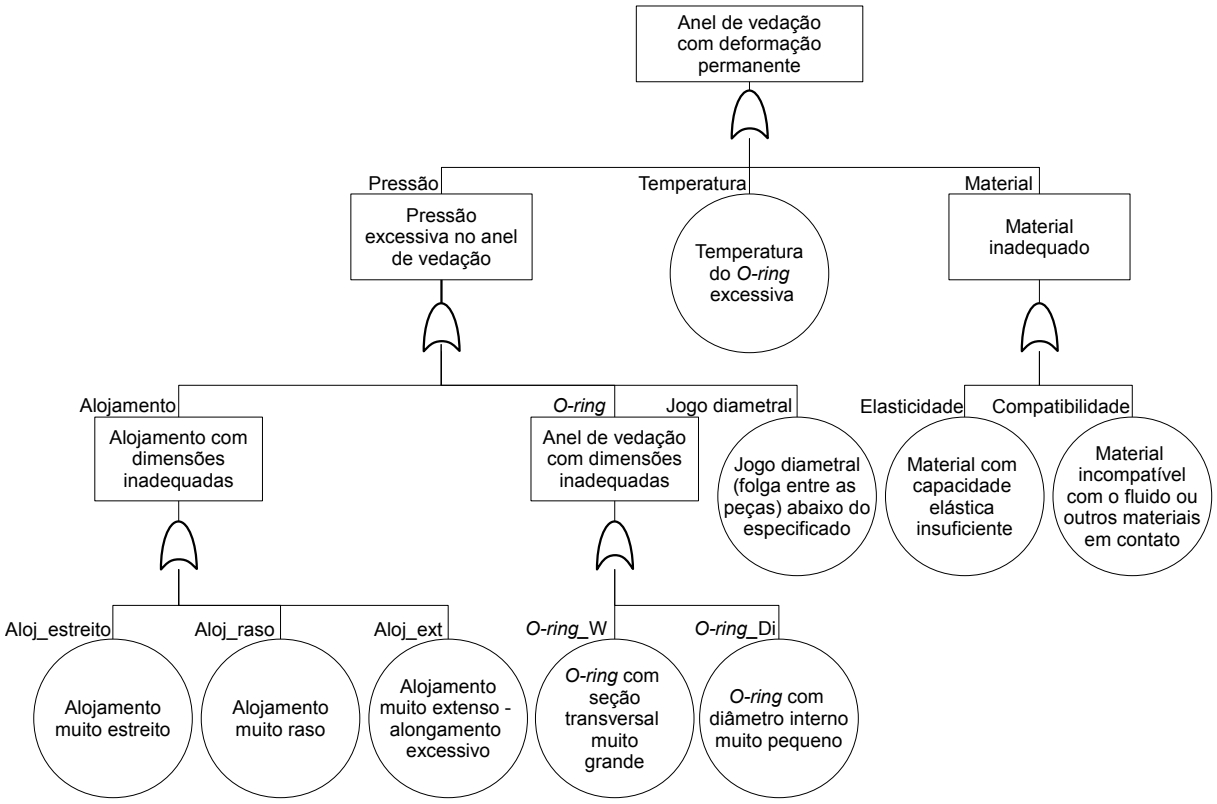


Figura 6.17: Diagrama FTA da falha "Anel de vedação com deformação permanente"
Fonte: UFSC/NeDIP (2008a)

Os disjuntores são equipamentos estáticos, o que contribui para se ter vedação por um longo período. Desta forma, a utilização de O-*rings* adequados pode estender o período entre manutenção.

A redução das atividades de manutenção periódica, por sua vez, diminuirá a possibilidade de contaminação do gás e, por consequência, reduzirá sua emissão para a atmosfera. No entanto, é necessário monitorar a condição do equipamento para garantir que ele se mantém em condição

de operação, i.e., disponível.

É interessante destacar que muitas das recomendações identificadas na análise do sistema técnico interferem nos processos de manipulação do SF_6. De forma análoga, as recomendações para a unidade organizacional também podem interferir na operação do disjuntor.

6.3 Aplicação na Celesc, no âmbito da unidade organizacional

A aplicação na Celesc ocorreu em 2005, quando a metodologia ainda estava sendo elaborada. Assim, ela se deu no formato de uma pesquisa-ação[11], na qual se delineiam hipóteses – previamente selecionadas – como possíveis soluções do problema de pesquisa e, com a aplicação, pode-se analisar as informações no sentido de aceitar ou rejeitar a hipótese (RICHARDSON; PERES, 1989).

A estrutura da pesquisa seguiu a norma ABNT ISO/IEC Guia 73, que inclui, na gestão de risco, a análise / avaliação, tratamento, aceitação e comunicação – conforme apresentado em Dias et al. (2006) –, e um resultado desta pesquisa foi a orientação da estrutura da metodologia apresentada nesta tese.

Nesta seção, apresenta-se esta aplicação estruturada, conforme o disposto no Capítulo 5, que traz a metodologia desenvolvida.

É interessante destacar que a aplicação da metodologia foi feita até a etapa de implementação. No entanto, a equipe da UFSC participou até o detalhamento dos planos, sendo a implementação realizada pela equipe da empresa. Desta forma, a implementação será omitida desta seção, e – em contrapartida – serão exploradas as fases do delineamento preliminar e detalhado, conforme Figura 6.18, que não foram abordadas na aplicação no DMS da Eletrosul.

6.3.1 Contextualização do problema

A Celesc (Centrais Elétricas de Santa Catarina S.A.) é a empresa distribuidora de energia elétrica no estado de Santa Catarina. Ela está estruturada em 16 agências regionais dispostas no estado, sendo que cada uma dessas regionais conta com um COD (centros de operação de distribuição de serviços), equipes de emergência e equipes de manutenção pesada – além de equipes comerciais, de apoio, dentre outras.

[11] Para um melhor entendimento da teoria de pesquisa-ação, recomenda-se a leitura de (THIOLLENT, 1996).

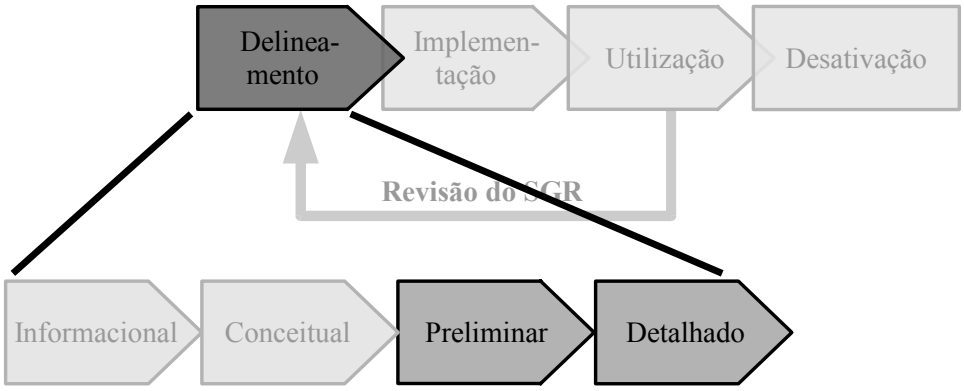


Figura 6.18: Fases da metodologia abordadas na aplicação na Celesc

Os CODs são responsáveis pela coordenação das equipes de manutenção de emergência, fazendo o direcionamento das ações das equipes e orientando as ações de manutenção para restabelecer o fornecimento de energia elétrica – com base, principalmente, nas informações provenientes do sistema de supervisão e controle (SDSC) e do *call center*.

O *call center* é centralizado e está instalado em Florianópolis. Ele é responsável por atender às chamadas comerciais e emergenciais de todo o estado, sendo que as emergenciais têm prioridade de atendimento.

Durante a operação normal, o COD tem um número de interrupções baixo e, por consequência, de ações de manutenção na rede. No entanto, na ocorrência de uma tempestade severa (como tempestades de verão, ciclones extratropicais, furacões, etc.) a demanda aumenta muito, o que dificulta a operação dos centros. Isto se deve não apenas por ter ocorrido um número maior de interrupções, mas também pelo fato de muitas dessas reclamações serem resultado de um mesmo incidente (a perda de um alimentador, por exemplo), o que dificulta o gerenciamento das ocorrências. Nestas condições de trabalho, a segurança pode ser comprometida pela demanda excessiva de trabalho e, eventualmente, pela falha de algum sistema técnico – como o de comunicação entre o despachante e as equipes de manutenção, por exemplo.

Na ocorrência do furacão Catarina – quando 20 municípios decretaram estado de emergência ou calamidade, sendo 9 na área de concessão da Celesc – ficou evidenciada a necessidade de se montar uma estrutura diferenciada para operar nessas condições (DIAS et al., 2006).

É interessante destacar que a resolução ANEEL N° 024, art. 22, I, considera que as "[...] interrupções associadas à situação de emergência ou de calamidade pública decretada por órgão competente serão desconsideradas para efeito de compensação [...]" (ANEEL, 1994, p. 18), portanto isentas de penalidades no que se refere à violação das metas estabelecidas pela agência.

No entanto, eventos desta proporção podem acarretar interrupções muito prolongadas, o que pode ser danoso para a sociedade. Assim, a fim de minimizar o período de restabelecimento do sistema, optou-se por priorizar os estudos referentes às interrupções resultantes das ações de tempestades severas nos CODs – apresentados nesta seção –, para, no futuro, implementar um sistema de gestão de risco mais amplo, considerando outros incidentes.

Assim, este projeto focou na elaboração dos planos de aceitação para atuar na ocorrência de uma tempestade severa, no âmbito do COD – apesar de muitas medidas adotadas terem extrapolado para outras unidades organizacionais.

Para tanto, foi instituído um grupo de trabalho formado por colaboradores da Celesc e pesquisadores do NeDIP/EMC/UFSC. É interessante destacar que este grupo foi definido em uma resolução interna e, portanto, tinha o apoio da alta gerência.

Este grupo foi responsável pelo planejamento e delineamento do programa, sendo que a implementação foi realizada sem a colaboração da equipe do NeDIP.

6.3.2 Etapa de delineamento

No que se refere ao delineamento, destaca-se – neste projeto – o delineamento detalhado dos planos. As fases do delineamento informacional, conceitual e preliminar foram executadas na perspectiva de identificar medidas que permitissem ao COD operar com mais eficiência e robustez.

Na ótica da Celesc (organização), o incidente analisado é a interrupção no fornecimento de energia elétrica ocasionado pela ocorrência de uma tempestade severa (evento gatilho), no qual a ação do COD é uma barreira para mitigar as consequências – neste caso, o período sem energia. Note-se que a possibilidade de ocorrer uma interrupção é potencializada pela incidência da tempestade severa, mas é uma característica da operação de distribuição de energia. Assim, apesar de ser possível tratar este risco, ele é inerente ao negócio.

Para o COD (unidade organizacional), por sua vez, a continuidade operacional se refere à manutenção de suas funções críticas – como a comunicação com as equipes de manutenção, a identificação de problemas na rede, etc.

Assim, a continuidade operacional do COD, considerando os requisitos de segurança, contribui para a continuidade do negócio da Celesc, neste caso atuando na mitigação dos efeitos decorrentes de uma interrupção, restabelecendo o fornecimento de energia no menor tempo possível.

Neste projeto, o foco foi na segurança e na continuidade operacional dos CODs; no entanto, ao longo das análises, evidenciaram-se algumas ações para reduzir o risco de interrupção no fornecimento de energia. Por exemplo, destacou-se a necessidade de uma restruturação no "programa de execução de podas" existente na empresa – que já tinha identificado que a presença de vegetação junto à rede de distribuição era uma causa de interrupção passível de ser controlada.

6.3.2.1 Fases do delineamento informacional e conceitual

Conforme já mencionado, a apresentação deste estudo de caso concentra-se nas fases do delineamento preliminar e detalhado. No entanto, alguns pontos das fases informacional e conceitual serão destacados.

No que se refere à análise funcional, esta foi feita, primeiramente, utilizando mapas de processo, que são mais intuitivos e possibilitam uma interação com os especialistas e, posteriormente, estes processos foram detalhados utilizando a técnica IDEF0, conforme ilustrado no Quadro 6.5.

Quadro 6.5: Estrutura dos IDEF0 feitos para o *call center* e o COD

Call Center
A0: *Call Center* – Atender usuário
- A1: Gerenciar Chamada
  - A11: Receber chamada
  - A12: Identificar chamadas via URA (unidade de resposta audível)
  - A13: Verificar se o telefone é cadastrado
  - A14: Passar informações eletronicamente
  - A15: Encaminhar chamada
- A2: Identificar cunho da chamada
- A3: Atender chamada comercial
- A4: Atender chamada de emergência
  - A41: Passar informações para usuário
  - A42: Preencher ou complementar NR
  - A43: Passar número do protocolo
  - A44: Encaminhar solicitação para o COD

COD
A0: Despachar serviço para atender NR
- A1: Priorizar NR
- A2: Despachar atendimento
- A3: Localizar ocorrência
- A4: Avaliar ocorrência
- A5: Executar ocorrência
- A6: Executar serviço

Destaca-se, ainda, que devido à grande interação do COD com o *call center*, também foi feito o mapeamento funcional desta unidade organizacional (vide Quadro 6.5).

Quanto à análise dos riscos, foi utilizada, principalmente, a técnica de diagramação causa e efeito – no caso diagrama Ishikawa. Assim, foram levantados os possíveis riscos que poderiam afetar um "despacho eficiente".

Com base nesta análise, foi possível levantar as possíveis barreiras para garantir a continuidade operacional do COD e a segurança do meio em que está inserida, de seus colaboradores (e outras pessoas afetadas pela sua operação) e dos sistemas técnicos que possam ser afetados.

Em relação à avaliação das barreiras, optou-se por adotar todas as identificadas e, então, planejar as implementações delas de acordo com a possibilidade do orçamento da diretoria. É interessante destacar que o projeto se concentrou nas questões relacionadas com a continuidade operacional do COD diante de uma tempestade severa – já que, no futuro, prevê-se a aplicação do sistema de gerenciamento de risco mais amplo.

6.3.2.2 Fases do delineamento preliminar

Na fase preliminar é que se viabiliza a implementação das barreiras – o que requer um razoável esforço dos participantes. Por exemplo, a comunicação com o despachante é fundamental para garantir a segurança das equipes de manutenção, além de possibilitar uma ação mais rápida e efetiva. Uma barreira para o risco de perda de comunicação, no caso de o sistema via rádio falhar, pode ser o uso de telefone celular. No entanto, como viabilizar esta comunicação por celular? A empresa deve ter celulares para serem utilizados nesta condição ou serão usados os celulares dos colaboradores? Neste último caso, como isto poderia ser feito considerando as questões legais?

Um outro exemplo está na mobilização de equipes de outras regionais. A fim de aumentar o número de equipes de manutenção da regional afetada pela tempestade severa, podem ser solicitadas equipes de outras regionais. Mas quais as regionais que fornecerão as equipes? Como será feita a acomodação destas equipes? Também, deve-se prever a alimentação. Como será feita a comunicação com estas equipes em campo – já que o sistema via rádio opera em faixas de frequência diferentes em cada regional? Etc.

É interessante destacar que muitas dessas medidas, para viabilizar os planos, alteram a forma de a empresa operar, por exemplo na introdução de uma nova tecnologia ou na introdução do terceiro tuno de uma função, para que trabalhe em regime ininterrupto.

Uma vez que as barreiras foram viabilizadas, já se tem como caracterizar as instalações da empresa e a forma de se executar as barreiras. Com isso, podem-se elaborar os planos preliminares. No caso da Celesc, utilizaram-se, intensamente, mapas mentais para organizar e

estruturar as informações para a elaboração dos planos.

O passo seguinte, então, foi a estimativa de esforço para implementar os planos. Fundamentalmente, este processo consiste no levantamento dos custos para implementar os planos e do uso dos recursos internos (tanto humano quanto material), para, posteriormente, avaliar se o esforço necessário é justificado, na avaliação custo-risco-benefício.

Por fim, foi feito um planejamento para a implementação dessas ações – destacando o responsável, o custo e o prazo para implementação –, que foi incluído no plano de ações.

6.3.2.3 Fases do delineamento detalhado

Os mapas mentais também auxiliaram no detalhamento dos planos. De fato, os planos de aceitação foram condensados em um único procedimento interno, chamado de "Instrução para atendimento em estado de contingência" (CELESC, 2005a), ilustrado na Figura 6.19[12] e apresentada no Anexo A.

No que se refere ao monitoramento & controle, optou-se por atuar na preparação para a ocorrência do incidente, já que não se pode controlar um evento meteorológico.

O planejamento da gestão do incidente foi trabalhado a fim de diminuir o período em que os consumidores passariam sem fornecimento de energia na ocorrência de uma tempestade severa, elaborando um plano de resposta emergencial (designado de "estado de contingência") e de retorno à condição normal de operação (fim do estado de contingência). Por fim, o Anexo I ilustra a cronologia por meio de um fluxograma.

O Quadro 6.6 traz a descrição dos principais itens da estrutura. Note-se que os três primeiros itens se referem ao monitoramento & controle, enquanto o quarto à resposta emergencial e, finalmente, o quinto item, ao retorno.

Observe-se que a comunicação com as partes envolvidas (*stakeholders*) está definida dentro da instrução – no item "das informações à mídia", por exemplo.

Quanto à capacitação, ela contemplou a apresentação do procedimento, a revisão das atribuições de cada envolvido e um teste de mesa. No teste de mesa, analisam-se, "passo a passo", as ações previstas na instrução, para verificar se houve um correto entendimento das ações, da cronologia, das interações delas e das atribuições de cada colaborador.

Também foi salientada a importância de se fazer exercícios periódicos, simulando uma

[12] Ao longo do projeto com a Celesc, foi utilizado o *software* View Your Mind <http://www.insilmaril.de/vym/>para a elaboração dos mapas mentais; no entanto, esta figura foi obtida a partir do *software* XMind <http://www.xmind.net/>

situação de contingência.

Adicionalmente, foi prevista a capacitação dos colaboradores envolvidos no processo de monitoramento, quanto às informações meteorológicas.

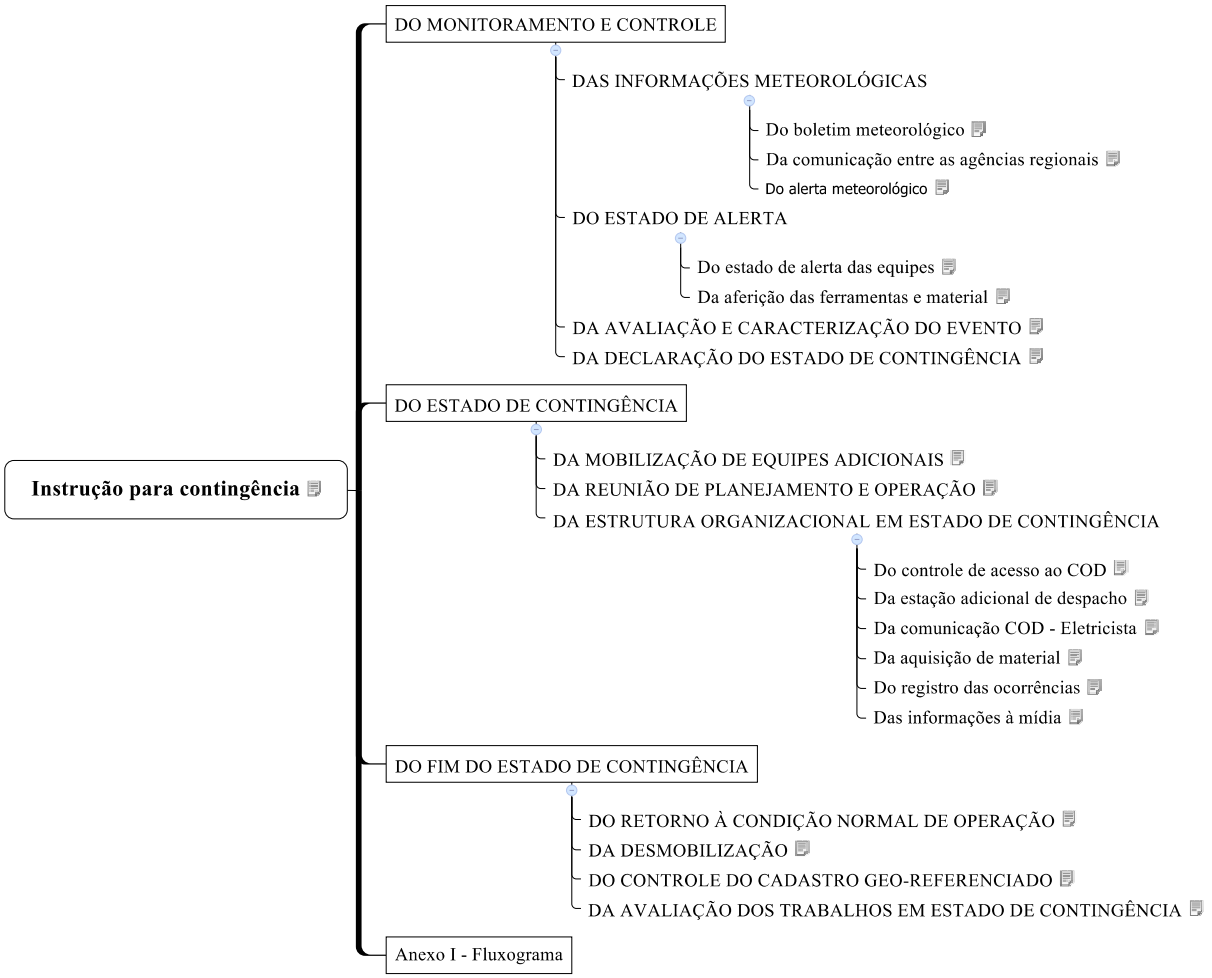


Figura 6.19: Estrutura da instrução para contingência (apresentada no Anexo A)

Por fim, foi elaborado um plano de ação para adequar as instalações e estrutura organizacional, para que a instrução fosse efetiva, chamado de "Insumos à implantação da instrução para atendimento em estado de contingência" (CELESC, 2005b).

Destacam-se medidas como (DIAS et al., 2006, p. 4):

- adequação das instalações, equipamentos e ferramental para possibilitar o atendimento em estado de contingência;
- implementação de sistemas alternativos de comunicação entre COD e equipes de campo;
- implementação do esquema de prioridade para restabelecimento de carga (religamento);

- geradores portáteis para alimentar estações repetidoras de telecomunicação da Celesc;
- disponibilização de uma verba anual para contingência; entre outras.

Quadro 6.6: Estrutura cronológica da instrução

1. **Monitoramento da condição meteorológica:** Definiram-se as fontes de informações e os indicadores a serem considerados, além dos responsáveis e da frequência.
2. **Estado de alerta:**Dada a possibilidade de ocorrência de uma tempestade severa, procura-se avaliar a disponibilidade de recursos para uma ação mais efetiva, corrigindo eventuais carências.
3. **Avaliação e caracterização do evento:** Diante da tempestade severa, estruturam-se ações para caracterizar o impacto real do evento e toma-se a decisão de decretar ou não estado de contingência.
4. **Estado de contingência:** Mobilizam-se equipes de campo adicionais (disponíveis na própria regional ou em outras, previamente definidas) para atuar no restabelecimento do fornecimento de energia. Modifica-se a estrutura organizacional da agência para ter controles mais rígidos de acesso à agência, disponibilizar alimentação e acomodação às equipes adicionais, definir como será feita a comunicação com as equipes adicionais, aumentar a capacidade de gerenciamento das equipes de campo por parte do COD, definir como será aferido o atendimento das reclamações dos consumidores e como deverá ser feita a comunicação com a mídia.
5. **Fim do estado de contingência:** Definiu-se como fazer o retorno à condição normal de operação e a desmobilização das equipes adicionais. Neste momento, deve-se fazer uma avaliação dos trabalhos em estado de contingência, destacando: o desempenho (erros e acertos cometidos); possíveis melhorias nos procedimentos; o cumprimento do procedimento de operação frente à tempestade severa; os custos associados ao processo de operação em estado de contingência; a análise do cumprimento dos procedimentos de segurança e levantamento do número de acidentes.

6.4 Avaliação da metodologia

A avaliação da metodologia desenvolvida foi feita de duas formas distintas, mas complementares entre si. A primeira objetivou avaliar o resultado dos estudos de caso realizados, e a segunda teve como objetivo confrontar a metodologia desenvolvida com alguns requisitos levantados, conforme apresentado nas duas próximas seções.

6.4.1 Avaliação com base nas considerações feitas pelas empresas onde foram realizados os estudos de caso

A avaliação da metodologia nas empresas onde foram realizados os estudos de caso foi feita por meio de entrevistas semiestruturadas, que se caracterizam pelo fato de o entrevistador decidir pela forma de abordar o assunto da entrevista e pela sequência dos pontos abordados – que são previamente especificados em uma guia de entrevista (lista de tópicos).

Esta forma de entrevista foi selecionada por permitir que os entrevistados discorram sobre os assuntos abordados, mantendo o rumo natural da conversa, sem perder o foco da pesquisa[13].

Foram entrevistados dois colaboradores[14] da Eletrosul Centrais Elétricas S.A. e um[15] da Celesc (Centrais Elétricas de Santa Catarina S.A.). As entrevistas foram realizadas em reuniões individuais, e os comentários foram sistematizados de acordo com os tópicos abordados e transcritos na forma de ata. Estas informações foram, então, tratadas e apresentadas a seguir:

- **Técnicas e ferramentas utilizadas:** Os entrevistados consideraram adequadas as técnicas e ferramentas utilizadas. No caso da Eletrosul, foi destacado que existia um sentimento dos especialistas sobre o que estava acontecendo e que as técnicas utilizadas permitiram comprovar a impressão que se tinha, formalizando o conhecimento (tanto no que se refere aos processos quanto ao disjuntor). Elas também possibilitaram ver o fluxo das informações, deixando claro a situação da empresa. Foi destacado, ainda, que as técnicas permitiram mapear e evidenciar o problema, traduzindo para uma forma mais clara; e que as técnicas podem ser úteis para a capacitação de colaboradores da empresa, pois o conhecimento está sistematizado. Por fim, destacou-se que a estrutura FMEA / CNEA se mostrou mais adequada ao projeto e que, inicialmente, tinha sido cogitado utilizar a estrutura ETA / FTA. No que se refere à Celesc, destacou-se que as técnicas e ferramentas utilizadas possibilitaram evidenciar as carências da empresa e as tomadas de decisão que foram bem sucedidas e as que atrasaram ou prejudicaram o processo de restabelecimento, em outras ocorrências de tempestades severas. Por fim, foi destacado que existem inúmeras técnicas e ferramentas para dar suporte aos processos, e a seleção de uma (ou mais) é dada pela conveniência. Eventualmente, uma técnica mais simples é suficiente, e a adoção de outras mais sofisticadas poderiam melhorar as respostas, mas com um custo que

[13] Santos & Candeloro (2006, p. 75) salientam que, na literatura pertinente à metodologia de pesquisa, não se encontra um conceito claro e preciso do que é uma entrevista semiestruturada. Entretanto, considerando que ela seja uma intermediária entre a estruturada e a não-estruturada, supõe-se que "[...] haja uma confluência de perguntas previamente elaboradas com outras pautadas a partir das respostas e elucubrações dos entrevistados".

[14] Gerente do Departamento de Manutenção do Sistema e Gerente de Projeto do Departamento de Planejamento Pesquisa e Desenvolvimento.

[15] Chefe da Divisão de Operação da Distribuição.

pode não ser justificado. No caso da Celesc, a única técnica utilizada que não se conhecia foi a IDEF0; no entanto, a técnica foi bem compreendida e não existiu dificuldade em utilizá-la.

- **Caracterização do sistema em análise:** Foi destacado, no projeto com a Eletrosul, que a caracterização foi adequada e realizada de maneira abrangente. O trabalho não se restringiu ao estudo de vazamento no disjuntor, mas se ateve a todo o gerenciamento do SF_6 na empresa. Com isto, foi possível evidenciar os maiores problemas relativos ao uso do SF_6. No caso da Celesc, a opinião foi de que a situação existente ficou bem caracterizada, o que possibilitou tomar ações direcionadas para os pontos-chave. Destacou-se que foi feito o delineamento da operação dos CODs em condição normal (utilizando IDEF0) e, posteriormente, foram feitas entrevistas com especialistas e com pessoas que vivenciaram a condição de operação na ocorrência de tempestades severas – o que permitiu identificar perturbações possíveis de ocorrer durante a operação nesta condição. Muitas destas perturbações já tinham sido levantadas e as entrevistas serviram para esclarecer como ocorreram; no entanto, foram identificadas situações que a equipe de análise não tinha considerado.
- **Integração dos atributos segurança e continuidade / disponibilidade:** Na Eletrosul, foi destacado que tratar a segurança e a continuidade (ou disponibilidade, no caso do disjuntor) de forma integrada possibilitou tomar ações de forma mais efetiva, pois tratou a situação como um todo. O resultado ficou mais claro, dinâmico e mais fácil de implementar. Se a segurança fosse tratada separadamente da continuidade (ou da disponibilidade), seriam delineadas muitas soluções e não se saberia o que implementar. Integrando estes dois atributos, puderam-se otimizar as soluções. Destacou-se, ainda, que pode até ser razoável, em uma análise, pensar nestes dois atributos separadamente; no entanto, em condição real, não é possível separá-los. Eles devem ser tratados de maneira integrada. No caso da Celesc, foi destacado que as ações são sempre delineadas pensando nestes dois atributos – possivelmente pelo fato de se estar trabalhando com redes elétricas, que têm um grande potencial para gerar dano. O estudo sobre o ferramental é um exemplo disso: possibilita uma ação mais efetiva e mais segura.
- **Soluções apontadas:** No projeto com a Celesc, foi destacado que, inicialmente, acreditava-se que o problema era apenas organizacional, o que seria solucionado apenas com a instrução. No entanto, com o projeto, identificaram-se outras necessidades na estrutura da empresa, resultando em dois planos de ação – um para a operação e outro para as telecomunicações. Na Eletrosul, destacou-se que as recomendações certamente irão contribuir para se alcançar o nível de perda de SF_6 que a empresa espera, mas a avaliação do impacto

dessas medidas somente será percebida depois de algum tempo. No entanto, acredita-se que simplesmente o fato de mostrar a preocupação com o gás já tenha despertado o interesse dos colaboradores pelo assunto, o que irá contribuir para a redução das perdas.

- **Implementação dos planos:** Na Celesc, o que não foi implementado está contemplado no planejamento. A ações foram passadas para a diretoria, que, por sua vez, decide pela implementação. A maioria das medidas foram de baixo custo e puderam ser rapidamente implementadas. Acredita-se que estas medidas terão maior impacto nos riscos, e as ações de maior custo contribuirão para aprimorar o que já foi implementado. Quanto à instrução, ela foi implementada e está em uso. As equipes de todos os COD receberam a devida capacitação quanto à instrução, além da capacitação prevista no plano de ações – quanto à formação meteorológica, por exemplo. No caso da Eletrosul, foi destacado que estão sendo implementadas, primeiramente, as recomendações que estão na esfera de decisão do DMS (portanto, não precisam de aprovação do orçamento da empresa), sendo que algumas delas já foram implementadas. Destacou, ainda, que algumas recomendações implicam alteração de procedimentos, o que requer uma tramitação interna, que demanda tempo. No entanto, estas alterações estão planejadas e serão implementadas dentro das prioridades da Eletrosul.
- **Utilização e revisão dos planos**[16]**:** A instrução está ativa e foi executada nas últimas situações em que ocorreram tempestades severas. A estrutura implementada com os planos de ação – como o *kit* contingência – está sendo mantida e utilizada, quando necessário. No entanto, por restrições da empresa, não tem sido executada a avaliação dos trabalhos ao final de cada execução da instrução (i.e., ao final do estado de contingência). Estas avaliações objetivavam formalizar as lições aprendidas e revisar os planos a fim de identificar possíveis deficiências e melhorias para que se tenha um aprimoramento contínuo.
- **Processo de aplicação da metodologia:** Para a Celesc, a metodologia possibilitou contornar alguns problemas fornecendo um método que, por exemplo, facilitou o entendimento dos processos (pelo IDEF0 e pelas entrevistas). Também foi destacado que a dedicação e o comprometimento da equipe foram fundamentais para o sucesso do projeto. A equipe do projeto estava disposta a trabalhar com pesquisa, possibilitando mesclar o conhecimento técnico dos especialistas com a estrutura metodológica trazida pelo NeDIP / UFSC. Na aplicação na Eletrosul, destacou-se a alocação de recursos humanos como sendo a grande dificuldade, pois os colaboradores tiveram dificuldade de dedicar tempo ao projeto, sem deixar de cumprir as atribuições normais de sua função dentro da empresa. Desta forma, o comprometimento da equipe com o trabalho foi fundamental para

[16]Os planos ainda não foram implementados na Eletrosul, portanto este item se restringirá à Celesc.

o sucesso do projeto. Outro ponto identificado foi o fato de o projeto envolver pessoas de diversas áreas e localidades diferentes (Curitiba, Xanxerê, Campos Novos, Palhoça, Florianópolis, entre outras), o que dificultou a comunicação e a reunião destes especialistas. Destacou-se, ainda, que a quantidade de informação gerada foi suficiente para o entendimento dos problemas e que, pela falta de tempo, existiu uma dificuldade de se absorver e depurar toda essa informação. Desta forma, o assunto não se esgotou dentro da empresa, e o conhecimento gerado no projeto ainda será mais explorado. Como pontos positivos, destacam-se: (1) o uso das técnicas, que foram de fácil entendimento, auxiliaram nos processos da metodologia e contribuíram para contornar o problema da falta de tempo disponível; (2) o fato de se ter integrado, formalizado e sistematizado o conhecimento tácito dos especialistas; e (3) a integração da empresa com a universidade na parceria realizada.

- **Resultados do projeto:** No que se refere ao projeto MitiSF6, com a Eletrosul, os resultados foram considerados bons e destacou-se que foi possível: racionalizar o uso do gás na Eletrosul; tratar os processos relativos à manipulação do SF_6 da melhor maneira possível; sistematizar as informações, já que a informação é que permite fazer o controle do uso do gás; etc. Também foi destacada a expectativa do livro que está sendo elaborado, objetivando condensar o conhecimento gerado no projeto. Quanto ao projeto com a Celesc, os produtos do projeto foram considerados bons: foi gerada uma instrução e dois planos de ação (para a operação e para as telecomunicações). No entanto, foi levantada a falta de métricas para avaliar o impacto da implementação da instrução na empresa. O chefes dos CODs comentam que executaram a instrução, elogiam, mas não se tem como avaliar, de forma objetiva, o benefício para a Celesc. Apesar disto, alguns pontos foram destacados: verificou-se que não existem mais restrições de uma agência regional fornecer equipes para outras; o boletim meteorológico e o alerta meteorológico têm auxiliado no monitoramento das tempestades severas; o ferramental disponível para as equipes de campo também melhorou e foi desencadeado um processo dentro da empresa que irá resultar em uma instrução para padronizar as ferramentas e garantir que os eletricistas tenham todas as ferramentas necessárias a sua disposição; etc. Desta forma, destacou-se que houve um aprimoramento geral: melhorou o atendimento diante de tempestades severas; melhorou a capacitação dos colaboradores; e melhorou a condição da empresa. Destacou-se, ainda, que isto possivelmente aconteceu por ter sido selecionado, como objeto de estudo do projeto, o que era o maior problema da empresa: operar diante de uma tempestade severa. É interessante destacar que a empresa ainda pretende implementar um sistema de gerenciamento de risco mais amplo.

6.4.2 Avaliação com base em requisitos identificados

Durante o projeto MitiSF6, com a Eletrosul, foi feito um desdobramento da função qualidade (QFD – *quality function deployment*), de como deveria ser a metodologia para mitigação de perdas de SF_6 que estava sendo desenvolvida, apresentado no documento MT-MP-RT-NE-01 (UFSC/NEDIP, 2008i). Pode-se, então, extrapolar os requisitos identificados – que são específicos para o contexto do SF_6 – para o contexto de uma metodologia de gerenciamento de risco. A seguir, apresentam-se os requisitos para a metodologia de gerenciamento de risco obtidos a partir do estudo realizado no projeto MitiSF6 (UFSC/NEDIP, 2008i), juntamente com outros que foram considerados relevantes:

a. A metodologia deve utilizar técnicas de suporte (em confiabilidade / manutenção / risco) consagradas.

   Comentário: As técnicas utilizadas – destacadamente FMECA; FTA; IDEF0; redes bayesianas; e atualização bayesiana – são largamente utilizadas em estudos em diversas áreas. É importante destacar que a técnica CNEA é recente, já que foi desenvolvida neste doutorado; no entanto, ela é baseaba em duas técnicas consolidadas – a saber: BTA e redes causais –. Assim, acredita-se que não existirão dificuldades em futuras aplicações. Note-se que as técnicas IDEF0, FMECA, CNEA e FTA foram utilizadas com fluência pelas equipes, no projeto com a Eletrosul – após uma pequena capacitação, apresentando cada uma delas.

b. Deve existir material didático disponível sobre as técnicas utilizadas.

   Comentário: O material disponível sobre as técnicas é vasto, tais como livros, normas técnicas, trabalhos acadêmicos (teses, dissertações, etc.), artigos, entre outros. Adicionalmente, foram gerados pelo NeDIP / UFSC textos didáticos, que – tipicamente – trazem um resumo sobre a técnica, exemplos de aplicação e uma lista de *softwares* para dar suporte à técnica (vide Quadro 4.1).

c. A metodologia deve levar em consideração as questões referentes à segurança e à disponibilidade (ou continuidade) do sistema.

   Comentário: A metodologia desenvolvida trata a segurança e a disponibilidade (ou continuidade) dos sistemas como atributos; portanto,puderam ser integrados em um único sistema de gestão de risco. No projeto MitiSF6 com a Eletrosul, por exemplo, foram considerados incidentes com comprometimento à segurança, tais como: dano à saúde dos colaboradores pela inalação de subprodutos tóxicos do SF_6 e dano ao meio ambiente pela contribuição ao efeito estufa decorrente do SF_6 perdido para a atmosfera. Também foram considerados incidentes com comprometimento à continuidade da operação do DMS e

a disponibilidade do disjuntor (no caso o Merlin Gerin, modelo FA4), tais como: atraso na manutenção por indisponibilidade de SF_6 e ocorrência de alarme seguido de *trip* do disjuntor, impossibilitando a execução de manobras do equipamento.

d. A metodologia deve indicar técnicas e ferramentas que possibilitem estudar os processos do sistema que se deseja analisar.

   Comentário: Ao longo do Capítulo 5, apresentam-se algumas técnicas que podem ser utilizadas. Nos estudos de caso, foram utilizadas as técnicas IDEF0, para análise funcional, e FMEA, CNEA e FTA para análise e tratamento dos riscos.

e. A metodologia deve auxiliar na identificação de métricas para avaliação dos riscos.

   Comentário: Na Seção 5.3.1.1, foram apresentados alguns exemplos de indicadores para avaliação de risco, no caso NetCAF, MTO e RPO. Também foi apresentado um método para avaliação com base em limites de ocorrência do incidente e níveis de benefícios decorrentes da exposição ao risco.

f. A aplicação da metodologia deve fomentar o comprometimento dos colaboradores da organização.

   Comentário: A implementação de um sistema de gerenciamento de risco já demonstra uma preocupação com os colaboradores e a sociedade de maneira geral, favorecendo o relacionamento entre a organização e todos afetados por sua operação (o que inclui seus colaboradores). A implementação da cultura do risco é outro fator importante nesta questão, pois os colaboradores passam a identificar a importância de suas ações na segurança e na disponibilidade dos sistemas técnicos, na operação da unidade organizacional e no negócio da organização. Adicionalmente, as novas atribuições decorrentes da implementação do SGR também são um fator motivacional – de acordo com a Teoria dos Dois Fatores de Frederick Herzberg –, o que também potencializa o comprometimento dos colaboradores da organização.

g. A aplicação da metodologia deve evidenciar a necessidade de se identificar leis, regulamentações e normas referentes ao escopo.

   Comentário: As leis, regulamentações e normas, na elaboração devem ser consideradas ao longo da aplicação da metodologia. Por exemplo: durante a caracterização do sistema em análise, na fase do delineamento informacional, é feito o levantamento das restrições, que incluem leis, regulamentações e normas. Estas restrições, por sua vez, serão consideradas para estipular os objetivos de risco. Na aplicação da metodologia na Celesc, por exemplo, a resolução ANEEL Nº 024 "Estabelece as disposições relativas à Continuidade da Distribuição de energia elétrica às unidades consumidoras" (ANEEL, 1994, p. 1).

h. A aplicação da metodologia deve possibilitar a caracterização de uma estrutura mínima,

que deve ser implementada para se executar os procedimentos definidos.

Comentário: A estrutura mínima deve ficar evidenciada na fase do delineamento preliminar, quando se viabiliza a implementação das barreiras identificadas na fase do delineamento conceitual. As ações para adequar a estrutura existente devem estar inseridas no plano de ações. Por exemplo, no projeto com a Eletrosul, foi delineada uma sugestão de estrutura mínima que continha, entre outros itens: equipamentos de tratamento do gás, instrumentos de medição, quantidade de cilindros de SF_6 disponível em cada local, etc.

i. A aplicação da metodologia deve possibilitar a identificação de formas de monitorar riscos e prevenir incidentes.

Comentário: Durante a análise dos riscos, utilizando a estrutura FMECA / CNEA, puderam-se identificar possíveis barreiras na corrente causal que possibilitem fazer o monitoramento dos riscos e controlar eventuais desvios. Estas barreiras, posteriormente, serão incluídas no plano de monitoramento & controle. Na Eletrosul, por exemplo, foi indicada a necessidade de se ter balanças para avaliar a massa de SF_6 nos cilindros, a fim de evitar atrasos na manutenção pela falta do gás. Esta medida possibilita o monitoramento da quantidade de gás disponível em cada local e, caso esteja abaixo do "estoque mínimo", deflagra-se o processo de controle, que é solicitação de SF_6.

j. A aplicação da metodologia deve possibilitar que se identifiquem formas de gerenciar o incidente, caso ele ocorra.

Comentário: Da mesma forma que as barreiras para o monitoramento do risco, as barreiras para gerenciamento de incidente serão obtidas das análises e, posteriormente, incluídas nos planos de resposta emergencial e de operação alternativa. O estudo de caso na Celesc ilustra esta situação nos procedimentos de inclusão de equipes de manutenção de outras agências regionais, para o caso de sobrecarga na manutenção de emergência.

k. A aplicação da metodologia deve possibilitar a identificação de requisitos para a especificação técnica de compra de equipamentos.

Comentário: Durante a análise de uma unidade organizacional, podem-se evidenciar requisitos para os sistemas técnicos (que devem ser considerados na fase do delineamento informacional da aplicação neste sistema). Na análise do sistema técnico, também podem ser identificadas barreiras que evidenciem requisitos deste sistema (ou de sistemas com que ele interage). Assim, é recomendado que estes requisitos façam parte das especificações técnicas de futuras aquisições de equipamentos. Isto pode ser ilustrado na análise do disjuntor, que evidenciou a necessidade de se incluir o padrão de conexão da linha de SF_6, na especificação técnica de compra. Também foram levantados requisitos para a especificação técnica dos equipamentos de tratamento do gás, na análise do DMS, tais

como: compressor e bomba de vácuo livres de óleo, possibilidade de operar com cilindro externo, reservatório incorporado, conexões por engate rápido padrão Eletrosul, etc.

6.5 Considerações finais

No Capítulo 6, foram apresentadas as aplicações da metodologia no âmbito da unidade organizacional e do sistema técnico.

Neste primeiro caso, a aplicação na Eletrosul abordou as etapas de planejamento e delineamento, até a fase preliminar – acontecendo o mesmo para o âmbito do sistema técnico. Na Celesc, por sua vez, destacou-se a elaboração dos planos, nas fases do delineamento preliminar e detalhado.

Na aplicação na Eletrosul, destaca-se, no planejamento, o comprometimento da empresa com o projeto MitiSF6. Já na etapa de delineamento, evidenciou-se a utilidade da estrutura CNEA/FMECA. Ela possibilitou identificar incoerências nas análises, pois os diagramas apresentam as ligações entre os elementos do modelo, além de apresentar elementos intermediários na cadeia causal.

No relatório MT-DJ-RT-NE-04 (UFSC/NEDIP, 2008a), destacou-se, ainda:

> O uso de CNEA mostrou-se fundamental para auxiliar no entendimento das relações entre as falhas, na comunicação entre os membros da equipe e, consequentemente, no desenvolvimento da FMEA. Uma das grandes vantagens do método é permitir visualizar os pontos onde serão implementadas as barreiras, sendo uma importante técnica para complementar as deficiências da FMEA.

De fato, o que se observou, nas implementações da estrutura FMECA / CNEA, foi que era comum fazer alterações significativas na FMECA quando se fazia a análise primeiramente na tabela e depois se modelavam os diagramas CNEA. No entanto, o conteúdo permaneceu o mesmo – ou sofreu alterações menores – quando se elaborou o diagrama e, posteriormente, representou-se na tabela.

Isto demonstra que a representação gráfica possibilitou uma melhor contextualização do modelo e, por consequência, uma análise mais eficaz – além de gerenciar melhor o conhecimento gerado, facilitando sua institucionalização.

Na aplicação na Celesc, mais uma vez, observou-se que o apoio da gerência foi fundamental para o sucesso do gerenciamento de risco, pois foi determinante para garantir a disponibilidade de recursos, o comprometimento dos colaboradores envolvidos e o apoio para a implementação das decisões.

Também foi evidenciada a necessidade de se adaptar os planos aos costumes da empresa. Neste sentido, a elicitação do conhecimento foi feita por entrevistas com colaboradores que vivenciaram o problema de se operar na ocorrência de uma tempestade severa, a fim de delinear a melhor forma de implementar as barreiras. O delineamento dos planos também contou com a constante participação de colaboradores que irão atuar durante a operação diante de uma tempestade severa. Posteriormente, a instrução foi submetida aos colaboradores para que eles comentassem, a fim de validá-la antes de submeter à aprovação da alta gerência. Desta forma, entende-se que, tanto a instrução gerada quanto o plano de ação tornam-se mais aderentes aos costumes e ritos já existentes, facilitando a implementação da cultura do risco no *modus operandi* da empresa.

Por fim, neste capítulo, foi feita a avaliação da metodologia desenvolvida. Esta avaliação foi feita em duas partes: uma procurou captar, das empresas em que foi aplicada a metodologia, a opinião sobre alguns pontos, apresentados na Seção 6.4.1; outra objetivou confrontar a metodologia com alguns critérios que se consideraram importantes.

7 *Conclusões e recomendações para trabalhos futuros*

Nos capítulos iniciais deste documento, procurou-se evidenciar a necessidade de integrar, em um único sistema de gestão, as questões abordadas no gerenciamento de segurança e no gerenciamento da continuidade de negócio – destacadamente no Capítulo 3, em que se apresentou uma revisão sobre gestão de segurança e continuidade em alguns setores; e na introdução (Capítulo 1), em que foi dado ênfase ao contexto das necessidades neste campo de conhecimento, com destaque para os objetivos e resultados esperados para este trabalho de doutorado.

No Capítulo 2, por sua vez, foram exploradas algumas considerações sobre a nomenclatura dessas duas abordagens e foram propostas, quando pertinente, definições de termos que permitam suprir as necessidades de um gerenciamento de risco que integre segurança e continuidade.

O Capítulo 4 conclui a revisão bibliográfica e apresenta, resumidamente, algumas técnicas que podem ser usadas para dar suporte à metodologia desenvolvida.

A metodologia desenvolvida está apresentada no Capítulo 5, e sua aplicação está no Capítulo 6. Na próxima seção, será feita uma análise dos resultados deste doutorado, destacando as contribuições do trabalho, e – por fim – na Seção 7.2, apresentam-se as recomendações para futuros trabalhos.

7.1 Análise dos resultados e identificação das contribuições

Como resultados do trabalhado, além da metodologia, destaca-se que foram compatibilizados conceitos e nomenclatura adotados no gerenciamento de segurança e de continuidade – apresentados ao longo do texto, destacadamente no Capítulo 2, e no Glossário. De fato, isto foi necessário, pois cada uma destas abordagens designava um mesmo conceito de maneira diferente, como destacado na Seção 3.7, dificultando a integração. Entende-se que a comunicação é um dos fatores de grande importância para as ações no contexto da segurança e continuidade, sendo, assim, oportuna a compatibilização da nomenclatura.

Também foram sistematizadas técnicas de suporte que podem contribuir com a unificação do gerenciamento de risco, apresentadas no Capítulo 4. Destaca-se o desenvolvimento da técnica CNEA, para a qual foi proposta uma sintaxe, identificando elementos que a compõem.

A metodologia desenvolvida faz, ainda, uso de uma estrutura de trabalho (*framework*) baseada nas técnicas FMECA e CNEA. Durante a aplicação desta estrutura, no estudo de caso com a Eletrosul, observou-se que ela permite uma análise mais eficiente dos modos de falha (ou de incidente). Também foram feitas análises de falha, utilizando FTA, de algumas causas da FMECA / CNEA do disjuntor, evidenciando a integração desta estrutura com outras técnicas. De fato, o detalhamento da causa poderia ter sido feito na própria CNEA; no entanto, optou-se por detalhá-la em uma FTA para não sobrecarregar o diagrama CNEA, além da possibilidade de visualizar os tipos de relações existentes na FTA por meio dos operadores lógicos. Note-se que a FTA exige um conhecimento maior sobre o sistema a ser modelado, mas, por outro lado, resulta em um diagrama mais detalhado. Num instante seguinte, por exemplo, poderia ser calculada a probabilidade de ocorrência do evento topo, em face da existência dos operadores lógicos. Esta ação não poderia ser feita na CNEA, sendo esta uma das limitações da técnica.

Assim, foi proposta a integração das técnicas redes bayesianas e atualização bayesiana à estrutura de trabalho. As redes podem contornar a carência de tratamento estatístico da FMECA / CNEA, e a atualização bayesiana pode ser utilizada para gerar estimadores para os parâmetros a serem utilizados nas redes e nas FTAs. No entanto, esta integração não foi aplicada no referido estudo de caso, sendo uma das limitações deste trabalho. Destaca-se que Léger et al. (2006) utilizam redes bayesianas em conjunto com BTA e que os autores incluem eventos intermediários na BTA, resultando em um diagrama similar a uma CNEA. Entretanto, os autores utilizaram a BTA para modelar incidentes no nível técnico e, posteriormente, incluíram estas informações em uma rede bayesiana mais abrangente. Note-se que, apesar de não utilizarem a teoria de redes bayesianas para fazer o tratamento estatístico de uma CNEA, eles apresentam aplicações que evidenciam esta possibilidade.

Outra limitação deste trabalho está no fato de a metodologia não ter sido aplicada no nível da organização. De fato, o objetivo geral deste trabalho está focado no âmbito do sistema técnico e da unidade organizacional, que foram contemplados nos estudos de caso. No entanto, acredita-se que a adaptação da metodologia para a realidade do nível da organização possibilitará uma gestão do negócio mais estruturada, por exemplo, gerenciando melhor os recursos para se obter uma ação mais efetiva no sentido dos valores da organização.

No que se refere aos estudos de caso nas duas empresas do setor elétrico, a aplicação da metodologia implicou recomendações e alterações nos procedimentos internos e na estrutura

das empresas, conforme apresentado no Capítulo 6. No entanto, estes estudos de caso não contemplaram todas as etapas da metodologia, sendo ainda necessária a sua aplicação como um todo.

No caso da distribuidora de energia, a aplicação contemplou as etapas de delineamento e de implementação – sendo que a implementação foi feita sem a participação da equipe do NeDIP / UFSC. Destaca-se, como resultado: a elaboração de uma instrução (norma interna) para atendimento emergencial diante de tempestades severas (apresentada no Anexo A); a adequação das instalações, equipamentos e ferramental para possibilitar o atendimento nesta condição; a implementação de sistemas alternativos de comunicação; a implementação do esquema de prioridade para restabelecimento de carga (religamento); a aquisição de geradores portáteis; a disponibilização de uma verba anual para contingência; entre outras. Note-se que estas medidas implicam melhorias tanto para a continuidade quanto para a segurança. A implementação de sistemas alternativos de comunicação, por exemplo, foi feita para garantir a comunicação do despachante com as equipes de manutenção de campo. Esta comunicação é muito importante para a segurança dos mantenedores que interagem com o despachante durante as ações de campo, solicitando o desligamento de um alimentador, por exemplo. Esta comunicação, ainda, possibilita o despacho de novos serviços para a equipe de campo, portanto atuando na continuidade da operação do COD. É importante observar que, na falha dos sistemas de comunicação, ainda existe um processo alternativo para a execução do despacho. Este processo alternativo é feito pela entrega das ordens de serviço em mãos, exigindo que a equipe de manutenção retorne ao COD. Isto implica considerável degradação no desempenho do despacho, consumindo um tempo importante – que poderia estar sendo utilizado em outra ação de manutenção a fim de restabelecer o fornecimento de energia elétrica.

Quanto à empresa transmissora de energia elétrica, a aplicação contemplou as fases do delineamento informacional, conceitual e a parte inicial do preliminar. Como resultado, destacam-se as recomendações referentes à política de atualização tecnológica; à política de atualização dos procedimentos; e à política de capacitação. Também foram elencadas algumas recomendações de responsabilidade da ANEEL (Agência Nacional de Energia Elétrica) referentes à política regulatória. Note-se que, aqui, a segurança e a continuidade também foram abordadas como atributos tratados durante o delineamento. Assim, as barreiras levantadas – e transcritas nas recomendações – foram delineadas a fim de atuar para a melhoria destes dois atributos.

Destaca-se, ainda, o desenvolvimento da ferramenta computacional OpenFMECA que, atualmente, auxilia a aplicação da técnica FMECA, mas está sendo desenvolvida para dar suporte a toda estrutura de trabalho proposta, o que inclui IDEF0, FMECA, CNEA, FTA e redes bayesianas, conforme apresentado na Seção 5.4 e no Apêndice A.

Assim, conclui-se que o trabalho alcançou seus objetivos específicos apresentados na Seção 1.2.2, a saber: propor vocabulário único para suprir as necessidades do gerenciamento da continuidade e de segurança; propor e sistematizar técnicas de suporte consolidadas que possam contribuir com a unificação do gerenciamento de risco; desenvolver uma estrutura de trabalho que integre essas técnicas; e desenvolver ferramenta computacional (*software*) para auxiliar a aplicação de técnicas.

Quanto ao objetivo geral deste trabalho – que era desenvolver uma metodologia para gerenciamento de risco com foco em unidades organizacionais e em sistemas técnicos durante o uso, integrando o gerenciamento da continuidade e o gerenciamento de segurança em um único sistema de gestão –, entende-se que ele foi cumprido. A metodologia, apresentada no Capítulo 5, aborda a segurança e a continuidade como dois atributos a serem tratados na gestão do risco, permitindo a integração – o que contribui para uma abordagem de gerenciamento de risco mais satisfatória, que Chapman (2005) concluiu ser necessária. Para tanto, estratificou-se a organização em três níveis, a saber: nível da organização, nível da unidade organizacional e nível do sistema técnico.

Observe-se que os sistemas de gestão da continuidade do negócio usualmente se restringem a analisar incidentes com grandes proporções (desastres) a ponto de impossibilitar a operação da organização, por isso se concentram na gestão da informação, pois esta pode viabilizar o restabelecimento da organização. Os sistemas de gestão da segurança, por sua vez, usualmente se concentram em garantir que a probabilidade de que ocorram danos, principalmente ao homem e ao meio ambiente, esteja abaixo do patamar que se considera aceitável. Desta forma, atuam fundamentalmente na análise dos sistemas técnicos e na sua relação com o homem e o meio.

Por outro lado, ao fazer a integração, podem-se gerenciar os riscos com impacto na segurança, na continuidade do negócio da organização, na continuidade operacional da unidade organizacional e na disponibilidade do sistema técnico. Desta forma, as decisões não ficam estanques a cada nível ou a um determinado tipo de consequência, e evidenciam-se as relações existentes entre os riscos dos diversos sistemas. É interessante observar que a relação entre segurança e continuidade (ou disponibilidade dependendo do caso) nem sempre é positiva, conforme apresentado na Seção 2.3. Por exemplo, em alguns casos, a confiabilidade (e consequentemente a disponibilidade) de um sistema técnico pode ser determinante para a segurança e para a continuidade do negócio; em outros, pode ir de encontro à segurança.

No Capítulo 6, então, apresentam-se as aplicações da metodologia no âmbito da unidade organizacional e do sistema técnico, em duas organizações do setor elétrico. Nestas aplicações, foi possível ilustrar a gestão do risco considerando os dois atributos.

Por fim, na Seção 6.4, é feita uma avaliação da metodologia, na qual se apresenta a opinião das empresas onde ela foi aplicada e, também, se evidencia a aderência da metodologia a alguns critérios considerados relevantes.

7.2 Recomendações para trabalhos futuros

Ao longo deste trabalho, foram identificadas algumas carências que não puderam ser tratadas e que podem ser alvo de futuras pesquisas, a saber:

- **Considerar as questões dinâmicas dos sistemas na estrutura de trabalho proposta:** Na estrutura de trabalho proposta, não foi tratado o dinamismo do sistema, tanto os existentes pela variação da taxa de falha quanto pela alteração da condição do sistema ao longo do tempo. Assim, pesquisas neste sentido farão a modelagem, a partir desta estrutura, se aproximar melhor da realidade e, por consequência, permitindo uma melhor análise, avaliação e tratamento dos riscos.
- **Elaborar indicadores de eficácia do SGR:** Fazer estudo a fim de elaborar indicadores que expressem o impacto de se ter implementado o sistema de gestão de risco (SGR) na organização. Isto possibilitará avaliar o desempenho do SGR e indicar a conveniência de se investir mais no gerenciamento de risco, ou não.
- **Fazer aplicações da metodologia como um todo:** Propõe-se que sejam feitos estudos que incluam aplicações da metodologia – contemplando todas as etapas, nos três níveis do desdobramento da organização –, a fim de identificar melhorias e evidenciar as adequações necessárias para a aplicação em diferentes tipos de organizações.
- **Fazer aplicações da estrutura de trabalho proposta:** As aplicações da estrutura de trabalho proposta, no estudo de caso com a Eletrosul, não incluíram a integração com as redes bayesianas e atualização bayesiana. Assim, estudos que apliquem a estrutura de trabalho completa são oportunos – pois podem evidenciar carências e melhorias ainda não identificadas.
- **Desenvolvimento de ferramentas computacionais:** O *software* OpenFMECA está sendo desenvolvido para auxiliar na aplicação da estrutura de trabalho proposta (vide Apêndice A); no entanto, outros processos podem ser suportados por *softwares*, por exemplo, o uso da técnica FHA. Neste sentido, propõe-se que sejam desenvolvidos estudos que abordem o desenvolvimento e a aplicação destas ferramentas computacionais.
- **Elaboração de textos sobre as técnicas:** Estão sendo elaborados, no NeDIP / UFSC, textos didáticos para algumas das técnicas utilizadas, no entanto os textos sobre FHA e

ESD ainda estão pendentes. Destaca-se ainda a necessidade de publicação de documentos que padronizem a sintaxe de algumas técnicas, destacadamente CNEA e ESD.

Referências

ABB. **Live Tank Circuit Breakers – Buyer's Guide**: Doc. N° 1HSM 9543 22-00. 4. ed. [S.l.], 2008. Disponível em: <http://library.abb.com/>. Acesso em: 15 jan. 2009.

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA. **Resolução ANEEL N^{o} 024, de 27 de janeiro de 2000**. [S.l.], 1994. Disponível em: <http://www.aneel.gov.br/cedoc/res2000024-.pdf>. Acesso em: 05 jan. 2009.

ALBERTON, A. **Uma metodologia para auxiliar no gerenciamento de riscos e na seleção de alternativas de investimentos em segurança**. Dissertação (Mestrado em Engenharia de Produção) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 1996.

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.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 5462**: Confiabilidade e matenabilidade – terminologia. Rio de Janeiro, 1994. 37 p.

____. **ABNT NBR ISO/IEC 17799**: Tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

____. **ABNT ISO/IEC Guia 73**: Gestão de risco – vocabulário – recomendações para uso de normas. 1. ed. Rio de Janeiro, 2005.

AYYUB, B. M. Risk analysis and management. In: ____. **The Handbook of engineering**. 2. ed. Boca Raton, Florida: CRC Press LLC, 2005. cap. 207. ISBN 0-8493-1586-7.

BACK, N. et al. **Projeto integrado de produtos**: planejamento, concepção e modelagem. 1. ed. São Paulo: Editora Manole Ltda., 2008. 601 p.

BBC BRASIL. China pede desculpas à rússia por desastre ecológico. **Agência Estado**, 27 nov. 2005. Disponível em: <http://www.estadao.com.br/rss/agestado/2005/nov/27/3.htm>. Acesso em: 16 dez. 2005.

BEERENS, H. I.; POST, J. G.; UIJT DE HAAG, P. A. M. The use of generic failure frequencies in QRA: The quality and use of failure frequencies and how to bring them up-to-date. **Journal of Hazardous Materials**, Elsevier, v. 130, n. 3, p. 265–270, 2006.

BERNSTEIN, P. L. **Desafio dos deuses**: a fascinante historia do risco. Rio de Janeiro: Elsevier, 1997. 389 p. ISBN 85-352-0210-2.

BOERLAGE, B. **Link Strength in Bayesian Networks**. 104 p. Dissertação (Master of science) — University of British Columbia Vancouver, Vancouver, Canada, 1994.

BOTHA, J.; VON SOLMS, R. A cyclic approach to business continuity planning. **Information management and computer security**, Emerald Group Publishing Limited, v. 12, n. 4, p. 328–337, 2004.

BRASIL. Câmara dos Deputados. Ouvidor pede cpi para vazamentos tóxicos. **Jornal da Câmara**, Câmara dos Deputados, Brasília, n. 982 (Ano 5), maio 2003.

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, 1998.

BRASIL. Ministério do Planejamento e Orçamento. **Glossário de defesa civil, estudos de riscos e medicina de desastres**. Brasília, DF, 1998.

BRASIL. Ministério do Trabalho e Emprego. **NR 10 – Normas regulamentadoras de segurança e saúde no trabalho nº 10**: segurança em instalações e serviços em eletricidade. Brasília, DF, 2004.

BÜHLMANN, H. **Mathematical methods in risk theory**. Berlin: Springer-Verlag, 1970.

BUSINESS CONTINUITY INSTITUTE. **Business Continuity Management**: Good practice guidelines. Caversham, UK, 2005.

CALIL, L. F. P.; HIRANO, E. W.; DIAS, A. A risks quantification procedure based on bayesian inference. In: INTERNATIONAL CONGRESS OF MECHANICAL ENGINEERING (COBEM 2005), Ouro Preto. In: . [S.l.: s.n.], 2005. **Proceedings ...**

CAPRA, F. **O tao da fisica**: um paralelo entre a física moderna e o misticismo oriental. 20ª. ed. São Paulo: Cultrix, 1988. 260 p. ISBN 8531603668.

CARPES JÚNIOR, W. P. **Análise da segurança humana para desenvolvimento de produtos mais seguros**. 251 p. Tese (Doutorado em Engenharia de Produção) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2004.

CASTRO, A. L. C. et al. **Manual de planejamento em Defesa Civil**. 1ª. ed. Florianópolis, 2005. volume I.

CELESC. DVOD (Divisão de Operação de Distribuição). **Instrução para atendimento em estado de contingência**. Florianópolis, 2005.

____. **Insumos à implantação da instrução para atendimento em estado de contingência**. Florianópolis, 2005.

CHAPMAN, J. Predicting technological disasters: mission impossible? **Disaster prevention and management**, Emerald Group Publishing Limited, v. 14, n. 3, 2005.

COOPER, D. F. **The australian and new zealand standard on risk management, AS/NZS 4360**: Tutorial standard. New Shouth Wales, Australia, 2004.

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**. Tese (Doutorado em Engenharia Mecânica) — Universidade Estadual de Campinas (UNICAMP), Campinas, 1996.

DIAS, A.; OGLIARI, A.; ALONÇO, A. S. Fatores de influência no projeto de produto para segurança. In: CONGRESSO BRASILEIRO DE GESTÃO DE DESENVOLVIMENTO DE PRODUTO (CBGDP), V., Curitiba. In: . [S.l.: s.n.], 2005. **Anais ...**

DIAS, A. et al. **Diagnóstico dos procedimentos de operação e de manutenção das empresas de geração de energia elétrica no Brasil**. [S.l.], 2000. Relatório final para a Superintendência de Fiscalização dos Serviços de Geração da Agência Nacional de Energia Elétrica (ANEEL).

____. Metodologia para gerenciamento de risco. In: SIMPÓSIO INTERNACIONAL DE CONFIABILIDADE (SIC), 4., Salvador. In: . [S.l.: s.n.], 2006. **Anais ...**

____. A framework for application of probabilistic risk analysis techniques. In: INTERNATIONAL CONGRESS OF MECHANICAL ENGINEERING (COBEM 2007), 19., Brasília. In: . [S.l.: s.n.], 2007. **Proceedings ...**

____. Análise de risco: uma síntese dos setores marítimo, aéreo e nuclear. In: CONGRESSO PAN-AMERICANO DE ENGENHARIA NAVAL TRANSPORTE MARÍTIMO E ENGENHARIA PORTUÁRIA (COPINAVAL), XX., São Paulo. In: . [S.l.: s.n.], 2007. **Anais ...**

DRJ (Disaster Recovery Journal); DRI (Disaster Recovery Institute International). **Business continuity glossary**. St. Louis, MO, 2005.

DROGUETT, E. L.; MOSLEH, A. Methodology for the treatment of model uncertainty. In: INTERNATIONAL CONFERENCE ON PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT (PSAM), 5., Osaka. In: . [S.l.: s.n.], 2000. **Proceedings ...**

ECO, U. **Como se faz uma tese**. 12ª. ed. São Paulo: Editora Perspectiva, 1977.

ECSS (European Cooperation for Space Standardization). **ECSS-Q-30-02A**: Space product assurance – failure modes, effects and criticality analysis (fmeca). Noordwijk, The Netherlands, 2001.

EHLERS, R. S. **Introdução a inferência bayesiana**. Curitiba, 2005. Disponível em: <http://www.est.ufpr.br/˜paulojus/CE227/ce227.pdf>. Acesso em: 11 ago. 2004.

ELETROSUL. **MC/04/DJ/017**: Manual de manutenção preventiva em disjuntores à SF_6, 550kv, fabricação Merlin-Gerin, tipo FA4. Florianópolis, 2006.

ENERVAC CORPORATION. **Informações sobre o produto**: equipamento de tratamento de gás SF_6. [S.l.], 2004. Disponível em: <http://www.enervac.com/Portuguese/01.shtml>. Acesso em: 14 jul.2006.

EPA (Environmental Protection Agency). **Emission Reduction Partnership for Electric Power Systems**: 2003 annual report. [S.l.], 2003. 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.], 2006. Disponível em: <http://www.epa.gov/electricpower-sf6/resources/index.html>. Acesso em: 2 jun. 2008.

ERICSON II, C. A. Fault tree analysis: A history. in: International system safety conference, 17. In: . [S.l.: s.n.], 1999. **Proceedings ...**

ERICSON II, C. A. **Hazard analysis techniques for system safety**. New Jersey: John Wiley & Sons, Inc., 2005.

EUROCONTROL (European Organisation for the Safety of Air Navigation). **Review of techniques to support the EATMP safety assessment methodology**. [S.l.], 2004.

____. **SAM Electronic**. v.2.1. [S.l.], 2006. Disponível em: <Disponível em: <http://www.eurocontrol.int/safety/gallery/content/public% -/library/SAM-/SAM_Electronic_Self_Assessment.zip>. Acesso em: 03 abr. 2007.

EVERDIJ, M. H.; BLOM, H. A. **Safety methods database**. Version 0.7. [S.l.], 2008.

FAA (Federal Aviation Administration). **RVSM status world wide**. Washington, 2007. Disponível em: <http://www.faa.gov/about/office_org/headquarters_offices/ato/ service_units-/enroute/rvsm/status_ww/>. Acesso em: 19 nov. 2008.

FERREIRA, A. B. d. 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.

GARCIA, P. A. d. A. **Uma abordagem *fuzzy* com envelopamento dos dados da análise dos modos e efeitos de falha**. 78 p. Tese (Doutorado em Ciências em Engenharia Nuclear) — Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, 2006.

GILL, J. **Bayesian Methods**: A social and behavioral sciences approach. London: Chapman & Hall/CRC, 2002.

GLENN, J. What is business continuity planning? How does it differ from disaster recovery planning? **Disaster Recovery Journal**, DRJ, St. Louis, MO, v. 15 (Issue 1), 2005.

GOVERNORS. **BowTieXp training guide**. v.2.0.1. [S.l.], 2005. Disponível em: <www-.bowtiexp.com>. Acesso em: 08 set. 2007.

GOWLAND, R. 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**, Elsevier, v. 130, p. 307 – 310, 2006.

HAMMER, W.; PRICE, D. **Occupational safety management and engineering**. 5ª. ed. Upper Saddle River, New Jersey: Prentice Hall, 2001. 603 p.

HEINRICH, H. W. **Industrial accident prevention**. 4ª. ed. New York: McGraw-Hill, 1959.

HENG, G. M. Developing a suitable business continuity planning methodology. **Infor mation management & computer security**, MCB University Press Limit, v. 4, n. 2, 1996. ISSN 0968-5227.

HOLTON, G. A. Perspectives:: defining risk. **Financial analysts journal**, CFA Institute, Charlottesville, VA, v. 97, n. 6, p. 0001 – 0011, 2004.

IAEA (International Atomic Energy Agency). **75-INSAG-3**: Basic safety principles for nuclear power plants. Rev. 1. Vienna, Austria, 1999.

____. **Safety Reports Series No. 25**: Review of probabilistic safety assessments by regulatory bodies. Vienna, Austria, 2002.

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. In: . [S.l.: s.n.], 2007. p. 354–360. **Proceedings ...**

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.

IMO (International Maritime Organization). **MSC/Circ.1023, MEPC/Circ.392**: Guidelines for formal safety assessment (fsa) for use in the imo rule-making process. London, 2002.

JENSEN, F. V. **Reliability in engineering design**. New York: Springer-Verlag, 2001.

KAPUR, K. C.; LAMBERSON, L. R. **Reliability in engineering design**. New York: John Wiley & Sons, Inc., 1977.

KARAKASIDIS, K. A project planning process for business continuity. **Industrial management & data systems**, MCB University Press Limit, v. 97, n. 8, 1997. ISSN 0263-5577.

KELLER, W.; MODARRES, M. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. **Reliability engineering and system safety**, Elsevier, Northern Ireland, v. 89, p. 271 – 285, 1998.

KIRCHSTEIGER, C. On the use of probabilistic and deterministic methods in risk analysis. **Journal of loss prevention in the process industries**, v. 12, n. 5, p. 339 – 419, 1999. ISSN 0950-4230.

KRANIDIOTIS, T. Risk assessment methodology. In: INTERNATIONAL SYSTEM SAFETY CONFERENCE (ISSC), 19., Huntsville, Alabama. In: . [S.l.]: System Safety Society's, 2001. **Proceedings ...**

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.

LEAVELL, H.; CLARK, E. G. **Medicina preventiva**. São Paulo: McGraw-Hill, 1976.

LEDERMAN F. NIEHAUS, B. T. L. Probabilistic safety assessment past, present and future: An iaea perspective. **Nuclear Engineering and Design**, Elsevier, Northern Ireland, v. 160, p. 273 – 285, 1996.

LEE, B. Using Bayes belief networks in industrial FMEA modeling and analysis. In: ANNUAL RELIABILITY AND MAINTAINABILITY SYMPOSIUM, Philadelphia, PA. In: . [S.l.: s.n.], 2000. **Proceedings ...**

LEFEVRE, M. A. P.; JIMENEZ, R. D.; BIANCHI, P. R. Managing risks: The ITAIPU Binacional experience. In: WATERPOWER, XII., Salt Lake City, Utah. In: . [S.l.]: HCI Publications, 2001. **Proceedings ...**

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 ...**

LEME, R. A. S. **Controle na produção**. São Paulo: Empresa gráfica da Revista dos tribunais, 1967.

LEVESON, N. **Safeware**: system safety and computers. New York: Addison-Wesley, 1995. 704 p. ISBN 0201119722.

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.

LIMA, F. d. P. A. **Contribuição à análise da insegurança no trabalho e ao projeto de máquinas mais seguras**. Dissertação (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 1985.

MAURINO, D. E. et al. **Beyond aviation huma factors**: safety in high technology systems. Aldershot, England: Ashgate Publishing Limited, 1995.

MORAND DEVILLER, J. O sistema pericial: Perícia científica e gestão do meio ambiente. In: ____. **Governo dos riscos**. Brasília: Gráfica Editora Pallotti, 2005.

MOSLEH, A.; DIAS, A. **Towards an integrated methodology for identification, classification, and assessment of aviation systems hazards**. [S.l.], 2004. Final Report. Center for Technology Risk – Studies.

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 ...**

NASA (National Aeronautics and Space Administration). **NASA-STD-8719.13A**: Software safety. Washington, 1997.

____. **Fault tree handbook with aerospace application**. Version 1.1. Washington, 2002.

____. **Probabilistic risk assessment procedures guide for NASA managers and practitioners**. Washington, 2002.

____. **NASA-NPR 8000.4**: Risk management procedural requirements. Change 1. Washington, 2004.

____. **NASA-NPR 8715.3**: NASA Safety manual. Washington, 2004.

____. **NASA-NPR 7120.5**: Program and project management processes and requirements. Washington, 2005.

NIST (National Institute of Standards and Technology). **FIPS PUBS 183**: Integration definition for function modeling (IDEF0). Gaithersburg, MD, 1993. Draft Federal Information Processing Standards Publication.

NIST (National Institute of Standards and Technology). SEMATECH (Semiconductor Manufacturing Technology). **e-Handbook of statistical methods**: assessing product reliability. [S.l.], 2003. Disponível em: <http://www.itl.nist.gov/div898/handbook% -/toolaids/pff/index.htm>. Acesso em: 10 ago. 2004.

GEEST, P. et al. (Ed.). **NLR-CR-2003-316**: Aviation safety management in Switzerland – Recovering from the myth of perfection. [S.l.], 2003.

O'CONNOR, J. J.; ROBERTSON, E. F. Thomas bayes. **MacTutor History of Mathematics**, June 2004. Disponível em: <http://www-groups.dcs.st-and.ac.uk/˜history/Printonly/Bayes-.html>. Acesso em: 18 de set. 2005.

PAPAZOGLOU, I. A. Mathematical foundations of event tree. **Reliability engineering and system safety**, Elsevier, Northern Ireland, v. 61 (Issue 3), p. 169 – 183, 1998.

PARADIES, M.; UNGER, L. **TapRoot**: the system for root cause analysis, problem investigation, and proactive improvement. Knoxville,Tennessee: System Improvements, Inc., 2000.

PEARL, J. **Probabilistic reasoning in intelligent systems**: networks of plausible inference. revised second printing. San Mateo, USA: MorganKaufmann Publishers Inc., 1988.

PHILLEY, J. Collar hazard with bow-tie. **Chemical Processing**, PutmanMedia, Itasca, IL, January 2006. Disponível em: <http://www.chemicalprocessing.com/articles/2005/612.html>. Acesso em: 1 out. 2008.

PMI (Project Management Institute). **PMBOK guide**: A guide to the project management body of knowledge. Newtown Square, PA, 2000.

____. **PMBOK guide**: A guide to the project management body of knowledge. Newtown Square, PA, 2004.

PRESLEY, A. R. **A representation method to support enterprise engineering**. Tese (Doctor of Philosophy) — Faculty of the Graduate School of University of Texas at Arlington, Arlington, 1997.

RAC (Reliability Analysis Center). Use of bayesian techniques for reliability. **Start – Selected Topics in Assurance Relates Technologies**, RAC, v. 10, n. 8, 2003.

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.

RICHARDSON, R. J.; PERES, J. A. d. S. **Pesquisa social**: métodos e técnicas. 2ª. ed. São Paulo: Atlas, 1989. (Broch.). ISBN 852240450X.

RODRIGUES FILHO, J. G.; BARZ, E. Solubilidade do ar em SF_6 fase líquida versus temperatura, e sua aplicação para purificação do SF_6. In SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA (SNPTEE), XVIII., Curitiba. In: . [S.l.: s.n.], 2005. **Anais ...**

SAE (Society of Automotive Engineers). **ARP 4761**: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. [S.l.], 1996.

____. **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.

SALDANHA, F. **Introdução a planos de continuidade e contingência operacional**. Edição revisada. Rio de Janeiro: Papel Virtual Editora, 2000.

SANTOS, V.; CANDELORO, R. J. **Trabalhos Acadêmicos**. Porto Alegre: Age, 2006.

SAVAGE, M. Business continuity planning. **Work study**, MCB University Press Limit, v. 51, n. 5, 2002. ISSN 0043-8022.

SILVA, P. A confiabilidade e a avaliação de segurança no projeto de aeronaves. In: SIMPÓSIO INTERNACIONAL DE CONFIABILIDADE SALVADOR (SIC), Salvador. In: . [S.l.: s.n.], 2006. **Anais ...**

SKJONG, R. Setting target reliabilities by marginal safety returns. In: JCSS WORKSHOP ON RELIABILITY BASED CODE CALIBRATION, Zurich. In: . [S.l.: s.n.], 2002. **Proceedings ...**

SMITH, A. M. **Reliability-centered maintenance**. Boston, MA: Mc Graw Hill, 2001.

SMITH, D. **Reliability, maintainability and risk**: pratical methods for engineers. Amsterdam: Butterworth Heinemann, 2001. ISBN 0 7506 5168.

SOUZA, G. C.; TENORIO, M. B.; NASSAR, S. M. Fatores motivadores para funcionários públicos e privados. In: IT CONFERENCE SUCESU-MT, Cuiabá. In: . [s.n.], 2002. **Anais ...** Disponível em: <www.inf.ufsc.br/˜silvia/disciplinas/sep/artigo01.pdf>. Acesso em: 10 ago. 2004.

STAMATELATOS, M. G. Probabilistic risk assessment: NASA strategy for capability enhancement. In: NASA PRA PRACTICES AND NEEDS INTO THE NEW MILLENNIUM, Washington. In: . [S.l.: s.n.], 2000. **Proceedings ...**

STAMATIS, D. H. **Failure mode and effects analysis**: FMEA from theory to execution. 7. ed. Milwaukee: ASQC Quality Press, 1995.

SWAMINATHAN, S.; SMIDTS, C. The mathematical formulation for the event sequence diagram framework. **Reliability engineering and system safety**, Elsevier, v. 65, p. 103 – 118, 1999.

THE american heritage dictionary. 4. ed. Boston: Houghton Mifflin, 2000. ISBN 0395339596.

THIOLLENT, M. **Metodologia da pesquisa-ação**. 7. ed. São Paulo: Cortez, 1996. 108 p. (Broch.). ISBN 8524900296.

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 ...**

UFSC (Universidade Federal de Santa Catarina). NEDIP (Núcleo de Desenvolvimento Integrado de Produtos). **MT-DJ-RT-NE-0**: FMEA dos disjuntores família FA. Revisão 3. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-DJ-RT-NE-01**: Relação e seleção dos disjuntores da Eletrosul para estudo no projeto MitiSF6. Revisão 2. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-DJ-RT-NE-03**: Análise funcional do disjuntor. Revisão 4. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-DJ-RT-NE-05**: Recomendações. Revisão 1. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-DS-AP-NE-2008-12-17**: Apresentação do relatório final. Florianópolis, 2008. Apresentação final do projeto MitiSF6.

____. **MT-GE-RT-NE-01**: Instituições e empresas de referência no manuseio, tratamento e normatização relativo ao gás SF_6. Revisão 2. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-GE-RT-NE-04**: Indicadores de consumo de SF_6 na Eletrosul. Revisão 2. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-GE-RT-NE-05**: Análise da base de dados de ações de manutenção da Eletrosul. Revisão 1. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-MP-RT-NE-01**: QFD da metodologia. Revisão 1. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-PR-RT-NE-01**: IDEF0 dos processos relacionados à manipulação do SF_6. Revisão 4. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-PR-RT-NE-02**: Procedimentos para manipulação do SF_6 utilizando a máquina da Cryoquip. Revisão 1. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-PR-RT-NE-03**: FMEA dos processos de manipulação de SF_6 na Eletrosul. Revisão 5. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-PR-RT-NE-04**: Sugestão de estrutura mínima necessária para dar suporte aos processos relativos à manipulação do SF_6. Revisão 2. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **MT-PR-RT-NE-05**: Recomendações para os processos relativos à manipulação do SF_6. Revisão 2. Florianópolis, 2008. Relatório do projeto MitiSF6.

____. **NE-RE-06**: Abordagem bayesiana. Revisão 1. Florianópolis, jun. 2008. Resumo de técnicas.

UNIÃO EUROPEIA. Regulamento (CE) N° 842/2006 do Parlamento Europeu e do Conselho de 17 de Maio de 2006: relativo a determinados gases fluorados com efeito de estufa. **Jornal Oficial da União Europeia**, n. L161, p. 0001 – 0011, 2006. Disponível em: <http://eur-lex-.europa.eu/LexUriServ/LexUriServ.do?uri =OJ:L:2006:161:0001:0011:PT:PDF>. Acesso em: 8 jan. 2009.

____. 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 recuperação 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 2007**: The physical science basis. Cambridge, 2007. Disponível em: <http://www.ipcc.ch/ipccreports/ar4-wg1.htm>. Acesso em: 2 jun. 2008.

UNO (United Nations Organization). UNFCCC (United Nations Framework Convention on Climate Change). **The Kyoto Protocol**. Kyoto, Japan, 1998. Disponível 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.

____. **MIL-HDBK-881**: Work breakdown structure. Washington, 1998.

USA (United States of America). NRC (Nuclear Regulatory Commission). **NUREG 0492**: Fault tree handbook. Washington, 1981.

WANE, S. Risky business. **Public Sector Forums**, August 2005. Disponível em: <http://www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Risk/Business-continuity/Risky-business/>. Acesso em: 23 out. 2008.

WANG, J. The current status and future aspects in formal ship safety assessment. **Safety science**, Elsevier, Northern Ireland, v. 38, p. 19 – 30, 2001.

WEICHSELGARTNER, J. Disaster mitigation: the concept of vulnerability revisited. **Disaster prevention and management**, MCB University Press, v. 10, n. 2, 2001. ISSN 0965-3562.

XU, K. et al. Fuzzy assessment of FMEA for engine systems. **Reliability engineering and system safety**, Elsevier, v. 75, p. 17 – 29, 2002.

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 (THE..., 2000), que sevem para criar uma realidade visual (FERREIRA, 1988).

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. Existem dois erros associados a avaliação da incerteza do risco: (1) erro quanto a determinação do efeito; e (2) erro na determinação da probabilidade de ocorrência. Por exemplo: na avaliação de um acidente, não se tem como garantir o 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.

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 (SAE, 2002) .

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 (ABNT, 2005).

Perfil do risco (*Risk profile*): É o vetor (L_i, O_i, U_i, CS_i, PO_i), onde O_i é o resultado; L_i é a chance do resultado ocorrer; U_i é utilidade; CS_i é o cenário causal; e PO_i é a população afetada (KUMAMOTO; HENLEY, 1996).

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 $P(Estado\ futuro\ \text{“}x\text{”} \mid Estado\ inicial)$ –, 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 (2005) exclui da transferência estratégias de reposicionamento de uma fonte de risco (como na terceirização).

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" (SOUZA et al., 2002).

APÊNDICE A – Ferramenta computacional OpenFMECA

Está sendo elaborado, no Núcleo de Desenvolvimento Integrado de Produtos da Universidade Federal de Santa Catarina (NeDIP / EMC / UFSC), desde outubro de 2006, um *software* com código fonte aberto (*open source*) para auxiliar no uso da técnica FMECA, chamado OpenFMECA[1].

A FMECA é uma técnica analítica que tem como propósito identificar, priorizar e eliminar falhas potenciais de um sistema, projeto e/ou processo antes que estas atinjam o usuário final. Ela teve sua origem no departamento de defesa dos Estados Unidos (DOD – Department of Defense), em 1949, com a norma militar MIL-P-1629A (*Military procedure* MIL-P-1629A: *procedures for performing a failure mode, effects and criticality analysis*). A FMECA distingue-se da FMEA (*failure modes effects and analysis*) pelo fato de agregar um índice de criticidade que orienta a prioridade nas ações a serem executadas pela organização. Após ter identificado os modos de falha potenciais, com suas causas e efeitos, associa-se a estes modos de falha um índice de risco ou nível de criticidade. A partir da priorização destes índices, ações corretivas são definidas e implementadas.

A elaboração de *software* com código fonte aberto (*software* livre) é uma das diretrizes do governo federal, corroborada pela maioria dos estados brasileiros[2]. Este projeto está em consonância com essa tendência e pretende deflagrar um programa, dentro do NeDIP, de desenvolvimento de *software* livre relacionado às técnicas mais importantes na área de projeto mecânico – neste caso a FMECA.

As duas primeiras versões do *software* foram feitas com o objetivo de dar suporte à utilização desta técnica[3]. No entanto, apesar de bastante consolidada, a FMECA possui alguns

[1] O texto apresentado neste apêndice foi elaborado pela equipe do projeto OpenFMECA, que é coordenado pelo Professor Acires Dias. Fazem parte da equipe (ou fizeram): Luís Fernando Peres Calil; Eduardo Yuji Sakurada; Heitor Azuma Kagueiama; Leonardo Mecabô; Daniel Koudi Nakano; Glauco Vinicius Gil Peron; André Ogliari; Emerson Rigoni; Gleber Estefani Diniz; e Thiago Nass de Holanda.

[2] Vide <http://www.softwarelivre.gov.br/>.

[3] A segunda versão do *software* foi uma reimplementação, objetivando melhorar a rapidez e o projeto gráfico.

inconvenientes, destacadamente: a dificuldade de conciliar a técnica com o tratamento estatístico das informações, a limitação da representação na forma de tabela e o tempo consumido em reuniões. A fim de mitigar estes inconvenientes – destacadamente os dois primeiros pontos –, foi proposta a estrutura de trabalho que associa a FMECA a outras técnicas.

Neste sentido, na versão em desenvolvimento do *software* OpenFMECA (versão α.3), pretende-se aprimorar a ferramenta computacional para que ela atenda a esta estrutura. Para tanto, o *software* está sendo totalmente reestruturado. Atualmente, estão sendo geradas as especificações técnicas do *software*, que consistem no levantamento das necessidades dos clientes (usuários e desenvolvedores); na definição de escopo; na definição do comportamento do *software* e na estrutura da base de dados, usando UML; etc. Também está sendo elaborado o planejamento da implementação, no qual se prevê a disponibilização do *software* no sítio SourceForge[4].

Também está sendo revisada a política de restrições dos usuários, a fim de minimizar o tempo em reuniões (o terceiro inconveniente citado). O *software* pode ser instalado em um servidor e ser acessado remotamente por um navegador de internet (*browser*). Isto possibilita que a FMECA seja preenchida sem a necessidade da presença de todos os membros da equipe reunidos no mesmo local. No entanto, se não existir uma política de restrições bem definida, pode-se perder o controle do desenvolvimento da FMECA.

Na próxima seção, serão apresentados os objetivos para o desenvolvimento do OpenFMECA, e, posteriormente, será feita uma breve apresentação da versão α.1 do *software* – que foi utilizada no projeto MitiSF6 com a Eletrosul.

A.1 Objetivos

O objetivo deste *software* é ser uma ferramenta para auxiliar no uso da estrutura de trabalho (*framework*) para gerenciamento de falha / incidente desenvolvida no NeDIP / EMC / UFSC, que é baseada nas técnicas FMECA / CNEA. Este *software* deve permitir que a FMECA seja (parcialmente ou totalmente) desenvolvida remotamente, a fim de reduzir o tempo dispendido em reuniões. Adicionalmente, prevê-se a inclusão de outras técnicas para suprir algumas carências da FMECA / CNEA, a saber: IDEF0, redes bayesianas e FTA – conforme apresentado a seguir.

[4] <http://sourceforge.net/>.

A.1.1 Ferramenta colaborativa

O OpenFMECA está sendo desenvolvido para ser instalado em um servidor e utilizado via navegador de internet de qualquer local (desde que tenha conexão com a internet) ou qualquer sistema computacional (PCs, *palmtops*, etc). Com isto, pode-se elaborar a FMECA de forma distribuída, na qual mais de uma pessoa pode trabalhar na mesma FMECA, em postos de trabalho diferentes. Nesta condição, o OpenFMECA passa a ser utilizado como uma ferramenta colaborativa, permitindo que se faça a análise de maneira não presencial, eliminando – ou, pelo menos, minimizando – a necessidade das reuniões.

A.1.2 FMECA estruturado

O módulo do *software* para FMECA estruturado foi desenvolvido nas versões anteriores do *software* e consiste na elaboração da análise em uma estrutura de árvore, na qual se desdobra o sistema até a resolução desejada e, posteriormente, analisam-se os potenciais modos de falha.

A.1.3 FMECA / CNEA

Verificou-se, nas aplicações da estrutura FMECA / CNEA, que a representação gráfica, mostrando o encadeamento de cada cenário, é fundamental na análise dos modos de falha.

O módulo de CNEA possibilitará que a análise dos modos de falha seja feita graficamente, sendo possível a exportação de relatórios na forma da tradicional tabela FMECA.

A.1.4 CNEA / Bayesiano

A técnica CNEA não possibilita fazer tratamento estatístico. Assim, será feita a associação de redes bayesianas com a CNEA – por meio de tabelas de correlações – para suprir esta necessidade.

A.1.5 IDEF0

Em muitos casos, a FMECA é baseada no desdobramento funcional realizado utilizando a técnica IDEF0. Assim, neste módulo, será possível elaborar diagramas IDEF0 básicos, que também serão apresentados no módulo FMECA estruturado, na forma de desdobramento do sistema em análise.

A.1.6 FTA

A FTA é uma forma gráfica de representar a relação entre as falhas fazendo uso de portas lógicas (E, OU, etc). Com este módulo, será possível elaborar análise por árvore de falhas de barreiras ou de causas que se pretendem detalhar melhor.

A.2 Apresentação da versão α.1

A estrutura de tabelas e informações relativas à FMECA, utilizada neste *software*, foi baseada nas recomendações apresentadas na SAE J1739[5].

A tela de abertura (*Home*) do *software* – ilustrada na Figura A.1 – está dividida em 3 seções: apresentação; sistemas; e configurações.

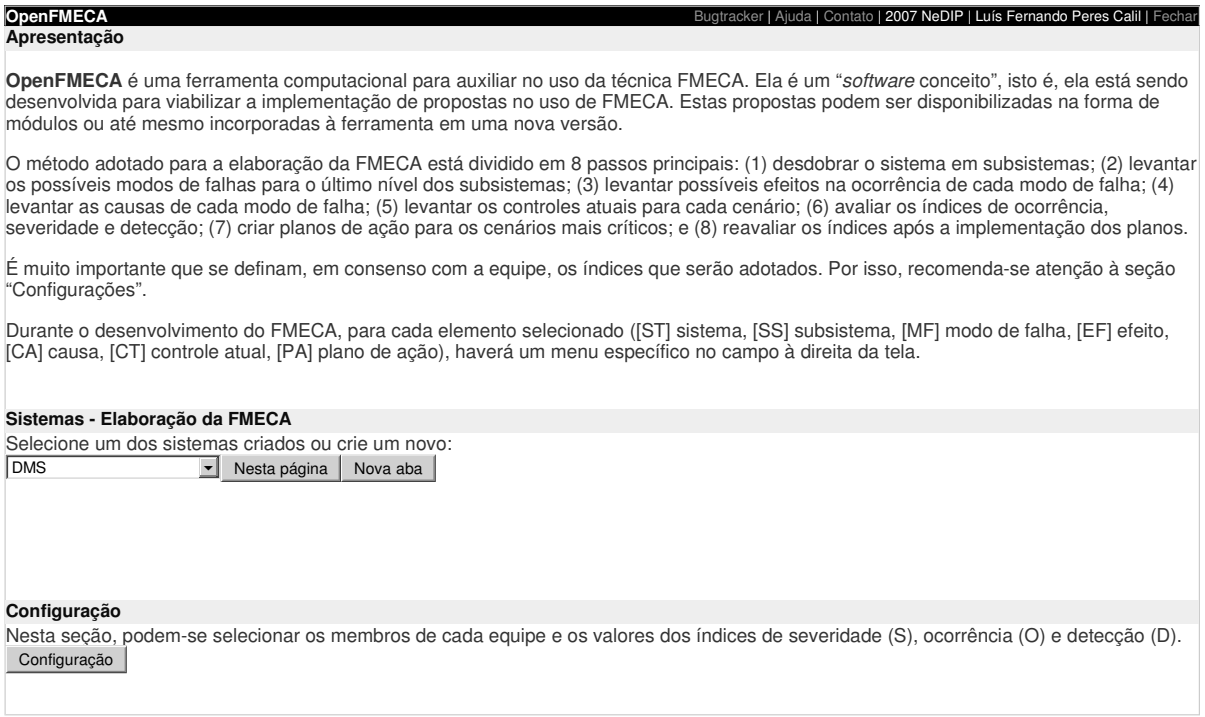


Figura A.1: Tela de apresentação do OpenFMECA

Na seção "Configuração", podem-se gerenciar os sistemas cadastrados no OpenFMECA, conforme ilustrado na Figura A.2.

Observe-se que é possível excluir um sistema pela opção "deletar" (opção restrita ao mode-

[5]Destaca-se que a SAE J1739 distingue 3 tipos de FMECA (de projeto, de processo e de maquinários), que no *software* foram simplificadas para que se elaborasse apenas uma estrutura. Assim, o *software* não cumpre, integralmente, a recomendações, mas se baseia nelas.

Figura A.2: Tela de cadastro de sistemas, nas "configurações"

rador do sistema), no entanto, este sistema é simplesmente transferido para uma "lixeira", onde se pode recuperá-lo sem perda de informação – somente o administrador do OpenFMECA tem poder para excluir definitivamente um sistema.

Na seção de configurações, pode-se, ainda, fazer a seleção das pessoas que farão parte da equipe de cada FMECA, ilustrado na Figura A.2.

Caso se deseje cadastrar um novo participante das FMECAs, pode-se fazê-lo acionando o botão "Cadastrar Pessoa", ilustrado na Figura A.4.

Adicionalmente, podem-se alterar os limites dos índice de severidade(S), ocorrência(O) e dificuldade de detecção (D), a fim de dar mais peso a um determinado atributo, por exemplo: severidade variando até 20, ocorrência até 10 e detecção até 5 – o que resulta em um peso relativo de 4 para 2 para 1, respectivamente.

Na seção "Sistemas – Elaboração da FMECA", é feita a seleção do sistema que se deseja analisar, ou criação de um novo sistema. Uma vez selecionado, pode-se abrir a FMECA do sistema na mesma ou em uma nova aba do navegador – a Figura A.5 ilustra a tela da FMECA do Departamento de Manutenção do Sistema da Eletrosul (DMS).

O primeiro passo da análise dos modos de falha – no OpenFMECA – é o desdobramento do sistema em subsistemas até a resolução desejada. Para tanto, utiliza-se a opção "novo sub-

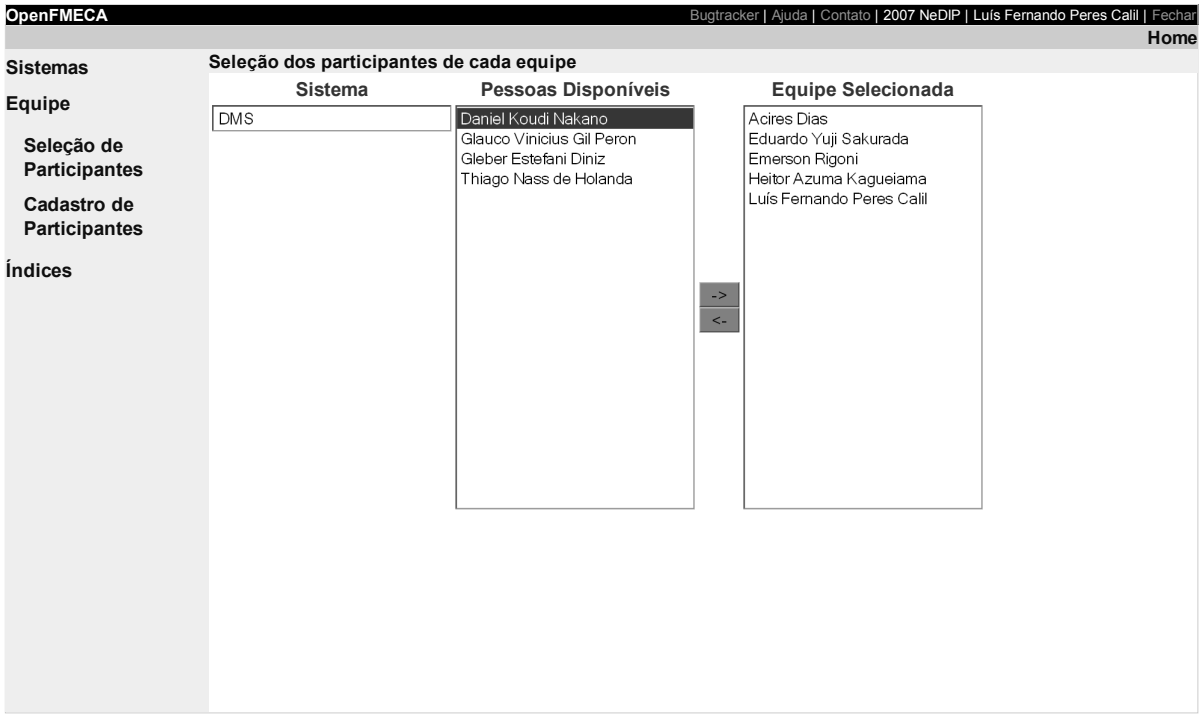


Figura A.3: Tela de seleção de participante, nas "configurações"

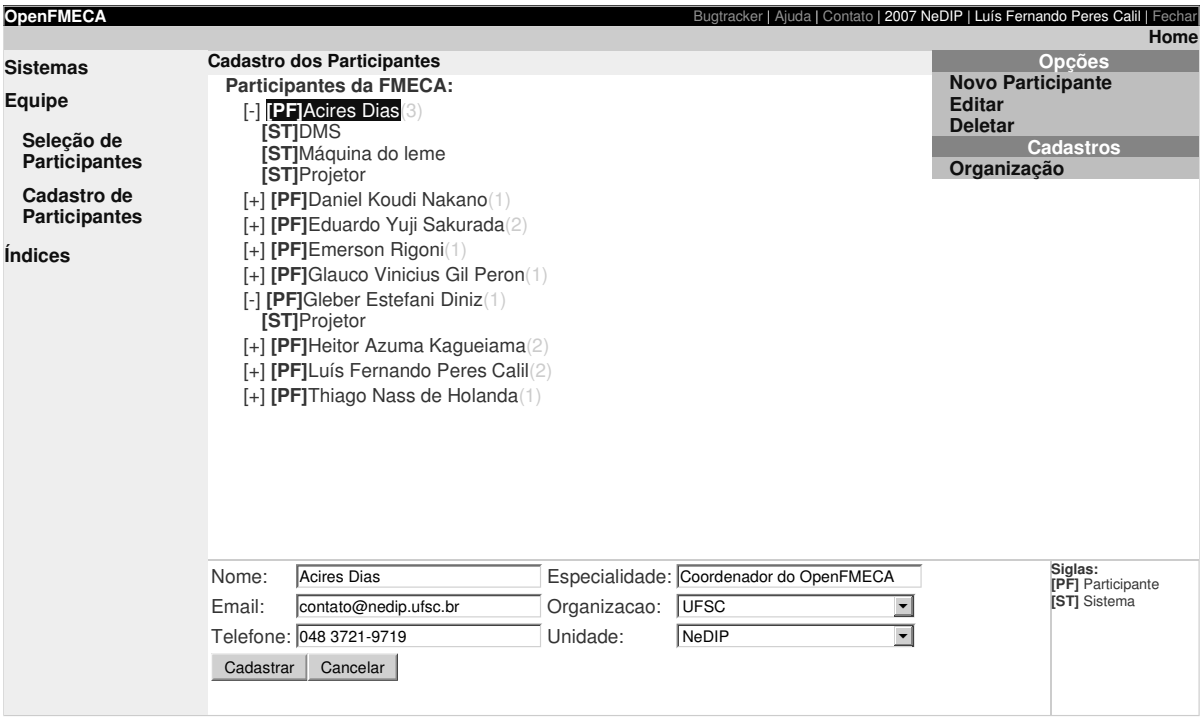


Figura A.4: Tela de cadastro de participante, nas "configurações"

sistema" na barra lateral direita. Podem-se, então, incluir os possíveis modos de falha (MF) dos subsistemas que estão no último nível do desdobramento. Desta forma, a FMECA é elaborada

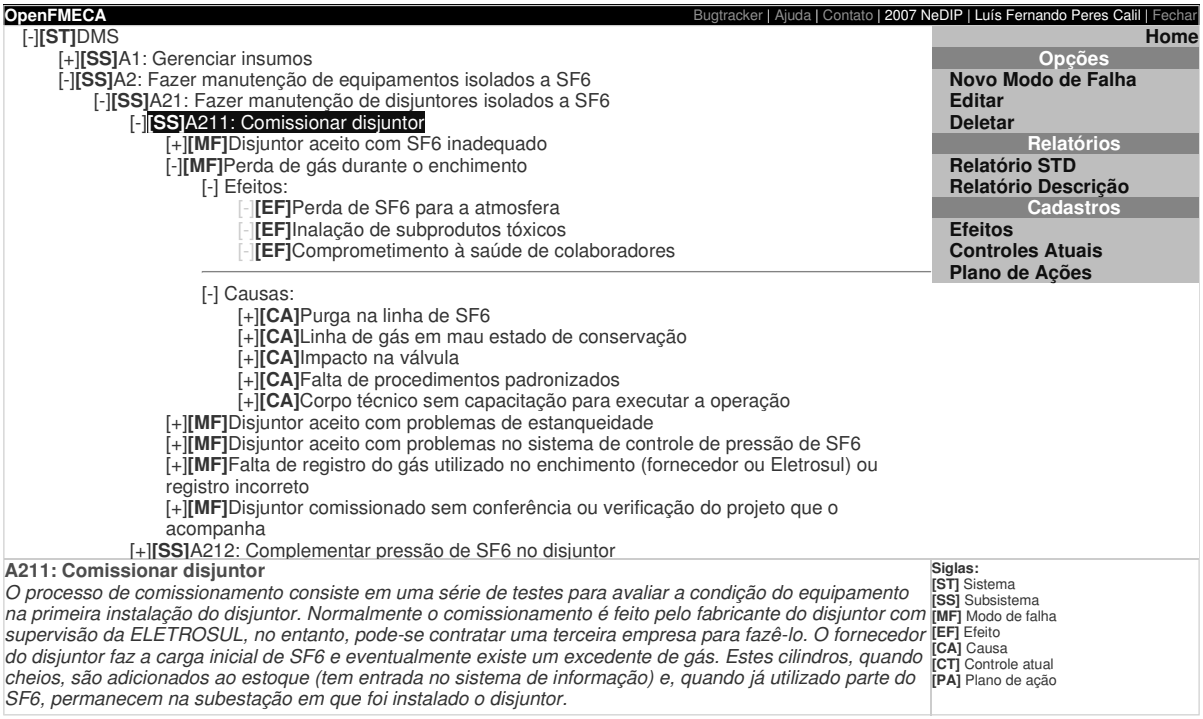


Figura A.5: Tela de elaboração da FMECA do DMS

no formato de árvore, o que melhora a visualização e o entendimento.

O passo seguinte é a inclusão dos possíveis efeitos e causas de cada modo de falha para cada subsistema – e, posteriormente, dos controles atuais e ações propostas (plano de ações).

Observe-se que as opções apresentadas na barra lateral são adaptadas ao contexto. Quando selecionado um sistema (ou subsistema) que já tenha um modo de falha cadastrado, por exemplo, exibem-se opções "novo modo de falha", "editar" e "deletar"; também, podem-se gerar "relatórios STD (*standard*)" e "relatórios de descrição"; e podem-se editar os cadastros de "efeitos", de "controles atuais" e de "plano de ações" – conforme ilustrado na Figura A.5. O Quadro A.1 indica os itens na barra lateral disponíveis para diferentes elementos da FMECA selecionados.

O passo seguinte é a determinação dos índices que irão compor a criticidade. Para tanto, seleciona-se a opção "avaliar índices" na barra lateral – vide Quadro A.1, item selecionado: Modo de falha – e uma nova aba abrirá com campos para serem preenchidos com as estimativas dos índices, conforme ilustrado na Figura A.6.

Assim que os índices de severidade, ocorrência e de detecção forem inseridos, o *software* apresentará o valor do NPR (número de prioridade de risco, que é o produto dos índices S, O e D).

Quadro A.1: Conteúdo da barra lateral direita para diferentes elementos da FMECA selecionados

Item selecionado	Conteúdo da barra lateral direita
Nenhum item selecionado	**Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Sistema raiz sem subsistema ou modo de falha	**Opções:** Novo subsistema, Novo modo de falha, Editar. **Relatório:** Relatório descrição, Relatório STD. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Sistema raiz com subsistema	**Opções:** Novo subsistema, Editar. **Relatório:** Relatório descrição, Relatório STD. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Sistema raiz com modo de falha	**Opções:** Novo modo de falha, Editar. **Relatório:** Relatório descrição, Relatório STD. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Sistema sem subsistema ou modo de falha	**Opções:** Novo subsistema, Novo modo de falha, Editar, Deletar. **Relatório:** Relatório descrição, Relatório STD. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Sistema com subsistema	**Opções:** Novo subsistema, Editar, Deletar. **Relatório:** Relatório descrição, Relatório STD. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Sistema com modo de falha	**Opções:** Novo modo de falha, Editar, Deletar. **Relatório:** Relatório descrição, Relatório STD. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Modo de falha	**Opções:** Novo efeito, Nova causa, Editar, Deletar. **Índices:** Avaliar, Reavaliar. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Efeito	**Opções:** Editar, Deletar. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Causa	**Opções:** Novo controle atual, Nova ação, Editar, Deletar. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Controles Atuais	**Opções:** Editar, Deletar. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.
Ações propostas	**Opções:** Editar, Deletar. **Cadastros:** Efeitos, Controles Atuais, Plano de Ações.

Podem-se, então, incluir as ações que deverão ser tomadas para a redução do NPR. Na opção "nova ações", disponível quando se seleciona uma causa, podem-se inserir, além da descrição da ação, o responsável, a data limite para a execução e a estimativa de custo.

Por fim, pode-se rever a estimativa dos valores dos índices após a implementação das ações na opção "reavaliar índices" – vide Figura A.7.

Adicionalmente, pode-se gerenciar o cadastro de efeitos, controles atuais e ações. Esses elementos da FMECA devem ser cadastrados no *software* para serem atribuídos a um determi-

DMS > A2: Fazer manutenção de equipamentos isolados a SF6 > A21: Fazer manutenção de disjuntores isolados a SF6 > A211: Comissionar disjuntor						
Perda de gás durante o enchimento: *Perda de SF6 decorrente do processo de enchimento, tais como: vazamento na válvula do cilindro, purga da mangueira, falta de vedação no engate rápido, etc.*						
Efeitos	**S**	**Causas**	**O**	**Controles Atuais**	**D**	**NPR**
-Perda de SF6 para a atmosfera -Inalação de subprodutos tóxicos -Comprometimento à saúde de colaboradores	--	Purga na linha de SF6	--		--	0
		Linha de gás em mau estado de conservação	--		--	0
		Impacto na válvula	--		--	0
		Falta de procedimentos padronizados	--	-Elaboração e verificação de procedimentos para o enchimento de gás e capacitação do corpo técnico	--	0
		Corpo técnico sem capacitação para executar a operação	--	-Elaboração e verificação de procedimentos para o enchimento de gás e capacitação do corpo técnico	--	0

Figura A.6: Tela de uma avaliação de índices

nado modo de falha. Assim, nestas seções, podem-se criar novos efeitos e excluir, substituir ou modificar efeitos existentes.

Quanto aos relatórios, a versão $\alpha.1$ disponibiliza a tabela STD[6] – que é a usual da FMECA, baseada na estrutura apresentada na SAE J1739 – e o relatório descritivo de cada elemento que compõe a FMECA.

A.2.1 Concepção do *software*

O paradigma adotado foi o orientado a objeto, o que simplificou o código comparando-o com um paradigma estrutural, e, como modelo do ciclo de vida do *software*, adotou-se o incremental.

Em virtude da decisão de utilizar um *browser* como interface, optou-se pelo uso de PHP[7], JavaScript e MySQL para programá-lo, o que permite que ele seja multiplataforma – possível de ser implementado em Windows, Linux e outros sistemas operacionais. Outra decisão impor-

[6] STD, do inglês *standard*.

[7] Acrônimo para *hypertext preprocessor*. É uma linguagem de programação dinâmica interpretada, muito utilizada para programação na internet.

DMS > A2: Fazer manutenção de equipamentos isolados a SF6 > A21: Fazer manutenção de disjuntores isolados a SF6 > A211: Comissionar disjuntor

Perda de gás durante o enchimento:
Perda de SF6 decorrente do processo de enchimento, tais como: vazamento na válvula do cilindro, purga da mangueira, falta de vedação no engate rápido, etc.

Efeitos	S	Causas	O	Controles Atuais	D	NPR	Plano de Ações	Índices após ações			
								S	O	D	NPR
-Perda de SF6 para a atmosfera -Inalação de subprodutos tóxicos	0	Purga na linha de SF6	0		0	0	Aquisição de bombas de vácuo Fazer vácuo em substitição a purga Cuidados quanto a fonte de calor em operações passíveis de ocorrer vazamento (ex. cigarro)	--	--	--	0
		Linha de gás em mau estado de	0		0	0	Elaboração de procedimento para verificação da condição de válvulas e conexões Cuidados	--	--	--	0

Figura A.7: Parte da tela de uma reavaliação de índices, após ações

tante foi a escolha do navegador no qual o *software* está sendo desenvolvido, já que JavaScript tem problemas de compatibilidade entre navegadores de internet. Desta forma, optou-se pelo Mozilla Firefox, que também é *open source*.

Durante os primeiros meses, foram levantados os requisitos do sistema e proposta uma implementação. O processo de desenvolvimento do *software* foi executado utilizando-se uma versão simplificada do processo unificado (*unified process* – UP).

A documentação é baseada em diagramas UML[8], bem como em comentários ao longo do código. Os diagramas UML selecionados foram: (1) diagrama de classes; (2) diagrama de banco de dados; e (3) diagrama de interação, conforme ilustrado na Figura A.8.

O modelo de implementação escolhido foi o "em camadas". A mais próxima com o usuário foi denominada "Interface" e faz a conexão entre as requisições do usuário e o sistema. Também

[8]Foi utilizado o *software* Enterprise Architect para gerar a documentação UML.

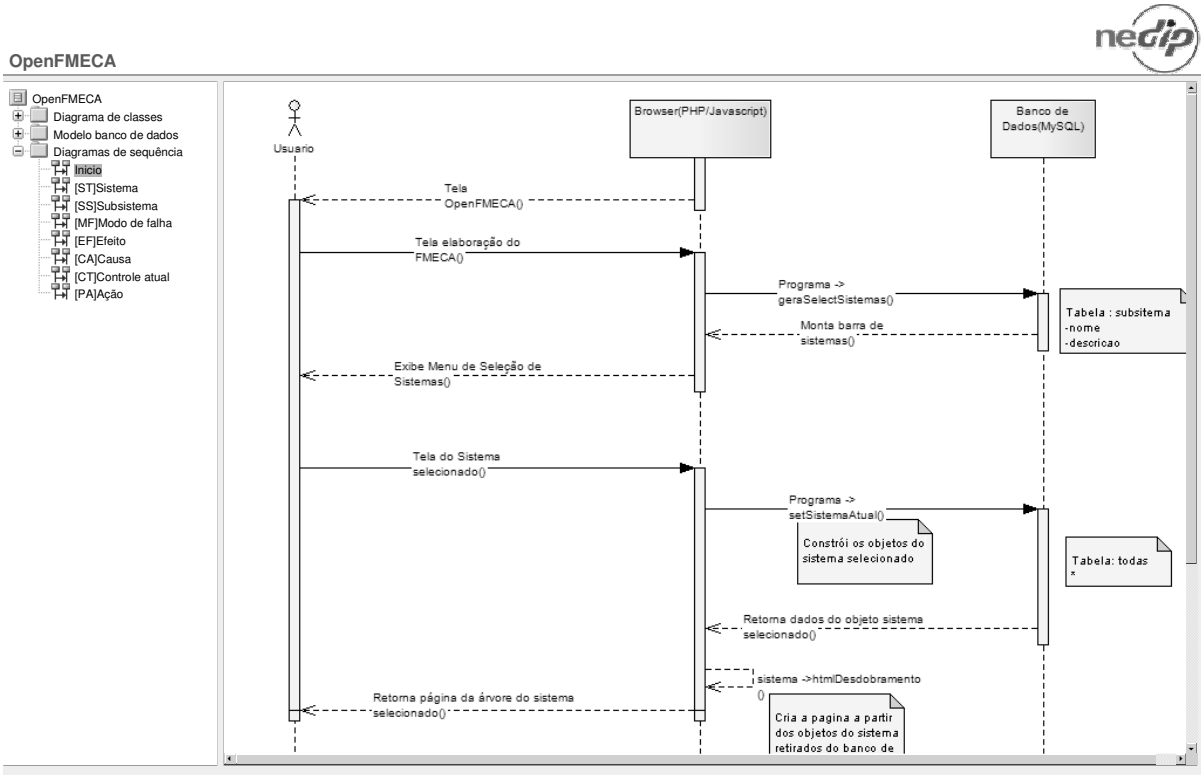


Figura A.8: Tela de um diagrama de sequência

faz a apresentação do sistema de maneira conveniente e intuitiva, gerando relatórios e páginas de visualização dos dados. A camada que contém o sistema foi denominada "Domínio". A última camada é o banco de dados .

Na camada Domínio, estão inseridas as regras e as estruturas de dados necessárias para representar a FMECA – optou-se por utilizar a linguagem PHP nesta camada.

Quanto à interface, foi escolhido o modelo de requisições de páginas "http[9]" utilizando-se solicitações assíncronas com JavaScript – destacadamente AJAX[10]. Esse modelo permite ao programador obter um maior controle sobre as ações do usuário no sistema do que no modelo tradicional. Isto também possibilita diminuir o tráfego de dados com o servidor, uma vez que apenas as informações novas são enviadas ao cliente. A linguagem JavaScript também foi escolhida para aprimorar a interface com o usuário do sistema, possibilitando respostas mais rápidas aos estímulos do usuário. Como biblioteca, optou-se pelo uso da XAJAX, que é uma biblioteca PHP, com código fonte aberto, para fazer aplicações *web* baseadas em AJAX.

As tabelas no banco de dados foram desenvolvidas para dar suporte ao modelo adotado.

[9] Acrônimo para *hypertext transfer protocol*, que significa protocolo de transferência de hipertexto.
[10] Acrônimo para *synchronous Javascript and XML.*

Esse modelo prevê a criação de uma tabela para cada classe de objeto. Para cada atributo de uma classe, uma coluna foi criada; para representar uma instância de uma classe, uma linha do banco.

A.2.2 Aspectos relevantes do *software*

Podem-se enumerar vários aspectos relevantes do OpenFMECA. Destaca-se, primeiramente, o fato de ele ser instalado em um servidor e ser utilizado via navegador de internet. Esta é uma tendência das ferramentas computacionais e traz uma série de benefícios, dentre eles:

- A possibilidade de se utilizar o *software* de qualquer sistema computacional (PCs, *palmtops*, etc.) ou sistema operacional (Windows, Linux, Mac OS, etc.) que tenha acesso à internet por meio de um *browser* – preferencialmente Mozilla Firefox .
- A possibilidade de elaborar a FMECA de forma distribuída, i.e, mais de uma pessoa trabalhando na mesma FMECA, em postos de trabalho diferentes, como uma ferramenta colaborativa. Neste sentido, pode-se pensar em fazer a FMECA de maneira não presencial, eliminando – ou, pelo menos, minimizando – a necessidade das reuniões.
- A utilização do *browser* como interface, o que diminui a curva de aprendizado do usuário, já que, usualmente, ele está familiarizado a este ambiente.
- A possibilidade de ser utilizado de qualquer local, sem a necessidade de instalação de *software* específico – não vinculando o trabalho a uma determinada máquina.

Adicionalmente, destaca-se o fato de o OpenFMECA ter seu código fonte aberto, o que permite que os usuários adaptem a ferramenta para as necessidades da organização em que ela está sendo implementada.

O *software* também traz uma abordagem diferente para a elaboração da FMECA. Ele propõe que a análise seja feita na forma de árvore. Isso permite melhor visualização da FMECA em relação à representação em forma de tabela, que, de acordo com Lee (2001), é fracamente estruturada e semanticamente pobre.

Por fim, destaca-se que o *software* possibilita melhor gestão do conhecimento, uma vez que, além do nome de cada elemento da FMECA (causa, efeito, modo de falha, etc.), também permite que se inclua um texto descritivo e, nas próximas versões, figuras ilustrativas.

REFERENCIAS DO APÊNDICE A

LEE, B. Using Bayes belief networks in industrial FMEA modeling and analysis. In: INTERNATIONAL SYMPOSIUM ON PRODUCT QUALITY AND INTEGRITY, Philadelphia, PA; 2001. **Proceedings...**

ANEXO A – Instrução para atendimento em estado de contingência

SISTEMA DE OPERAÇÃO E MANUTENÇÃO DA DISTRIBUIÇÃO

SUBSISTEMA PROCEDIMENTO E CONTROLE DA OPERAÇÃO DA DISTRIBUIÇÃO

CÓDIGO	TÍTULO	FOLHA
I-332.0027	ATENDIMENTO EM ESTADO DE CONTINGÊNCIA	1/13

1. FINALIDADE

Planejar, organizar e racionalizar os procedimentos de operação frente a uma condição de estado de contingência.

2. ÂMBITO DE APLICAÇÃO

Aplica-se à Diretoria Técnica - DTE e Agências Regionais.

3. ASPECTOS LEGAIS

a) Instruções Normativas da Celesc;

b) Norma Regulamentadora - NR 10.

4. CONCEITOS BÁSICOS

4.1. Tempestade Severa

Caracteriza-se pela agitação violenta da atmosfera, de abrangência e intensidade excepcionais, cuja conseqüência é no mínimo dezenas de quilômetros de sistema de distribuição avariado. As tempestades severas diferenciam-se das demais tempestades devido a sua abrangência e intensidade, pois geralmente vários bairros e municípios são fortemente atingidos. As tempestades severas ocasionam centenas de reclamações de falta de energia e dezenas de alimentadores desligados. São exemplos de tempestades severas: Furacão Catarina ocorrido em 31 de março de 2004, em Criciúma e demais municípios vizinhos e o Ciclone Extra Tropical ocorrido em 08 de agosto de 2005, em Florianópolis, Palhoça, São José e demais municípios litorâneos.

4.2. Adversidade Meteorológica

Caracteriza-se pela agitação discreta da atmosfera, sempre acompanhada de chuva, raio e vento, de abrangência e intensidade reduzida, cuja conseqüência é a avaria de partes isoladas do sistema de distribuição. As adversidades meteorológicas diferenciam-se das tempestades severas, devido à sua abrangência e intensidade, pois apenas alguns bairros são fortemente atingidos. As adversidades meteorológicas ocasionam dezenas de reclamações de falta de energia, assim como eventualmente alguns alimentadores desligados. São exemplos de adversidade meteorológica: tempestades de verão, vendavais isolados associados a frentes frias e ciclones extra tropicais moderados.

4.3. Estado de Contingência

Período correspondente ao intervalo desde a decretação do estado de contingência, até a decretação do retorno à condição normal de operação, tornando-se necessária, neste período, a aplicação desta Instrução Normativa. O estado de contingência aplica-se em dois níveis:

a) Nível I - quando há a necessidade de mobilização de todo o efetivo de atendimento da Agência Regional decretante do estado de contingência;

b) Nível II - quando, além da mobilização de todo o efetivo da Agência Regional, há necessidade de mobilizar equipes de atendimento de outras Agências Regionais.

4.4. Equipes Adicionais

São as equipes extras que estarão trabalhando em regime especial no estado de contingência, compostas por turmas de manutenção de emergência (Celesc), turmas de manutenção pesada (Celesc e empreiteiras) e equipes de atendimento comercial (Celesc), tanto da Agência Regional decretante, quanto de outras Agências Regionais. Após o fim do estado de contingência, estas equipes retornam às condições de origem.

4.5. Estação Adicional de Despacho

Estação adicional de despacho, composta por uma estação VHF (mesmo canal), uma máquina SIMO e um telefone, para trabalho com um despachante adicional, a fim de facilitar o trabalho dos despachantes através da divisão de tarefas, definidas previamente pelo Chefe da Supervisão de Operação e Distribuição - SPOD.

5. PROCEDIMENTOS GERAIS

5.1. Do Monitoramento e Controle

5.1.1. Das Informações Meteorológicas

5.1.1.1. Do Boletim Meteorológico

O Boletim Meteorológico, de responsabilidade de emissão do CIRAM/EPAGRI, deverá ser enviado, diariamente, para os chefes de Departamentos da Diretoria Técnica - DTE e a todos os chefes da Divisão de Distribuição - DVDI, chefes da Divisão de Operação e Manutenção - DVOM e Chefes da SPOD das Agências Regionais.

O Boletim Meteorológico deverá conter informações sobre as tendências dos modelos meteorológicos de forma clara e objetiva, possibilitando aos que o receberem, o acompanhamento das condições climáticas.

5.1.1.2. Da Comunicação Entre as Agências Regionais

Recomenda-se a comunicação entre os chefes da SPOD das Agências Regionais, de modo a indicar tendência de tempestade severa e/ou adversidades meteorológicas em locomoção de uma região para outra, de forma a complementar a previsão com o alerta meteorológico.

5.1.1.3. Do Alerta Meteorológico

O Alerta Meteorológico, de responsabilidade de emissão do CIRAM/EPAGRI, deverá ser encaminhado para os chefes de Departamentos da DTE e aos chefes da DVDI, chefes da DVOM e chefes da SPOD das Agências Regionais.

Cabe ao chefe da SPOD o repasse deste alerta meteorológico ao corpo operacional da Agência Regional, entre eles, os despachantes, o Supervisor de Despacho, quando existir, e o órgão de apoio.

O Alerta Meteorológico deverá conter informações sobre possível incidência de tempestade severa e/ou adversidade meteorológica em determinada região da concessionária, de forma clara e objetiva, possibilitando aos que o receberem, o entendimento da abrangência e a intensidade do evento previsto.

5.1.2. Do Estado de Alerta

5.1.2.1. Do Estado de Alerta das Equipes

Quando a tempestade severa e/ou adversidade meteorológica for iminente, poderá o chefe da SPOD, através das demais chefias da Agência Regional, efetuar a mobilização das equipes de manutenção de emergência, manutenção pesada e comercial, conforme inciso 5.2.1., constante nesta Instrução Normativa.

5.1.2.2. Da Aferição das Ferramentas e Material

Constatada a possibilidade de uma tempestade severa e/ou adversidade meteorológica, cabe ao Chefe da SPOD a aferição e a adequação das ferramentas disponíveis nos veículos, do KIT de Contingência, e do material disponível necessário para intervenção na rede elétrica, inclusive tomando providências quando constatada a falta de algum material, conforme subinciso 5.2.3.5., constante nesta Instrução Normativa.

Constatada a possibilidade de uma tempestade severa e/ou adversidade meteorológica, cabe aos chefes da SPMD, Supervisão de Projeto Cadastro e Construção - SPPC e DVCL/Supervisão de Utilização de Energia - SPUE a aferição e adequação das ferramentas e materiais disponíveis nos veículos necessários para intervenção na rede elétrica, inclusive tomando providências quando constatada a falta de algum material, conforme subinciso 5.2.3.5., constante nesta Instrução Normativa.

5.1.3. Da Avaliação e Caracterização do Evento

Dada a ocorrência de um evento de tempestade severa e/ou adversidade meteorológica, cabe ao chefe da DVDI, com o apoio dos chefes da SPOD, SPMD e SPPC, caracterizar a abrangência e intensidade do impacto causado pelo evento adverso para dimensionamento logístico, estimativas de prazo de restabelecimento geral e dimensionamento da necessidade de equipes, levando em conta, os seguintes itens:

a) número de Notas de Reclamação - NR em espera;

b) número de alimentadores fora;

c) inspeção “in loco”.

5.1.4. Da Decretação do Estado de Contingência

Cabe ao chefe da DVDI coordenar uma reunião, com a participação dos chefes da SPOD, SPMD e SPPC, para analisar a avaliação e a caracterização do evento, de forma a definir a necessidade ou não da decretação de estado de contingência.

Cabe ao chefe da Agência Regional, mediante solicitação do chefe da DVDI, decretar o estado de contingência e comunicar, através de contato telefônico e e-mail formal, conforme anexo 7.2. desta instrução Normativa, ao Diretor Técnico para fins de cientificação do estado de contingência.

O estado de contingência decreta-se em dois níveis:

a) Nível I - quando há a necessidade de mobilização de todo o efetivo de atendimento da Agência Regional decretante do estado de contingência;

b) Nível II - quando, além da mobilização de todo o efetivo da Agência Regional decretante, há necessidade de mobilizar equipes de atendimento de outras Agências Regionais.

A qualquer momento, poderá o chefe da Agência Regional, mediante solicitação do chefe da DVDI, alterar o nível de decretação do estado de contingência, cientificando ao Diretor Técnico, através de contato telefônico e e-mail formal, conforme anexo 7.2. desta Instrução Normativa.

5.2. Do Estado de Contingência

5.2.1. Da Mobilização de Equipes Adicionais

Quando da decretação do estado de contingência, para o aumento do efetivo de atendimento, deve-se mobilizar as equipes adicionais de atendimento, conforme o nível de contingência abaixo:

5.2.1.1. Nível I - Mobilização das Equipes Internas à Agência Regional

Cabe ao chefe da SPOD mobilizar o total efetivo das equipes de manutenção de emergência.

Cabe ao Chefe da DVDI mobilizar o total efetivo das equipes de manutenção pesada.

Cabe ao chefe da Agência Regional, mobilizar o total efetivo das equipes de atendimento comercial.

5.2.1.2. Nível II - Mobilização das Equipes Internas e Externas à Agência Regional

Além das mobilizações constantes no Nível I, também deverão ser mobilizadas equipes de outras Agências Regionais, conforme descrito a seguir:

Cabe ao chefe da Agência Regional o contato com o chefe de outras Agências Regionais, para fins de mobilização das equipes adicionais, cabendo ao chefe contatado a confirmação da viabilidade da solicitação, e quando da negativa, a justificativa do indeferimento.

Cabe ao chefe da SPOD, que enviar equipes adicionais para a Agência Regional solicitante, o envio de e-mail para o Chefe da SPOD da Agência Regional solicitante, informando o nome e matrícula dos eletricistas e o número do veículo da Celesc.

As equipes adicionais provenientes de outras Agências Regionais deverão estar com veículos em boas condições, com ferramentas adequadas para o atendimento e a equipe de eletricista capacitada para a intervenção na rede, e deverão dirigir-se ao Centro de Operação da Distribuição - COD solicitante, onde deverão ser recepcionadas pelo chefe da SPOD ou outro empregado delegado por ele.

5.2.2. Da Reunião de Planejamento e Operação

Cabe ao chefe da DVDI coordenar uma reunião geral, com a participação dos chefes da SPOD, SPMD e SPPC, despachantes, supervisores e eletricistas, de modo a efetuar o planejamento do atendimento em estado de contingência, visando abordar também os seguintes itens:

a) alerta ao corpo operacional quanto ao estado de contingência;

b) orientação aos eletricistas e despachantes do registro rigoroso das interrupções quanto à abertura e preenchimento das NR, principalmente quanto às informações de restabelecimento, de modo a subsidiar o filtro de reclamações no “Call Center”, bem como para as questões de segurança das equipes em atendimento emergencial;

c) orientação à correta aplicação dos procedimentos operacionais e de segurança (instruções normativas e normas regulamentadoras), salientando a sua importância frente ao desgaste excessivo e ao cansaço decorrente do trabalho exaustivo, o que propicia uma condição suscetível para acidentes;

d) apresentação da estrutura organizacional em estado de contingência, conforme inciso 5.3.2. desta Instrução Normativa.

5.2.3. Da Estrutura Organizacional em Estado de Contingência

5.2.3.1. Do Controle de Acesso ao COD

Em estado de contingência, somente será permitido o acesso ao COD pelos despachantes, chefe da SPOD, chefe da DVDI e demais pessoas envolvidas no processo, desde que devidamente autorizadas pelo Chefe da SPOD.
Cabe ao chefe da SPOD fazer cumprir o disposto acima.

5.2.3.2. Da Estação Adicional de Despacho

A utilização da estação adicional de despacho, composta por uma estação adicional de VHF, com o mesmo canal, uma máquina SIMO e um telefone, é opcional quando da decretação de estado de contingência Nível I, ficando a critério do chefe da SPOD, sendo, todavia, obrigatória para o Nível II.

5.2.3.3. Da Comunicação COD - Eletricista

No atendimento em estado de contingência, o despachante não deverá atender ligações telefônicas com exceção às referentes exclusivamente à função de despacho, sendo, portanto, necessário o repasse das ligações de terceiros (clientes consumidores e demais solicitantes de informações) para o órgão de apoio.

5.2.3.4. Da Acomodação e da Alimentação

Cabe ao chefe da Agência Regional fornecer as condições de alimentação e acomodação adequadas a todo o corpo operacional envolvido no atendimento em estado de contingência.

5.2.3.5. Da Aquisição de Material

Constatada a falta de material, cabe ao chefe da SPOD solicitar a aquisição do material faltante nas seguintes condições:

a) solicitar ao chefe da DVDI, que deverá contatar o chefe da Agência Regional, para verificar o material junto ao almoxarifado da Agência;

b) se o almoxarifado da Agência Regional não atender a necessidade, cabe ao chefe da DVDI contatar o chefe da Agência para tentar a aquisição de material do almoxarifado da Agência Regional mais próxima;

c) se o almoxarifado das Agências Regionais próximas não atenderem a necessidade, cabe ao chefe da Agência o contato com o Diretor Técnico para tentar a aquisição de material do Almoxarifado Central da Palhoça; e

d) se necessário, cabe ainda ao chefe da Agência Regional o contato com os fornecedores para providenciar a compra dos materiais.

5.2.3.6. Das Informações à Mídia

Cabe ao chefe da Agência Regional, através da interface de informações à mídia, disponível no SIMO e demais fontes, prestar informações à mídia em geral, assim como publicar à sua conveniência, indicadores percentuais do processo e restabelecimento do fornecimento.

5.3. Do Fim do Estado de Contingência

5.3.1. Do Retorno à Condição Normal de Operação

Cabe ao chefe da DVDI, com o auxílio dos chefes da SPOD, SPMD e SPPC, e, baseado nas informações de NR em espera e Alimentadores fora, solicitar ao chefe da Agência Regional o fim do estado de contingência, e o retorno às condições normais de operação.

Cabe ao chefe da Agência Regional, mediante solicitação do chefe da DVDI, decretar o fim do estado de contingência e comunicar, através de contato telefônico e e-mail formal, conforme anexo 7.2., ao Diretor Técnico para fins de cientificação do estado de contingência.

5.3.2. Da Desmobilização das Equipes Adicionais

Cabe ao chefe da SPOD efetuar a desmobilização das equipes adicionais, cientificando todo o efetivo que a Agência Regional retornou à condição normal de operação.

Cabe ao chefe da DVDI desmobilizar a estrutura organizacional instalada para operar em regime de contingência.

5.3.3. Do Controle do Cadastro Geo-Referenciado

Cabe ao chefe da DVDI definir um grupo de trabalho para avaliar o impacto da tempestade severa na depreciação do cadastro geo-referenciado da rede elétrica, efetuando as devidas correções quando da não conformidade comprovada.
O grupo deverá considerar:

a) levantamento das interrupções com incidência de mudança na topologia da rede elétrica, tais como alteração de condutores, alteração na fase de ligação do ramal do consumidor, etc;

b) inspeção “in loco” para constatação de alterações no cadastro da rede elétrica;

c) constatada as alterações, estas deverão ser atualizadas no cadastro geo-referenciado (GeneSis).

5.3.4. Da Avaliação dos Trabalhos em Estado de Contingência

Cabe ao chefe da DVDI preencher relatórios avaliando os indicadores de desempenho de cada um dos processos correlatos a esta Instrução Normativa, citados abaixo:

a) Relatório de Avaliação dos Trabalhos - contendo avaliação dos trabalhos, do desempenho e do cumprimento desta Instrução Normativa frente à decretação do estado de contingência;

b) Relatório Econômico-financeiro - contendo a avaliação dos custos associados ao processo de atendimento emergencial frente à decretação do estado de contingência;

c) Relatório de Segurança no Trabalho - contendo avaliação e análise do cumprimento dos procedimentos de segurança e levantamento do número de incidentes e eventuais acidentes.

Cabe ao DPOP a disponibilização e o controle do preenchimento dos relatórios citados no disposto acima.

6. DISPOSIÇÕES FINAIS

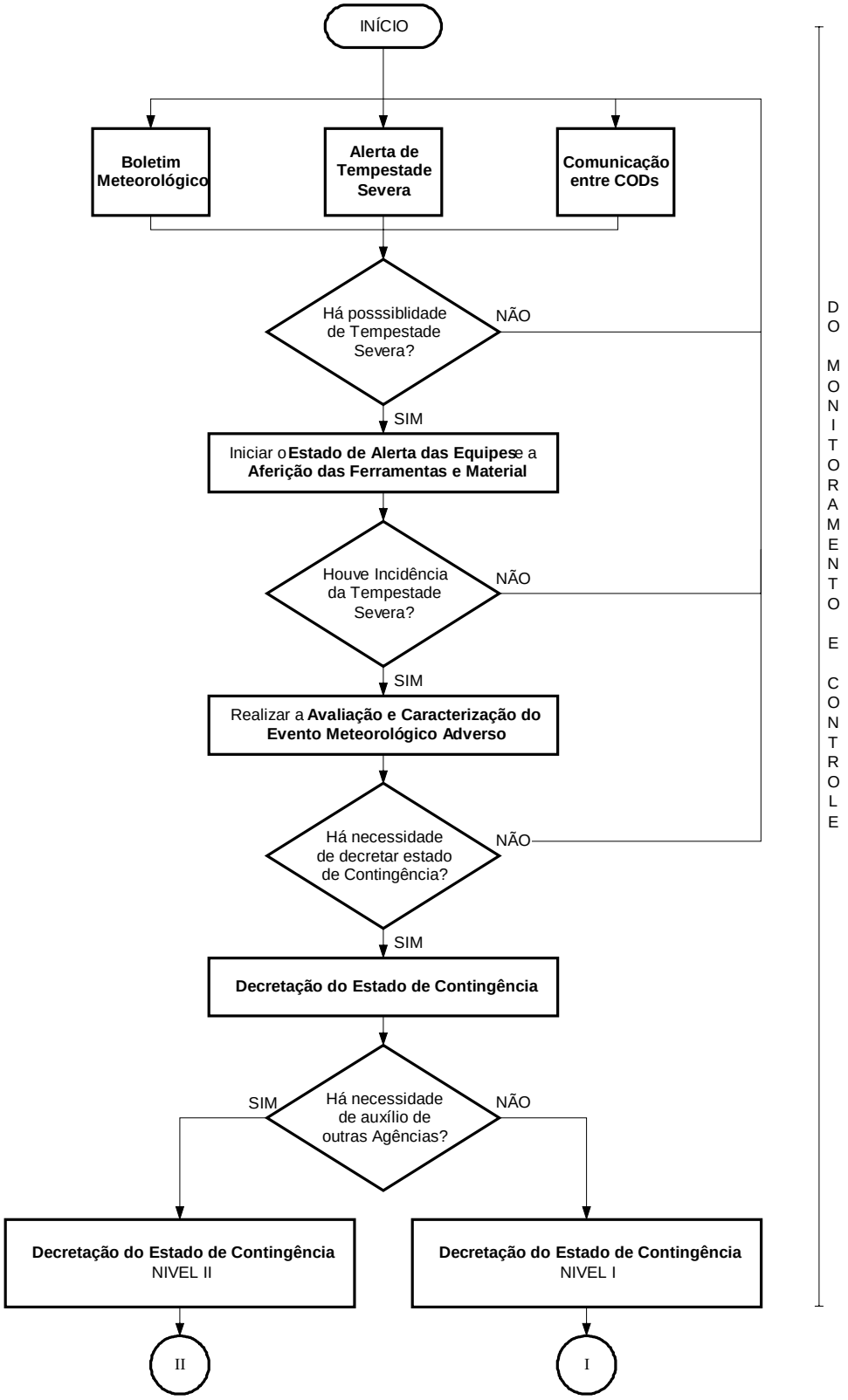
Não há.

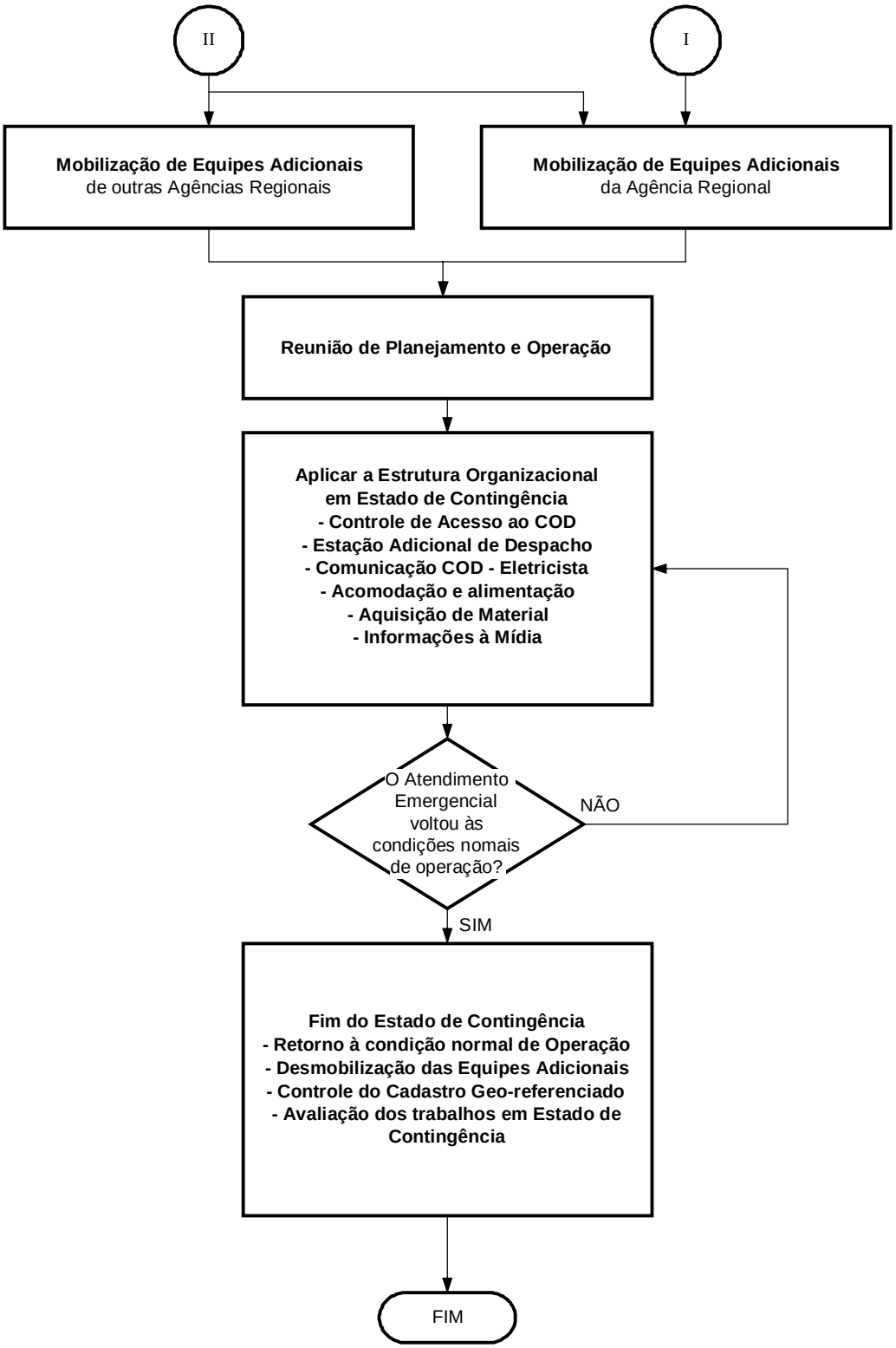
7. ANEXOS

7.1. Fluxograma do Processo

7.2. E-mail para Decretação do Estado de Contingência, Alteração do Nível de Decretação do Estado de Contingência e de Decretação do Fim do Estado de Contingência

7.1. Fluxograma do Processo




II
I
Mobilização de Equipes Adicionais
de outras Agências Regionais
Mobilização de Equipes Adicionais
da Agência Regional
Reunião de Planejamento e Operação
Aplicar a Estrutura Organizacional
em Estado de Contingência
- Controle de Acesso ao COD
- Estação Adicional de Despacho
- Comunicação COD - Eletricista
- Acomodação e alimentação
- Aquisição de Material
- Informações à Mídia
O Atendimento Emergencial voltou às condições nomais de operação?
NÃO
SIM
Fim do Estado de Contingência
- Retorno à condição normal de Operação
- Desmobilização das Equipes Adicionais
- Controle do Cadastro Geo-referenciado
- Avaliação dos trabalhos em Estado de Contingência
FIM
DO ESTADO DE CONTINGÊNCIA
DO FIM DO ESTADO DE CONTINGÊNCIA

7.2. E-mail para Decretação do Estado de Contingência, Alteração do Nível de Decretação do Estado de Contingência e de Decretação do Fim do Estado de Contingência

Assunto: Decretação do Estado de Contingência

Senhor Diretor,

Cientificamos a vossa excelência que esta Agência Regional decretou estado de contingência em nível (especificar se nível I ou II), conforme previsto na Instrução Normativa sobre Atendimento em Estado de Contingência.

Atenciosamente,

Nome do Chefe da Agência Regional
Nome da Agência Regional

****

Assunto: Alteração do Nível de Decretação do Estado de Contingência

Senhor Diretor,

Cientificamos a vossa excelência que esta Agência Regional alterou o nível de decretação do estado de contingência de nível I para nível II, conforme previsto na Instrução Normativa sobre Atendimento em Estado de Contingência.

Atenciosamente,

Nome do Chefe da Agência Regional
Nome da Agência Regional

****

Assunto: Decretação do Fim do Estado de Contingência

Senhor Diretor,

Cientificamos a vossa excelência que esta Agência Regional decretou o fim do estado de contingência, conforme previsto na Instrução Normativa sobre Atendimento em Estado de Contingência.

Atenciosamente,

Nome do Chefe da Agência Regional
Nome da Agência Regional