LUIZ HENRIQUE MAIORINO BARBARINI

**ANÁLISE DE RISCO PARA EMBARCAÇÕES COM SISTEMAS DE
ALARMES COM FOCO NOS FATORES HUMANOS E
ORGANIZACIONAIS**

Tese apresentada à Escola Politécnica da
Universidade de São Paulo para obtenção
do Título de Doutor em Ciências

São Paulo
2012

LUIZ HENRIQUE MAIORINO BARBARINI

**ANÁLISE DE RISCO PARA EMBARCAÇÕES COM SISTEMAS DE
ALARMES COM FOCO NOS FATORES HUMANOS E
ORGANIZACIONAIS**

Tese apresentada à Escola Politécnica da
Universidade de São Paulo para obtenção
do Título de Doutor em Ciências

Área de Concentração:
Engenharia Naval e Oceânica

Orientador:
Prof. Dr. Hernani Luiz Brinati

São Paulo
2012

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

São Paulo, 23 de maio de 2012

Assinatura do autor

Assinatura do orientador

Barbarini, Luiz Henrique Maiorino

**Análise de risco para embarcações com sistemas de alarmes
com foco nos fatores humanos e organizacionais / L.H.M.**

Barbarini. – ed. rev. -- São Paulo, 2012.

237 p.

**Tese (Doutorado) - Escola Politécnica da Universidade de
São Paulo. Departamento de Engenharia Naval e Oceânica.**

**1. Análise de risco 2. Embarcações 3. Sistemas de alarmes
4. Erro humano 5. Fatores humanos 6. Fatores organizacionais I.
Universidade de São Paulo. Escola Politécnica. Departamento
de Engenharia Naval e Oceânica II. t.**

DEDICATÓRIA

À minha esposa, pais, familiares e amigos,
pelos momentos que não pude me dedicar a vocês.

AGRADECIMENTOS

Ao professor Bernardo Luis Rodrigues de Andrade, que acompanhou a elaboração deste trabalho desde sua concepção até seus momentos finais.

*“Shipping is perhaps the most international of all the world's great industries
and one of the most dangerous.”*

International Maritime Organization (IMO)

RESUMO

Este trabalho apresenta uma proposta de modelo de análise de risco para embarcações, incorporando em sua formulação a influência das interações entre os sistemas de alarmes e os fatores humanos e organizacionais presentes a bordo. De acordo com estatísticas de sociedades classificadoras, o homem é o maior responsável por acidentes marítimos, e, desta forma, é um dos principais componentes da segurança de uma embarcação. A relevância do elemento humano se dá pelo fato de que ações e decisões humanas estão relacionadas tanto à causa, quanto à prevenção de acidentes.

O sistema de alarmes é um equipamento de segurança obrigatório, e com direta participação na dinâmica de um acidente, fornecendo informação para a tomada de decisão das ações por parte da tripulação na resolução do problema. O estudo da interação entre este equipamento e o elemento humano a bordo permite a gestores e armadores elaborar diretrizes para investimentos em sistemas de segurança e políticas que influenciam o desempenho humano, e, portanto, a segurança a bordo.

O modelo proposto, inspirado em relatório de acidentes marítimos, tem como ponto de partida uma estrutura sequencial do acidente e leva em consideração uma sucessão usual e simplificada dos eventos ocorridos, iniciando a partir de uma falha no sistema físico. O elemento humano, então, é incorporado à análise de risco através das técnicas de análise de confiabilidade humana, as quais têm como princípio a visão do homem como mais um componente do sistema, ou o “liveware” interagindo com “software” e “hardware”. Sob este ponto de vista, uma abordagem sócio-técnica é aplicada, ou seja, considera-se que um navio é composto não apenas de sua estrutura e máquinas, mas também de toda a tripulação.

Com o objetivo de exemplificar passos e hipóteses de uma aplicação do modelo proposto, é apresentada a aplicação ao caso do acidente da embarcação *Maersk Doha*, ocorrido em outubro de 2006 nos Estados Unidos, cujo relatório de investigação do acidente é de acesso público via Internet, no site da Marine Accident Investigation Branch – MAIB.

Palavras-chave: Análise de risco. Sistema de alarmes. Erro humano. Fatores humanos. Fatores organizacionais.

ABSTRACT

This work presents a risk analysis model for ships, focusing on the scenarios where the crew interacts with the alarm and monitoring system. According to statistics of classification societies, humans are largely responsible for accidents on board and, therefore, are considered a major component of the safety of vessels. The relevance of the human element is given by the fact that human decisions and actions are related to the cause of accidents, either being the direct causative factor of failure or influencing the probability of failure, and the prevention of accidents or mitigation of the consequences.

The alarm system is a mandatory component of certified vessels, with direct participation in an accident. It supplies information for the decision making process of the crew, considering their actions to recover the system. The study of the interactions between this automation equipment and the human element on board provides guidelines to managers and owners to invest in proper security systems and policies that influence human behavior, and therefore the safety on board.

The model, inspired in accident reports, has as starting point a sequential structure of the accident, and takes into account a typical and simplified sequence of events, starting from a failure in the physical system. The human element is incorporated into the risk analysis through techniques of human reliability analysis, which place man as another component of the system, or the "liveware" interacting with software and hardware. From this point of view, a socio-technical approach is applied, considering that a ship is composed of not only its structure and machinery, but also of the entire crew.

In order to illustrate the steps and assumptions to be done by an analyst applying the proposed model, the accident of the vessel Maersk Doha, occurred in October of 2006 in the United States, is analyzed. The report on the investigation of this accident is public and accessible via the Internet site of the Marine Accident Investigation Branch – MAIB.

Keywords: Risk analysis. Alarm system. Human error. Human factors. Organizational factors.

SUMÁRIO

1. INTRODUÇÃO.....	1
1.1. Contextualização.....	1
1.2. Motivação e Objetivos	5
1.3. Perspectiva de contribuição	9
1.4. Interdisciplinaridade do estudo	11
1.5. Organização do texto.....	11
2. ANÁLISE DE RISCO NA ÁREA NAVAL.....	13
2.1. Conceitos iniciais.....	13
2.2. Atores da indústria naval e o conflito de interesses.....	17
2.3. Análise de risco, IMO e sociedades classificadoras.....	19
2.4. O processo de análise de risco	25
2.4.1. Técnicas de análise de risco	27
2.4.2. Limitações do processo de avaliação de risco	29
2.4.3. Análise de sensibilidade.....	32
2.5. Análise probabilística de risco: abordagem pró-ativa	33
2.6. Critérios de aceitação do risco e análise custo benefício.....	36
2.7. Perigos relacionados ao setor de transporte marítimo	44
2.8. Métodos de consulta a especialistas	46
2.9. Análise de acidentes com embarcações.....	48
2.9.1. Definições	48
2.9.2. Modelos de acidentes	50
3. ERROS E FATORES HUMANOS	55
3.1. Conceitos básicos.....	56
3.1.1. Sistemas sócio-técnicos.....	56
3.1.2. Fatores Humanos.....	57
3.1.3. Erro Humano.....	59
3.1.3.1. Modelos do comportamento humano	61
3.1.3.2. Classificação dos erros humanos.....	63
3.1.3.3. Classificação dos erros humanos para a PRA	65
3.1.4. Fatores organizacionais	66

3.1.4.1.O modelo de Reason.....	68
3.1.4.2.Fatores organizacionais na área naval.....	70
3.1.4.3.Cultura de segurança como fator organizacional	72
3.1.5. Análise da confiabilidade humana.....	73
3.2. Visão teórica versus visão prática.....	74
3.3. Técnicas de Análise da Confiabilidade Humana	77
3.3.1. Histórico	77
3.3.2. Fatores de condicionamento de desempenho	78
3.3.3. Técnicas de primeira geração	82
3.3.3.1.Matriz de Confusão	82
3.3.3.2.Estimativa de especialistas	85
3.3.3.3.Success Likelihood Index Method (SLIM)	85
3.3.3.4.Correlação Tempo-confiabilidade.....	86
3.3.3.5.Confiabilidade Cognitiva Humana	88
3.3.3.6.THERP	90
3.3.3.7.Seleção dos métodos.....	93
3.3.3.8.Críticas aos métodos da primeira geração	93
3.3.4. Técnicas da segunda geração	94
3.3.4.1.Cognitive Reliability and Error Analysis Method (CREAM).....	95
3.4. Análise de sensibilidade.....	103
3.5. Revisão bibliográfica de metodologias para incorporar fatores humanos e organizacionais em PRA.....	104
4. SISTEMAS DE ALARMES PARA EMBARCAÇÕES E ERROS HUMANOS ASSOCIADOS	109
4.1. Considerações iniciais	109
4.2. Definições básicas	110
4.3. Histórico.....	111
4.4. Componentes do sistema de alarmes	112
4.5. Exigências das sociedades classificadoras	117
4.6. Modelos de comportamento relacionados aos alarmes.....	120
4.7. Fatores e erros humanos relacionados ao sistema de alarmes	123
4.7.1. Projeto da interface	125
4.7.2. Gerenciamento de alarmes	127

5. METODOLOGIA DE ANÁLISE DE RISCO PARA EMBARCAÇÕES COM SISTEMAS DE ALARMES	132
5.1. Premissas para a elaboração da metodologia	132
5.2. Proposta de um modelo de acidentes com sistema de alarmes.....	133
5.3. O modelo cognitivo para as ações humanas	137
5.4. Modelagem do sistema de alarmes	142
5.5. A estrutura do modelo de acidente para a análise de risco	145
5.6. Formulação matemática	147
5.7. Métodos aplicáveis para o cálculo das probabilidades.....	150
5.8. Aplicação da metodologia.....	154
6. ESTUDO DE CASO	156
6.1. Resumo do relatório de investigação do acidente.....	157
6.1.1. Síntese da narrativa do acidente.....	157
6.1.2. Causas do acidente	160
6.1.3. Tripulação	160
6.1.4. Sistema de alarmes.....	161
6.2. Modelagem e análise do acidente.....	162
6.2.1. Definição do problema e dos objetivos.....	163
6.2.2. Familiarização com o sistema e levantamento de dados	163
6.2.3. Identificação do evento iniciador	165
6.2.4. Estruturação dos cenários.....	166
6.2.5. Identificação dos fatores humanos e organizacionais	173
6.2.6. Modelagem do problema e formulação matemática	176
6.2.7. Análise quantitativa	190
6.2.8. Análise das incertezas e análise de sensibilidade	196
6.2.9. Interpretação dos resultados.....	200
6.2.10.Opções de controle do risco.....	201
6.2.11.Avaliação custo-benefício.....	203
6.2.12.Recomendações para a tomada de decisão e conclusões	204
7. CONCLUSÕES	206
7.1. Contribuições da metodologia.....	207
7.2. Observações sobre a aplicação da metodologia	208

7.3. Desenvolvimentos futuros	209
7.4. Considerações finais	210
REFERÊNCIAS.....	212

LISTA DE FIGURAS

Figura 1 - Principais causas de acidentes em navios.....	6
Figura 2 – Componentes do sistema integrado.....	10
Figura 3 – Perfil de risco comparando frequências anuais de fatalidades	14
Figura 4 – Os cinco pontos de vista do risco.....	17
Figura 5 – Metodologia da FSA.....	23
Figura 6 – Processo de análise e avaliação de risco	26
Figura 7 – Principais métodos de análise/avaliação de risco	28
Figura 8 – Domínios de funcionamento de um sistema	32
Figura 9 – Fluxograma típico de uma PRA	35
Figura 10 – Exemplo de curva F-N.....	37
Figura 11 – Diagrama típico do princípio ALARP	39
Figura 12 – Processo de análise de segurança aplicando critérios de aceitação	40
Figura 13 – Equilíbrio entre custo versus consequência	41
Figura 14 – Implementação ótima das medidas de segurança	41
Figura 15 – Perfil de risco e curva de Pareto	44
Figura 16 – Processo de consulta a especialistas.....	47
Figura 17 – Modelo genérico de acidente	51
Figura 18 – Modelo de acidente LCM	51
Figura 19 – Modelo da corrente causal para análise de perigo.....	53
Figura 20 – Três níveis de desempenho do operador humano.....	63
Figura 21 – Sequência de propagação de uma falha.....	63
Figura 22 – Tipos de erros de acordo com GEMS de (REASON, 1990a)	64
Figura 23 – Fontes do erro humano	65
Figura 24 – Árvore de ação do operador.....	66
Figura 25 – Modelo do queijo suíço de Reason (1990a) - adaptado.....	69
Figura 26 – Modelo do acidente organizacional	69
Figura 27 – Categorias do erro segundo critério de resposta	75
Figura 28 – Árvore de eventos do THERP	91
Figura 29 – Modelo de SMOc.....	97
Figura 30 – Modelo de COCOM.....	98
Figura 31 – Modelo de classificação do CREAM	99
Figura 32 – Matriz de resultado do CPCs e modos de controle	102
Figura 33 – Árvore de decisão da análise de sensibilidade	105

Figura 34 – Estrutura da metodologia SAM	108
Figura 35 – Componentes típicos do sistema de alarmes.....	112
Figura 36 – Arquiteturas centralizada e distribuída dos sistemas de alarmes.....	114
Figura 37 – Exemplo de sistemas de alarmes com arquitetura distribuída	115
Figura 38 – Faixas de operação do sensor e alarmes	116
Figura 39 – Exemplo de um sistema cognitivo	121
Figura 40 – Controle Homem-Máquina de um navio.....	121
Figura 41 – Ciclo de vida do gerenciamento de alarmes	130
Figura 42 – Modelo de acidente para embarcação com sistema de alarmes	135
Figura 43 – Expansão do modelo de acidentes	137
Figura 44 – Modelo das ações de recuperação da tripulação.....	138
Figura 45 – Analogia dos fatores organizacionais a uma mesa de mixagem.....	141
Figura 46 – Linha do tempo da deterioração do sistema	144
Figura 47 – Estrutura do modelo para a análise de risco	146
Figura 48 – Variáveis da estrutura do modelo.....	148
Figura 49 – Modelo de acidente completo para aplicação na análise de risco	151
Figura 50 – Resumo dos métodos sugeridos para cálculo dos termos	154
Figura 51 – Embarcação Maersk Doha.....	157
Figura 52 – Diagrama esquemático do sistema de geração de vapor	164
Figura 53 – Diagrama da sequência de eventos do acidente	169
Figura 54 – Árvore de eventos do acidente.....	171
Figura 55 – Sequência de eventos – fase 1	176
Figura 56 – Sequência de eventos – fase 2	181
Figura 57 – Sequência de eventos – fase 3.....	183
Figura 58 – Sequência de eventos – fase 4.....	186
Figura 59 – Visão de recuperação do sistema	189
Figura 60 – Visão de falha do sistema	189
Figura 61 – Modo de controle do método CREAM aplicado à fase 3.....	193
Figura 62 – Modo de controle do método CREAM aplicado à fase 2.....	195

LISTA DE TABELAS

Tabela 1 – Atores da indústria que influenciam a segurança	18
Tabela 2 – Risco anual aceito pela sociedade nos Estados Unidos	38
Tabela 3 – Risco máximo tolerado para embarcações no Reino Unido	39
Tabela 4 – Medidas de risco no setor naval	42
Tabela 5 – Classificação dos tipos primários de erro (REASON, 1990a)	64
Tabela 6 – Classificação dos PSF segundo (SWAIN; GUTTMANN, 1983)	80
Tabela 7 – CPC e a confiabilidade do desempenho	81
Tabela 8 – Dependência entre CPC	82
Tabela 9 – Matriz de confusão	83
Tabela 10 – Matriz de resposta da planta	83
Tabela 11 – Matriz de procedimentos para o evento iniciador	84
Tabela 12 – Matriz de entradas e procedimentos	84
Tabela 13 – Tabela de PSF para HCR	89
Tabela 14 – Erros na verificação e leitura de monitores	91
Tabela 15 – Probabilidade de erros humanos para nível de estresse	92
Tabela 16 – Métodos de ACH e tipos de erro	93
Tabela 17 – Intervalo de probabilidades dos modos de controle	102
Tabela 18 – Exemplo de aplicação da análise de sensibilidade	104
Tabela 19 – Tabela de alarmes para plantas de geração de energia elétrica	118
Tabela 20 – Atividades humanas relacionadas ao sistema de alarmes	140
Tabela 21 – Alarmes relevantes em relação à caldeira e economizador	161
Tabela 22 – Cronologia dos eventos importantes para a análise	165
Tabela 23 – Fases do acidente	167
Tabela 24 – Estados do sistema de alarmes	170
Tabela 25 – Fatores humanos identificados no relatório de investigação	174
Tabela 26 – Fatores organizacionais relacionados à tripulação	174
Tabela 27 – Fatores organizacionais relacionados ao sistema técnico	175
Tabela 28 – Fatores organizacionais relacionados aos níveis de perda	175
Tabela 29 – Conjunto das variáveis do modelo na fase 1 do acidente	177
Tabela 30 – Conjunto das variáveis do modelo na fase 2 do acidente	181
Tabela 31 – Conjunto das variáveis do modelo na fase 3 do acidente	184
Tabela 32 – Conjunto das variáveis do modelo na fase 4 do acidente	186
Tabela 33 – Análise do erro de interpretação na fase 3	192

Tabela 34 – CPCs específicos referentes à fase 3 do acidente	193
Tabela 35 – Análise do erro de interpretação na fase 2	194
Tabela 36 – CPCs específicos referentes à fase 2 do acidente	195
Tabela 37 – Tabela de análise de sensibilidade CPCs da fase 3.....	197
Tabela 38 – Resultado da análise de sensibilidade CPCs da fase 3	198

1. INTRODUÇÃO

We live in a global society which is supported by a global economy – and that economy simply could not function if it were not for ships and the shipping industry. (IMO, 2006, p. 4)

1.1. Contextualização

A engenharia moderna vem revolucionando a maneira como as embarcações são construídas e operadas. Ferramentas computacionais poderosas são capazes de simular o desempenho de um navio completo, mesmo antes de sua primeira caverna ser soldada. Cartas náuticas tridimensionais, radares sofisticados e posicionamento dinâmico também vêm sendo largamente empregados nas embarcações, aumentando a segurança na navegação. E ainda assim acidentes acontecem. As sociedades classificadoras mais conceituadas sugerem a adoção de técnicas de análise de risco há vários anos ou décadas, e ainda assim “o navio perfeito” está à milhas de distância da realidade. Está claro que ao longo do século passado, as máquinas e estruturas se tornaram muito mais confiáveis. Por conta disso, o desafio atual está em garantir que outro componente do sistema falhe menos: o ser humano.

A preocupação com o elemento humano não é recente, e também não é exclusiva da área naval. A disciplina sobre fatores humanos, conceito que será propriamente definido nos capítulos a seguir, teve seu início durante a Segunda Guerra Mundial, quando se percebeu que as armas modernas necessitavam de uma engenharia especial para a interface entre pessoas e máquinas (SHERIDAN, 2002). Adequar o homem à máquina seria a nova tarefa dos engenheiros, não mais só em relação ao tamanho e força, mas também agora em relação aos limites de visão, audição, experiência e capacidade de aprendizado.

As estatísticas de acidentes envolvendo erros humanos também impulsionaram os estudos sobre o elemento humano na indústria. Segundo Hollnagel (1998), da década de 1960 para cá, a parcela dos acidentes atribuídos ao ser humano, na indústria em geral, ficou mais significativa. Não porque os

operadores estejam errando mais, mas porque as máquinas e sistemas, por conta do avanço tecnológico, estão falhando menos.

Um estudo da guarda costeira americana – United States Coast Guard (USCG, 2010 apud HETHERINGTON; FLIN; MEARNS, 2006), reportou que, em um período de 5 anos, acidentes comuns envolvendo embarcações, como colisões e encalhes, tiveram uma redução de sua incidência. E isto se explicava devido ao aperfeiçoamento da tecnologia de auxílio à navegação. Em contrapartida, a *Marine Accident Investigation Branch* (MAIB) aponta que “um fator que ainda domina a maioria dos acidentes marítimos é o erro humano” (MAIB, 2000, p. 4). Hetherington e colaboradores concluem:

There are two sides to the technological advances. Improvements in ship design and navigation aids have reduced the frequency and severity of shipping incidents. In turn, the reduction of failures in technology has revealed the underlying level of influence of human error in accident causation. (HETHERINGTON; FLIN; MEARNS, 2006, p. 402)

A relevância do elemento humano se dá pelo fato de que ações e decisões humanas estão relacionadas (i) à causa de acidentes, sendo diretamente o fator causador de uma falha ou influenciando na probabilidade de uma falha, e (ii) à prevenção dos acidentes ou mitigação das consequências.

Rothblum (2000) demonstra a mesma preocupação sobre a relevância dos erros humanos na área marítima:

Over the last 40 years or so, the shipping industry has focused on improving ship structure and the reliability of ship systems in order to reduce casualties and increase efficiency and productivity. We've seen improvements in hull design, stability systems, propulsion systems, and navigational equipment. Today's ship systems are technologically advanced and highly reliable. Yet, the maritime casualty rate is still high. Why? Why is it, with all these improvements, we have not significantly reduced the risk of accidents? It is because ship structure and system reliability are a relatively small part of the safety equation. The maritime system is a people system, and human errors figure prominently in casualty situations. (...)Therefore, if we want to make greater strides towards reducing marine casualties, we must begin to focus on the types of human errors that cause casualties. (ROTHBLUM, 2000, p. 1)

Rothblum (2000) também aponta que cerca de 75% a 99% dos acidentes são causados, pelo menos em parte, por erros humanos, sendo que os erros humanos correspondem a:

- 84 a 88% dos acidentes com navios-tanque
- 75% dos naufrágios com rebocadores
- 89 a 96% das colisões
- 75% dos abalroamentos
- 75% dos incêndios e explosões

Para a indústria naval e petrolífera brasileira, o assunto também é deveras atual. Em 2005, a Petrobras, uma das pioneiras no Brasil em investir em estudos direcionados ao ser humano a bordo, implantou a iniciativa estratégica “Fator Humano” na Frota Nacional de Petroleiros (Fronape), com o objetivo principal de melhorar o desempenho em SMS (Segurança, Meio Ambiente e Saúde) (FREITAS; VENÂNCIO; ARRUDA, 2006). Através da contratação de serviços de treinamento comportamental, a empresa busca promover mudanças comportamentais nos gestores de bordo, como comandantes e chefes de máquinas, aprimorando o gerenciamento do fator humano nos navios. O objetivo principal destas ações é reduzir os fatores humanos considerados fatores de risco para acidentes, através da conscientização e incentivos para a construção de ambientes que possibilitem maior bem-estar da tripulação, maior qualidade de vida e maior comprometimento com a empresa.

Sabe-se, porém, que além dos fatores humanos, também é importante estudar e avaliar os aspectos da organização que interferem nestes fatores. Por trás das variadas causas dos erros humanos ocorridos em sistemas complexos, como um navio, fatores gerenciais e organizacionais também exercem importante influência sobre as ações e decisões dos indivíduos. Perrow (1999 apud HETHERINGTON; FLIN; MEARNS, 2006) cita que a indução do erro humano, em sistemas como navios, está relacionada com a organização social da tripulação, às pressões econômicas, a estrutura da indústria, e às dificuldades de regulamentação internacional. Segundo Murphy e Paté-Cornell (1996), acidentes que ficaram “famosos” como os de Chernobyl, Three Mile Island e do ônibus espacial Challenger, entre vários outros acidentes (também nos setores aéreos e marítimos), tiveram suas causas relacionadas a fatores humanos e organizacionais. Reason (1990b) identifica este contexto como “a era dos acidentes organizacionais”, onde os perigos surgem de aspectos sociais e organizacionais do sistema.

Com esta abordagem, é possível compreender que não apenas o ser humano a bordo de um navio influi nas probabilidades de falha de seus sistemas. Os fatores organizacionais também terão um papel nas fases de projeto, operação e, no pior dos casos, na dinâmica de um acidente, contribuindo positiva ou negativamente no comportamento da tripulação e no estado da planta. Captar esta influência da organização na resposta da tripulação, portanto, é extremamente desejável, pois permite aos gestores elaborarem políticas assertivas para prevenção de acidentes.

Entre as publicações da área, vários estudos já foram feitos com o objetivo de estudar os erros humanos na operação de máquinas, ou de equipamentos eletrônicos para navegação (MATURANA; MARTINS, 2008; MOREL; CHAUVIN, 2006; WU; CONTI, 2007). No entanto, pouco é estudado sobre o sistema de alarmes e monitoramento de máquinas. Os sistemas de automação, dentre eles o sistema de alarmes, é um tema frequente em relatórios de acidentes e em normas de segurança de navios. Estes estão relacionados diretamente aos fatores humanos, principalmente no que se refere à consciência situacional (HETHERINGTON; FLIN; MEARNS, 2006).

O sistema de alarmes, cuja arquitetura será apresentada em detalhes na seção 4.4, tem o papel de adquirir e processar dados de sensores espalhados pelas principais máquinas, como motores, geradores, tanques, bombas de porão, válvulas, temperaturas, etc. De acordo com sua programação, o sistema alerta o usuário quando algum dos pontos medidos alcançou algum estado indesejável, permitindo-se a imediata reação e intervenção no problema. No passado, grandes embarcações operavam 24 horas por dia sob a monitoração de homens na praça de máquinas, tripulantes para limpeza, para checagem de água e óleo, bombeiros, e engenheiros. O sistema de alarmes e monitoramento contribuiu para automatizar muitas destas tarefas, tornando realidade a operação de uma praça de máquinas desguarnecida.

Atualmente em embarcações modernas, toda a monitoração é feita remotamente, permitindo que a manutenção seja feita em horário regular de trabalho, das 9 às 17 horas, por exemplo. Com interação direta com a tripulação, o sistema de alarmes possui um papel fundamental antes e durante a ocorrência do acidente. O conjunto sistema de alarmes–tripulação se torna um elemento crítico na propagação ou mitigação do problema a bordo.

O sistema de alarmes de um navio deve atender a diversas normas técnicas, estabelecidas por sociedades classificadoras (por exemplo: ABS (2008a); ABS

(2008b); BV (2005) e GL (1996)), quanto ao seu projeto, como requisitos de interface, resistência ao ambiente marítimo, nível sonoro dos alarmes; e quanto a sua operação, evitando confundir os operadores, e garantindo que todos os tripulantes pertinentes recebam a informação do problema que está ocorrendo. As principais máquinas devem ser constantemente monitoradas, como motores de propulsão, geradores, aquecedores, sistemas de energia elétrica; devem ser monitorados também níveis de tanques, alagamentos dos porões, e assim por diante. O porte e função de cada embarcação irá determinar o nível de exigência a se cumprir e número de pontos que o sistema de alarmes deverá monitorar.

Este trabalho poderá ser aplicado a qualquer porte ou tipo de embarcação, no entanto, conforme será discutido no Capítulo 4, o interesse principal será os sistemas que abrangem apenas o monitoramento das máquinas, e não o controle ou comando (automático ou manual) dos sistemas e máquinas a bordo.

1.2. Motivação e Objetivos

Estima-se que cerca de 80% de todos os acidentes no mar são atribuíveis aos erros humanos, enquanto os 20% remanescentes são consequência de falhas no casco ou equipamentos (SQUIRE, 2005). Neste tipo de sistema complexo, fatores humanos vêm ganhando importância cada vez maior. Estudos realizados pela Guarda Costeira Americana (COMPERATORE; RIVERA, 2003) demonstraram que existem fatores humanos a bordo de navios que afetam os limites de tolerância dos tripulantes e geram condições que aumentam a possibilidade de erros humanos e, consequentemente, a ocorrência de acidentes. Segundo a UK P&I Club (ALERT!, 2003), erros humanos custam à indústria marítima 541 milhões de dólares ao ano. Conforme esta análise, eles constataram que 62% dos 6.091 casos de acidentes ocorridos num período de 15 anos foram atribuídos a erros humanos. O estudo publicado no *International Maritime Human Element Bulletin* (ALERT!, 2003), apresentado na Figura 1, detalha estas estatísticas.

Um fato recente, cuja causa foi atribuída a um erro humano, foi o naufrágio do navio de cruzeiro Costa Concordia, no Mar Mediterrâneo, em 13 de janeiro de 2012. As investigações preliminares apontam que o navio se chocou com rochas devido a

uma manobra imprudente do comandante da embarcação, causando um rompimento no casco do navio, que transportava mais de 4200 pessoas, entre passageiros e tripulantes.(REVISTA VEJA, 2012)

Em contrapartida, a existência do elemento humano, com suas características únicas, como capacidade de adaptação e solução de problemas, é o que tem evitado um número muito maior de falhas de sistema. “Na verdade, a análise dos grandes acidentes industriais revela que os operadores de sistemas de controle são apenas a ponta de uma cadeia de problemas, muitas vezes latentes, que apenas se mostram quando combinados em alguma situação catastrófica.” (FILGUEIRAS, 1996, p. 4).

Figura 1 - Principais causas de acidentes em navios
– adaptado de (ALERT!, 2003, p. 3)

Como já mencionando na seção 1.1, erros humanos podem ter origem em fatores organizacionais, conforme explicado por Schönbeck (2007):

(...) human errors may be of various origins and part of larger, organizational processes that encourage unsafe acts, which ultimately produce system failures. (...) unsafe acts are preceded by reasons, motives, expectations, plans, and ways of reasoning, which together are labeled psychological precursors. (SCHÖNBECK, 2007, p. 26)

Assim como na indústria, sistemas automatizados em embarcações fazendo funções antes exercidas por seres humanos é algo crescente e irreversível. E, por

conta disso, onde houver um ser humano interagindo com um sistema, existe uma questão sobre fatores humanos. Koene e Vedam (2000) citam que investigações de incidentes na indústria revelam que o sistema de alarmes pode ser um fator que contribui para o acontecimento de acidentes, quando o equipamento não está propriamente dimensionado ou projetado.

Frente ao cenário de crescente foco em fatores humanos e organizacionais, e frente à irreversível tendência do emprego de sistemas automáticos exercendo funções relacionadas ao monitoramento das máquinas nos navios, a proposta desta tese é abordar, de modo unificado, o estado da arte de técnicas de análise de risco e técnicas de análise de confiabilidade humana, fatores humanos e organizacionais, e aspectos relacionados ao sistema de alarmes e monitoramento. Assim, contribuindo com armadores, estaleiros, projetistas, gerentes e decisores para responder as seguintes questões:

1. Qual a contribuição do sistema de alarmes na redução do risco da embarcação?
2. Como melhorar o projeto de um sistema de alarmes considerando os fatores humanos e organizacionais?

As respostas destas perguntas não são óbvias ou diretas. Para buscar chegar à resposta destas perguntas, percorrer-se-á o caminho de levantar e criticar os métodos e técnicas de análise de risco disponíveis, e, baseado em um método que aborda os fatores humanos e organizacionais, o modelo *System-Action-Management* (SAM) (MURPHY; PATÉ-CORNELL, 1996), será proposto um modelo de análise específico, onde estarão representadas explicitamente as funções do sistema de alarmes. A preocupação principal no desenvolvimento deste modelo é que este seja aplicável e gerenciável, e que contemple os eventos e particularidades existentes no setor naval. Aplicável significa que o modelo não pode apenas contar com dados históricos e estatísticas confiáveis, uma vez que a disponibilidade de dados é bastante restrita. Gerenciável, pois o modelo deve permitir que o analista escolha a quantidade de informações que são relevantes, e consequentemente, o custo financeiro e de recursos humanos a serem investidos para a análise. As particularidades existentes em um navio foram estudadas por meio de relatórios de investigações de acidentes, os quais descrevem com detalhes e clareza questões

dentro e fora da praça de máquinas, envolvendo gestores, culturas e políticas corporativas.

A metodologia SAM inicia-se a partir de um modelo de análise de risco do sistema técnico, se expandindo para incluir as ações e decisões humanas que afetam o desempenho deste sistema e os fatores organizacionais que influenciam estas ações. A sequência de eventos de um acidente é analisada, através de equações de probabilidades condicionais, o que facilita a análise sistemática dos diversos cenários. A interpretação e expansão do modelo SAM, proposta neste trabalho, alinha-se com os objetivos expostos acima. Entretanto, a ferramenta resultante não responde as perguntas anteriores com um número exato ou uma fórmula genérica, assim como nenhum método de análise de risco o faz. No entanto, o modelo estabelece uma forma racional para abordar um problema complexo, já que envolve o estudo do comportamento humano, e estabelece um norte para a tomada de decisão.

Em síntese, este trabalho tem como objetivo geral propor uma metodologia de análise de risco para embarcações com sistemas de alarme, considerando tanto o sistema técnico, quanto os fatores humanos e fatores organizacionais.

Os objetivos específicos são:

- 1) Associação das técnicas de análise de risco e de análise de confiabilidade humana ao modelo proposto.
- 2) Elaborar uma ferramenta que permita aos gestores identificar e direcionar investimentos que melhor influenciem na segurança da embarcação, através da melhoria dos fatores humanos e organizacionais.
- 3) Auxiliar e prover subsídio para as respostas das perguntas sobre a contribuição e o projeto do sistema de alarmes.

Os seguintes pontos serão explorados:

- 1) Levantamento das técnicas de análise de risco e sua aplicação na área naval.
- 2) Estudo das técnicas de confiabilidade humana e dos fatores humanos e organizacionais presentes em um navio.
- 3) Associação das técnicas de análise de risco e de análise de confiabilidade humana ao modelo proposto.

1.3. Perspectiva de contribuição

Wang et al. (2004) mencionam que desde quando se começou a buscar alternativas às regulamentações prescritivas, ou seja, que apenas descrevem o que deve ser feito, abriu-se espaço para tentativas de se utilizar regulamentações baseadas em análise de risco, abrindo um campo vasto para novos desenvolvimentos de modelos de análise de risco e tomada de decisão. Ren et al. (2008) defendem que “existe a necessidade de repensar a metodologia de avaliação de segurança de sistemas *offshore*”. Segundo este, há 20 anos se utilizam técnicas de análise de risco e confiabilidade para se reduzir risco no Reino Unido. No entanto, o foco foi tradicionalmente em aspectos técnicos do projeto, construção e operação, sem atenção aos fatores humanos e organizacionais. Para tal, modelos descritivos e não preditivos são utilizados, e estes são pouco efetivos em apontar como prevenir acidentes.

A revisão da literatura sobre a contribuição humana em acidentes marítimos e sobre análise de risco para embarcações revela o grande desafio de se despertar o interesse de armadores e estaleiros a respeito da importância do elemento humano na confiabilidade e dependabilidade¹ da embarcação (CLOAREC, 1994). Hetherington, Flin e Mearns (2006) mencionam que, “aparentemente, muito pouca pesquisa foi feita sobre fatores humanos na indústria naval” (tradução nossa).

Em seu trabalho sobre os recentes progressos na área de avaliação de risco na indústria naval, Wang (2006) cita quatro temas mais presentes nas pesquisas:

1. Métodos de consulta a especialistas, com métodos de tomada de decisão subjetiva baseadas em segurança;
2. Otimização de projeto e operação com abordagem baseada em segurança;

¹ Em linhas gerais, dependabilidade (do inglês, *dependability*), também traduzido como “confiança no comportamento” ou “segurança de funcionamento”, significa garantir a qualidade do produto ao longo de um período de tempo (CLOAREC, 1994). Em outras palavras, dependabilidade de um navio é uma medida qualitativa da capacidade deste entregar um serviço que se pode confiar, seja este serviço o transporte de carga, passageiro, ou um reboque. A dependabilidade tem um papel importante, pois fornece uma visão global da confiabilidade e manutenibilidade do sistema, e, portanto, da sua segurança e disponibilidade.

3. Aplicação de métodos de outras disciplinas, como redes neurais e redes Bayesianas para estimar riscos e tomar decisões;
4. Métodos que modelam fatores humanos e organizacionais.

De fato, esta tese se enquadra no quarto tema. A proposição de um modelo de análise de risco, que contemple o sistema de alarmes e os fatores organizacionais, deverá contribuir para que as embarcações apresentem melhores características de confiabilidade e de segurança. A abordagem aqui apresentada também será conveniente para uma análise quantitativa do risco de acidentes dentro de um cenário delimitado, permitindo a comparação dos valores obtidos em cada cenário e a análise de sensibilidade das probabilidades de ocorrência de acidentes. A Figura 2 mostra o entendimento da IMO (*International Maritime Organization*) sobre a visão de um sistema integrado, envolvendo o sistema técnico, tripulação, organização, gerência e ambiente. Esta figura será mais bem explicada nos capítulos seguintes.

Figura 2 – Componentes do sistema integrado
– adaptado de (IMO, 2002a, p. 17)

Acredita-se que esta abordagem poderá servir de subsídio para empresas certificadoras e seguradoras aperfeiçoarem exigências de segurança, uma vez que o estudo racional das formas de interação do sistema de alarmes com a tripulação acaba por apontar combinações de fatores, por vezes não óbvios, que podem contribuir significativamente para o risco de acidente. Segundo, uma destas empresas certificadoras, a American Bureau of Shipping (ABS):

[...] methods for calculating risks and capturing of data in the maritime industry are still in their infancy. It will take a period of learning and maturing before risk calculations can gain a good degree of repeatability and confidence necessary for use as acceptance criteria. In the meantime, while more research and development is going on to help in the accomplishment of this goal, philosophical development of safety frameworks based on risk consideration should be advanced and debated in the industry (ABS, 2000, p. 84) .

1.4. Interdisciplinaridade do estudo

A elaboração de um modelo de análise de risco de embarcações envolvendo sistema físico e comportamento humano certamente exige estudos interdisciplinares, abrangendo disciplinas de Engenharia Naval, Confiabilidade de Sistemas, Análise de Risco, Tomada de Decisão, Confiabilidade Humana e Automação Industrial.

Apesar da interdisciplinaridade exigida, a base deste trabalho está relacionada aos temas de análise de risco e tomada de decisão. Todavia, os conceitos de confiabilidade humana são fundamentais, pois desta se extraem os modelos cognitivos humanos necessários para o entendimento do comportamento humano em uma situação de estresse ou perigo, como durante um acidente marítimo.

1.5. Organização do texto

Esta tese está organizada nos capítulos como segue:

O Capítulo 1 é esta Introdução, que compreende a contextualização do assunto, as motivações e objetivos do estudo e sua interdisciplinaridade. Procura-se situar o leitor através de estatísticas, de forma apontar a importância e relevância do estudo.

O segundo, terceiro e quarto capítulos fazem parte da revisão bibliográfica do trabalho, onde será apresentado o estado da arte sobre os temas abordados. O Capítulo 2 apresenta os diversos aspectos sobre a análise de risco na área naval e seus principais métodos e referências na literatura. Abordam-se as técnicas de

análise de risco e o tema de análise de acidentes envolvendo embarcações. No Capítulo 3, descrevem-se os principais conceitos sobre erros e fatores humano na área naval, bem como, detalha-se as técnicas de análise da confiabilidade humana. Busca-se explicar e relacionar o erro humano e os fatores humanos e organizacionais ao ambiente de uma embarcação, dando subsídio ao entendimento dos passos considerados na proposição do modelo.

O Capítulo 4 abordará assuntos relacionados ao sistema de alarmes. Inicia-se com um breve histórico do sistema, as exigências de sociedades classificadoras e descrição de seus componentes e funções. Em seguida, faz-se a ligação com os capítulos anteriores, apresentando-se modelos do comportamento humano relacionados a sistemas de alarmes.

O quinto capítulo contém a proposição do modelo de análise de risco para embarcações com sistemas de alarmes. São apresentados o modelo de acidente escolhido para representar o problema e os modelos cognitivos que serão utilizados na análise. A estrutura da metodologia e sua formulação matemática são apresentadas, juntamente com os métodos de análise de confiabilidade humana sugeridos para a análise quantitativa da equação geral do modelo. O Capítulo 6 contém um estudo de caso, onde se ilustra a aplicação do modelo proposto a um caso real. São demonstrados os principais passos de uma análise de risco, discutindo-se os resultados e contribuições do modelo proposto.

Por fim, o Capítulo 7 apresenta as conclusões da tese.

2. ANÁLISE DE RISCO NA ÁREA NAVAL

Shipping has from time to time been under attack for unacceptable safety and environmental performance. (KRISTIANSEN, 2005, p.3)

Este capítulo pertence à parte inicial desta tese, compreendendo os aspectos teóricos relacionados, onde serão abordados temas que servirão de base para a estruturação do modelo de análise a ser proposto no Capítulo 5. Neste capítulo, serão discutidos os principais pontos sobre análise e gestão de risco no contexto da indústria naval e de transportes marítimos. Os temas específicos necessários para entendimento das discussões posteriores serão apresentados, como técnicas de análise de risco, modelos de acidentes, conceitos de análise de risco pró-ativa e critérios de aceitação de risco.

2.1. Conceitos iniciais

A palavra “risco” contém vários significados. Muito utilizada popularmente, mesmo as definições do dicionário não são suficientemente precisas para as aplicações de análise e gestão de risco.

O dicionário Michaelis define risco como “possibilidade de perigo, incerto mas previsível, que ameaça de dano a pessoa ou a coisa” (WEISZFLOG, 1998). Guimarães (2003) define risco como “a percepção ou avaliação das possibilidades da efetiva ocorrência de um evento indesejável”. Kumamoto e Henley (1996), assim como a norma ABNT ISO/IEC Guia 73², por outro lado, definem formalmente risco como sendo o par ordenado representado pela probabilidade P de ocorrência de um evento (ou frequência) e sua correspondente consequência C :

$$Risco \equiv \{(P_1, C_1), (P_2, C_2), \dots, (P_n, C_n)\} \quad (1)$$

² A norma ABNT/ISO IEC Guia 73 foi elaborada para conter o vocabulário utilizado nos processos de gestão de riscos, com os termos e definições corretos traduzidos para português.

A consequência, ou gravidade, pode ser expressa como o número de pessoas afetadas, propriedade destruída, quantidade de vazamento, área afetada, tempo de atraso, ou dinheiro perdido (ABS, 2000). A eq. (1) remete a ideia de valor esperado da Teoria das Probabilidades, onde o risco é o “valor esperado” de uma determinada consequência.

A distribuição dos pares ordenados (P,C) é chamada de curva ou perfil de risco, ou curva Farmer, e pode ser representada graficamente com a probabilidade de ocorrência no eixo vertical, e consequência no eixo horizontal, como apresentado na Figura 3.

Figura 3 – Perfil de risco comparando frequências anuais de fatalidades
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 5)

Kumamoto e Henley (1996) propuseram uma expressão para representação do risco que inclui outros aspectos que o par (P,C) não representa, destacando que o risco pode ser avaliado em função de outros fatores, como a utilidade U , o cenário de causa S e a população afetada PA . Neste caso, a eq. (1) poderia ser reescrita de forma genérica como:

$$Risco \equiv \{(P_i, C_i, U_i, S_i, PA_i | i = 1, \dots, n)\} \quad (2)$$

A utilidade U , ou função utilidade, é muito utilizada nos métodos de tomada de decisão (SHIMIZO, 2002), já a população afetada PA foi criada para análises na indústria nuclear.

Em sua forma mais usual, Ayyub (2003) aponta que o risco é avaliado da seguinte maneira:

$$Risco \left(\frac{Consequência}{Tempo} \right) \equiv Probabilidade \left(\frac{Evento}{Tempo} \right) \cdot Impacto \left(\frac{Consequência}{Evento} \right) \quad (3)$$

O que deve estar claro é que o risco não possui uma medida única, já que a consequência analisada pode ser de diferentes naturezas, como financeira, fatalidades, entre outras. Kauer et al. (2002) citam as principais medidas de risco, dentre as muitas usualmente utilizadas, como sendo (i) risco à saúde ou segurança de um indivíduo ou público; (ii) risco ao ambiente; e (iii) risco a questões econômicas (como lucros ou prejuízos).

No caso da análise de sistemas complexos, a quantificação do risco pode envolver diversos aspectos, sendo mais conveniente expressar o risco total através de cenários de risco (KRISTIANSEN, 2005). A eq. (4) calcula o risco total de acordo com cada cenário e cada fase do acidente:

$$Risco \equiv \sum_i^{Nc} \sum_j^{Nf} p_{ij} c_{ij} \quad (4)$$

onde:

Nc é número de cenários que podem causar uma determinada consequência

N_f é o número de fases de uma consequência de acidente (ex. evento iniciador, mitigação, evacuação e resgate)

c_{ij} é a medida de consequência na fase j em um cenário i

p_{ij} é a probabilidade ou frequência da consequência c_{ij} , dado um cenário i e uma fase de acidente j

O perfil de risco de uma dada situação é resultado do que se chama de análise probabilística de risco. A análise probabilística de risco (do inglês, *Probability Risk Analysis* – PRA) é uma metodologia sistemática de avaliação de risco largamente empregada em sistemas complexos, utilizando a análise do sistema e conceitos de probabilidades para a avaliação do risco.

A PRA se inicia com a identificação de perigos e define o perfil de risco associado aos possíveis eventos iniciais de falha.

Entende-se como falha, um evento que implica a interrupção da capacidade de um sistema atender uma função requerida (GUIMARÃES, 2003). A gestão de risco envolve a prevenção da ocorrência de eventos iniciais de falha e/ou controle da propagação dos eventos iniciais e mitigação de consequências no interior e no exterior da planta. O processo de gestão de risco avalia os perfis de risco, propõe alternativas, e permite a tomada de decisões com foco na segurança, escolhendo alternativas para o controle do risco e ações corretivas.

Kumamoto e Henley (1996) consideram que a fase de análise probabilística de risco é mais científica, técnica, quantitativa e formal, ao passo que a fase de gestão de risco é mais subjetiva e qualitativa, envolvendo julgamento de valores, heurísticas e questões sociais e políticas. O resultado final do gerenciamento do risco é a decisão. Isto é, nem a análise probabilística nem o gerenciamento possuem fim em si mesmos, mas servem primordialmente como auxílio ao processo de tomada de decisão. Paté-Cornell (1996) afirma que a análise de risco é somente uma ferramenta de informação, e não leva a uma decisão ótima sem um julgamento de valores que reflita as preferências do tomador de decisão.

2.2. Atores da indústria naval e o conflito de interesses

There are two basic reasons for conducting an accident investigation: (1) to assign blame for the accident and (2) to understand why it happened so that future accidents can be prevented. When the goal is to assign blame, the backward chain of events considered often stops when someone or something appropriate to blame is found. (LEVESON, 2004, p. 4)

O risco pode ser enxergado ou interpretado sob diferentes perspectivas. Kumamoto e Henley (1996) apontam cinco diferentes pontos de vista, conforme mostrado na Figura 4.

Figura 4 – Os cinco pontos de vista do risco
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 19)

Quando se verificam especificamente os atores do cenário da indústria de construção naval e transporte marítimo, fica evidente que os interesses relacionados à gestão de risco e segurança nem sempre são harmoniosos. De fato, como será mais bem discutido posteriormente, a raiz de muitos acidentes está nas divergências de expectativas das partes envolvidas na construção e operação de uma embarcação.

Kristiansen (2005) descreve os atores essenciais desta indústria, apontando sua influência na segurança de um navio, conforme apresentado na Tabela 1.

Assim como em qualquer ramo de negócios, na indústria naval, cada parte envolvida, ou *stakeholder*, possui um objetivo particular, que pode ser conflitante em relação ao das outras partes envolvidas. O *stakeholder* pode ser definido como

sendo um dos participantes do negócio, investindo no risco da operação de um navio, podendo afetar ou ser afetado por um risco (KRISTIANSEN, 2005). Os conflitos existem, pois nem sempre quem impõe o risco é a parte que irá assumir este risco. Além disso, cada parte envolvida enxergará o risco e os custos e benefícios de forma diferente, avaliando cada fator com sua própria balança.

Tabela 1 – Atores da indústria que influenciam a segurança
- adaptado de (KRISTIANSEN, 2005, p. 4, tradução nossa)

Ator	Influência na segurança
Estaleiro	<ul style="list-style-type: none"> ▪ Padrões técnicos da embarcação
Armador	<ul style="list-style-type: none"> ▪ Decide o padrões e requisitos técnicos mínimos necessários ▪ Seleciona tripulação, ou empresa gestora da tripulação e operação ▪ Decide sobre políticas de segurança operacional e organizacional
Proprietário da carga	<ul style="list-style-type: none"> ▪ Paga pelo transporte da carga, e consequentemente, pela qualidade e segurança da embarcação ▪ Pode exigir avaliação independente da qualidade do prestador de serviço
Seguradora	<ul style="list-style-type: none"> ▪ Assume parte do risco em nome armador e do proprietário da carga ▪ Pode exigir avaliação independente da qualidade do prestador de serviço
Empresa gestora	<ul style="list-style-type: none"> ▪ Responsável pela tripulação, operação e manutenção em nome do armador
País de bandeira	<ul style="list-style-type: none"> ▪ Controla os padrões da embarcação, da tripulação e da gestão do transporte
Sociedade classificadora	<ul style="list-style-type: none"> ▪ Controla os padrões e requisitos técnicos em nome da seguradora ▪ Assume algumas funções de controle em nome do país da bandeira
Porto	<ul style="list-style-type: none"> ▪ Responsável pelas práticas de segurança no porto ▪ Pode controlar requisitos de segurança e negar acesso a navios sem requisitos necessários

Considere, por exemplo, uma empresa que deseja instalar uma refinaria em uma cidade perto da costa. Para a comunidade local (população), esta nova construção pode produzir efeitos positivos ou negativos, que a levarão a se posicionar contra ou a favor do empreendimento. Efeitos positivos seriam melhorias na infraestrutura do local, como novas ruas de acesso, ou novas linhas de transporte público. Ou mesmo o aumento da oferta de emprego na região. Por outro lado, a população pode rejeitar a obra por temer o aumento de poluição, desvalorização imobiliária, etc. Já para a empresa petrolífera, o risco do empreendimento possui

outros aspectos. A companhia pode estar visando o aumento da receita e participação no mercado, mas pode decidir abortar a construção devido ao alto risco de acidentes, ou por poder ter sua reputação manchada devido a uma provável poluição no local (KRISTIANSEN, 2005).

Outro exemplo é o eventual conflito que pode ocorrer quando se pratica a modalidade de negócios de preço de venda fechado, a qual tipicamente estabelece contratos entre armadores e estaleiros, baseados em uma especificação básica de segurança e um preço de venda pré-estabelecido. Uma vez definido o preço de venda de um navio, o estaleiro procurará os insumos e equipamentos de menor custo que atendam minimamente as especificações, a fim de maximizar a margens de lucro do negócio, em detrimento a possíveis melhorias na segurança da embarcação. A tripulação, por sua vez, possui pouco poder de decisão, e vê itens de conforto e segurança tratados com baixa prioridade. Nesta situação, a fiscalização das sociedades classificadoras idôneas e competentes é fundamental, a fim de que nenhuma norma seja descumprida por razões comerciais.

2.3. Análise de risco, IMO e sociedades classificadoras

Na comunidade naval, existem tentativas de se utilizar as metodologias de análise de risco como ferramenta na elaboração de novas regulamentações para segurança marítima e proteção ambiental. Assim como na indústria aeronáutica, aeroespacial ou mesmo nuclear, na indústria naval o objetivo da análise de risco e suas consequências é primordialmente se antecipar a novos acidentes, buscando identificar modos de falha e pontos de vulnerabilidades que ainda não foram pensados ou considerados em projeto. A possibilidade, ainda que remota, de consequências catastróficas, como a morte de seres humanos, não pode suportar somente a filosofia de se aprender com erros, mas deve pregar que a antecipação e prevenção de problemas inéditos são fundamentais para prevenção de acidentes.

Devido ao caráter internacional da indústria naval e de transportes marítimos, em 1948 a Organização das Nações Unidas (ONU) colaborou para a criação de uma agência especializada, chamada *International Maritime Organization* (IMO). A IMO se posiciona no topo da estrutura internacional de regulamentação da segurança

marítima, responsável por regras e convenções internacionais. Com sede no Reino Unido e com 169 estados membros, a IMO tem a função de atualizar a legislação vigente e adotar novas normas, através de reuniões com especialistas e membros de governos (IMO, 2010). A IMO tem a responsabilidade de criar normas e regras de segurança, visando as questões ambientais, legais e técnicas, mas não tem poderes para impô-las às empresas (KRISTIANSEN, 2005).

Dentre as regulamentações mais notórias, podem-se citar as convenções SOLAS (*Safety of Life at Sea*) cujo principal objetivo é estabelecer padrões mínimos para construção, equipamentos e operação de embarcações (IMO, 2004); MARPOL (*International Convention for the Prevention of Pollution from Ships*) que trata de aspectos ambientais do projeto e construção de navios (IMO, 2006); e o ISM Code (*International Management Code for Safe Operation and Pollution Prevention*) cujo objetivo é induzir as empresas do setor a criar um sistema de gestão comprometido com a qualidade e segurança (IMO, 2002). Este último estabelece procedimentos de SMS (*Safety Management System*) para a identificação de equipamentos e sistemas cuja falha repentina possa provocar uma situação de perigo.

Duas abordagens são predominantes entre as normas das sociedades classificadoras (SII; WANG; ELEYE-DATUBO, 2005):

- Abordagem prescritiva: as regras são baseadas em resultados da experiência de vários anos de operação. Estas regras e normas são muito úteis para servir como diretrizes para gerar um novo projeto de forma rápida, e servir como uma fonte de consulta familiar aos estaleiros.

Segundo Dias et al. (2007), as normas prescritivas estabelecem:

[...]diretamente requisitos e restrições sobre parâmetros e características dos navios e seus sistemas e componentes sem esclarecer as metas de segurança subjacentes. A suposição básica é que a segurança do navio estará garantida uma vez que todas as regras e regulamentos sejam cumpridos. (DIAS et al., 2007, p.8)

- Abordagem baseada em risco: são baseadas em “*safety cases*” e avaliações de risco. Algumas sociedades classificadoras já estão preparadas para prover classificação baseadas em risco, e já publicaram diretrizes sobre esta abordagem. Ver (ABS, 2000).

De fato, nos últimos anos, algumas organizações começaram a preferir a utilização de regras e normas baseadas em risco, ao invés de regulamentos prescritivos. Isso criou uma nova perspectiva para desenvolvimentos em modelagem de risco e métodos de tomada de decisão baseadas em risco. Segundo Wang et al. (2004), acredita-se na mudança da filosofia de “me fale o que fazer” para “mostre-me como fazer” ou “envolva-me neste processo”. Esta mudança é vista como positiva, pois certamente motivará o desenvolvimento de novas abordagens para a avaliação de risco e tomada de decisão.

Conforme descrito por Dias et al. (2007b), o início da utilização da análise probabilística de risco (PRA) como uma nova ferramenta científica para avaliação da segurança do transporte marítimo foi no começo da década de 1990, após a publicação, em 1992, do relatório do acidente do *ferry Herald of Free Enterprise*, ocorrido em 1987. Este relatório de análise, conhecido como *Lord Carver's Report*, motivou a utilização da avaliação formal de segurança (*Formal Safety Assessment – FSA*), baseada na PRA. Em 2002, a IMO publica uma diretriz em forma de uma metodologia para uso no processo de elaboração de regras (IMO, 2002a). Wang et al. (2004) mencionam que, no momento, uma das principais preocupações da FSA é a simplificação da abordagem e o estudo de caso para produzir mais diretrizes, com o intuito de facilitar a aplicação prática dos fatores humanos e organizacionais.

Algumas considerações relevantes a esta diretriz da IMO, intitulada “*Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process*”, estão destacadas abaixo:

- 1) Constata-se a importância de se realizar a análise com dados apropriados. No entanto, é sabido que na indústria naval, pelas próprias características do setor, a frequência de acidentes nem sempre é suficiente para prover uma amostra para cálculos estatísticos. Neste caso, recomenda-se utilizar técnicas que utilizam opiniões de especialistas, modelos físicos, simulações ou modelos analíticos. Trata-se de uma observação sensata, e torna viável muitas análises e estudos, uma vez que a obtenção de dados pode se tornar um processo muito custoso e demorado.

- 2) O documento dedica espaço para a discussão a respeito do elemento humano, “um dos fatores contribuintes mais importantes à causa e a prevenção de acidentes”. Menciona-se que o elemento humano deve ser tratado como parte de um sistema integrado (ver Figura 2, pág. 10), e deve ser considerado na FSA através de técnicas apropriadas, associado à ocorrência do acidente, causa básica ou influência.
- 3) Sugere-se que o modo aceitável de se incorporar o elemento humano à FSA é por meio de técnicas de análise de confiabilidade humana - ACH (do inglês, *Human Reliability Analysis* - HRA). Um guia para a utilização da ACH é apresentado em uma seção à parte, com conceitos e instruções práticas. O texto alerta que, apesar da ACH ter origem na indústria nuclear, a bordo de um navio o ser humano possui mais graus de liberdade para interromper o sistema, e, portanto, as técnicas de ACH devem ser adaptadas.
- 4) Também é mencionado que, na maioria das vezes, a análise qualitativa da confiabilidade e erros humanos é suficiente. No caso da necessidade de uma análise quantitativa, as técnicas de julgamento de especialistas é a mais indicada. Como alternativas a esta, as técnicas HEART (*Human Error Assessment and Reduction Technique*) e THERP (*Technique for Human Error Rate Prediction*) são também sugeridas. Nestes casos, deve-se considerar que:
 - a. uma estimativa aproximada da magnitude do erro humano é suficiente;
 - b. a quantificação do erro humano pode ser bastante efetiva para fins de comparação de cenários;
 - c. o nível de detalhes da análise deve ser compatível com o nível de detalhes da FSA;
 - d. existem inúmeras técnicas de análise de erros humanos, e a ferramenta escolhida deve ser compatível com as necessidades da análise.

Estas são quatro observações bastante lúcidas e realistas em relação à indústria naval. O estudo e aplicação das técnicas de ACH podem exigir

bastante rigor e fundamentação, uma vez que a modelagem do comportamento humano é objeto de grande discussão e controvérsia. Com estas considerações, a IMO impõe uma visão prática à aplicação das técnicas de ACH.

- 5) Reforça-se a necessidade de se analisar o custo-benefício e as opções de controle do risco (tema abordado a seguir na seção 2.6). Uma FSA pode ter um custo financeiro alto, no entanto, dada as proporções da consequência, o investimento pode ser justificado. O texto busca conscientizar o leitor de que o custo-benefício do processo é relevante para o resultado final, e que os objetivos da análise devem estar bem definidos desde o início.
- 6) O uso da FSA deve ser sempre consistente com o processo de tomada de decisão, servindo como uma ferramenta para facilitar a tomada de decisão de forma transparente, conforme pode ser visto no fluxograma da FSA proposto pela IMO na Figura 5. Isso reforça o argumento da seção 2.1, de que a análise de risco não é um fim em si mesmo.

Figura 5 – Metodologia da FSA
– adaptado de (IMO, 2002a, p. 15)

Os benefícios de se adotar a FSA como uma ferramenta de regulamentação são (WANG, 2006):

- Possuir um regime de regulamentação que trata todos os aspectos de segurança de forma integrada;
- Possuir uma maior relação custo-benefício;
- Utilizar uma abordagem pró-ativa, permitindo investigar os perigos que ainda não foram considerados nas análises passadas;
- Servir como uma base racional para tratar novos riscos devido à constante evolução tecnológica dos equipamentos.

O processo da FSA pode ainda ter um potencial maior que simplesmente colaborar com o processo de elaboração de normas. A FSA pode ainda ser explorada em um contexto mais amplo de projeto e operação de navios (WANG, 2006).

Segundo a ABS (*American Bureau of Shipping*), devido ao entendimento individual de cada parte interessada em relação à segurança, a análise/avaliação de risco tem a vital função de ser uma ferramenta racional de julgamento, se opondo a possíveis conflitos de interesse (ABS, 2000). Isso demonstra a importância desta ferramenta nos processos de tomada de decisão das sociedades classificadoras do setor naval. Estas são empresas, entidades ou organismos independentes que estabelecem padrões de projeto, construção e manutenção de embarcações. As normas destas classificadoras geralmente cobrem a parte de projeto de cascos, materiais, máquinas principais e auxiliares, instalações elétricas, sistemas de controle e equipamentos de segurança.

A ABS também publicou diretrizes para avaliação e análise de risco (ABS, 2000). Seu documento é bastante alinhado com as diretrizes da IMO, e também reforça a importância dos fatores humanos, indicando a ACH como a melhor abordagem para avaliar os erros humanos na FSA. Este relatório conclui que os métodos de análise quantitativa de risco e de levantamento de dados da indústria naval ainda estão engatinhando. Ainda levará algum tempo para que estes métodos ganhem um grau razoável de repetibilidade e confiança para serem utilizados como critérios de aceitação. Por isso, para atingir estes objetivos, a pesquisa e desenvolvimento relacionados às metodologias baseadas em risco e visando a segurança são essenciais.

2.4. O processo de análise de risco

A análise de risco é o processo de se calcular o risco de perigos identificados, levando em conta um determinado cenário, suas possíveis consequências e impactos associados a uma população exposta ao risco. A avaliação de risco é o processo que se utiliza da análise de risco para aperfeiçoar a segurança de um sistema através da redução do risco. A norma ABNT/ISO define avaliação de risco como sendo o processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco (ABNT ISO/IEC, 2005).

Vários autores apresentam metodologias de análise de risco, a maioria seguindo uma mesma sequência e estrutura, tais como ABS (2000), Ayubb (2003), Dias et al. (2007a), Kristiansen (2005), Kumamoto e Henley (1996), SAE (1996) e USCG (1997).

A Figura 6 apresenta um possível diagrama do processo de análise e avaliação de risco. A análise de risco inicia-se com a definição dos objetivos da análise, com a identificação de perigos e definição dos cenários de falha. Após a fase de identificação dos perigos, inicia-se a coleta de dados referente às falhas observadas, quando disponível. Em seguida, inicia-se a fase de análise de risco, que é o processo de estimar o risco qualitativa ou quantitativamente. A análise de frequência é feita para estimar as probabilidades de um acidente ou perigo ocorrerem. Em paralelo, a avaliação das consequências dirá quais os efeitos e consequências, caso o perigo identificado ocorra. Combinadas, a probabilidade de ocorrência e as consequências darão a medida do risco.

No processo de avaliação de risco, aplicam-se medidas de gerenciamento da integridade do sistema com o emprego de políticas de prevenção de falhas e mitigação de consequências. As opções de controle do risco devem ser escolhidas baseadas nos conceitos de tomada de decisão. A análise de custo-benefício, por sua vez, é uma ferramenta para avaliar se as medidas de segurança para controle de risco são justificáveis.

Um dos benefícios do processo de análise de risco é ser capaz de identificar deficiências no sistema que não são óbvias para os projetistas ou operadores. Em regra, o analista de risco é uma pessoa que não participou do projeto do sistema. Isso porque, o foco do projetista é sempre voltado para o sistema em

funcionamento, ou como o sistema “pode dar certo”. Já o analista de risco deve estar livre de qualquer vício ou linha de pensamento, focado em como o sistema “pode dar errado”.

Por fim, vale ressaltar que a análise de risco provê apenas informações e subsídios para o tomador de decisão. Nenhuma decisão pode ser tomada baseada somente na análise de risco, ou em um valor numérico isolado. A decisão deve ser sempre tomada levando em conta os resultados da análise de risco, mas também as preferências do tomador de decisão ou os valores de risco aceitáveis. A análise de risco por si só não determinará uma escolha (PATÉ-CORNELL; DILLON, 2006).

Figura 6 – Processo de análise e avaliação de risco
– adaptado de (KRISTIANSEN, 2005, p. 209)

2.4.1. Técnicas de análise de risco

Segundo Paté-Cornel e Dillon (2006), a análise de risco é especialmente útil para decisões que envolvem probabilidades de acidentes ou situações de perigo que podem resultar em fatalidades. Um ponto chave para o sucesso da análise de risco é a escolha do método adequado, ou da combinação destes métodos. Talvez, os métodos de análise de risco disponíveis na literatura possam ultrapassar uma centena. Se o foco da análise de risco é prover informações para os decisores, o método escolhido deve ser capaz de avaliar as consequências e cenários que interessam a estes. Alguns fatores são importantes para a escolha do método (ABS, 2000; USCG, 1997):

- A natureza do problema a ser analisado;
- Tipo dos resultados necessários;
- As diferentes partes do negócio (*stakeholders*) envolvidas;
- Os custos associados para a realização do processo de análise de risco;
- A disponibilidade de informações do problema analisado;
- Tipo do acidente que se deseja analisar.

O objetivo deve ser realizar a análise de risco no menor nível de detalhe possível que resulte nas informações necessárias e suficientes para os decisores. A situação onde o tomador de decisão faz escolhas baseadas em dados imprecisos ou limitados é tão ineficaz quanto a situação onde se apresentam dados desnecessários e modelos complexos demais. Uma análise superdimensionada irá não somente atrapalhar o tomador de decisão, como também consumir tempo e recursos financeiros da empresa.

Os resultados desejados também devem ser considerados na escolha de técnica de análise. Segundo ABS (2000), a maior parte das técnicas produzem as seguintes informações para o tomador de decisão:

- Lista das áreas potenciais de problemas;
- Lista de como estes problemas ocorrem;
- Lista de alternativas para a redução do potencial de cada problema;
- Lista de áreas que necessitam de análises posteriores;
- Priorização dos resultados.

A análise de risco com o foco na engenharia dos sistemas irá também prover a informação se o sistema é “suficientemente seguro” e definir prioridades nas ações de gerenciamento do risco, identificando pontos fracos que devem receber mais atenção e recursos.

A Figura 7 apresenta um resumo das principais técnicas de análise e avaliação de risco. Neste trabalho, não serão discutidas em detalhes estas técnicas, apenas quando estas apresentarem alguma particularidade relevante para o entendimento ou desenvolvimento.

Figura 7 – Principais métodos de análise/avaliação de risco
– adaptado de (ABS, 2000, p. 16)

Cada vez mais estas técnicas vêm sendo aplicadas no setor naval para aperfeiçoar as regulamentações e normas, através da criação de novas abordagens. ABS (2000) cita quatro áreas onde a avaliação de risco tem sido de real utilidade:

- Na identificação e proteção dos perigos (perigos à tripulação, ao ambiente, aos sistemas embarcados);
- Na melhoria das operações de navios (como recomendação de criação de programas de manutenção preventiva, treinamento para emergências);
- No uso eficiente de recursos (inclusive recursos humanos);

- Na criação e atendimento às normas de segurança (como a FSA – *Formal Safety Assessment*) (DIAS et al., 2007a).

2.4.2. Limitações do processo de avaliação de risco

Apesar do processo de avaliação de risco ser uma ferramenta poderosa de tomada de decisão, deve-se atentar ao fato de que este também possui algumas limitações, especialmente relacionadas às análises quantitativas. As limitações mais significantes giram em torno das incertezas nas informações: incertezas dos dados e dos modelos do sistema e nos métodos de análise (ABS, 2000).

A falta de dados estatísticos é provavelmente a limitação mais comum no setor naval, onde a frequência dos acidentes de larga escala é baixa. Por conta disso, é possível que um problema, o qual se deseja estudar, não possua dados estatísticos; ou não se ter recursos suficientes para a coleta destes dados; ou que a qualidade destes dados seja duvidosa. Ou ainda, no caso de um novo desenvolvimento (um novo tipo de navio ou um novo tipo de plataforma *offshore*, por exemplo) nem sempre os dados históricos de sistemas semelhantes são adequados.

Outra limitação comum é a incerteza dos modelos utilizados na análise. Isso ocorre pelo fato de ser necessário analisar sistemas complexos, e, por conseguinte, se elaborar modelos que incorporam simplificações e suposições. Nem sempre é possível realizar experimentos em escala real, ou utilizar simulações computacionais complexas. As simplificações também geram incertezas.

Paté-Cornell e Dillon (2006) classificam as incertezas em epistêmicas e aleatórias. As incertezas epistêmicas são aquelas relacionadas ao conhecimento do sistema, e podem ser reveladas através da opinião de especialistas, os quais podem discordar sobre determinada consulta. Estas poderiam ser reduzidas através do aumento do conhecimento do sistema e seus modelos, ou com a coleta de mais dados do sistema. As incertezas aleatórias não podem ser reduzidas, e correspondem à variabilidade do sistema não compreendida. Estas incertezas podem envolver:

- falhas no sistema técnico;
- erros humanos;

- acoplamentos de fatores do sistema técnico, ou dos erros humanos, ou de ambos.

Possíveis propostas para o tratamento das incertezas poderão ser encontradas em (PATÉ-CORNELL, 1996), a qual julga a necessidade da análise e detalhamento destas incertezas de acordo com cada caso.

Por outro lado, os métodos de análise, ou métodos de tomada de decisão, também não são perfeitos. Mesmo com dados estatísticos confiáveis, a decisão final pode não ser a melhor, se utilizados critérios ou métodos de tomada de decisão inadequados. Em todos os níveis, o processo de tomada de decisão pode envolver o tratamento de incertezas ou informações incompletas (WANG et al., 2004).

Kristiansen (2005) também cita a não consideração de fatores humanos e organizacionais como uma importante limitação de alguns métodos. Dada a enorme relevância destes fatores em acidentes, tanto como um fator causador como na mitigação das consequências, ignorar a influência da organização e dos erros humanos implica resultados incompletos. Normalmente, os fatores humanos e organizacionais são mais facilmente empregados em análises qualitativas, devido à dificuldade de se incorporar estes fatores de forma quantitativa. O modelo de análise que será apresentado nesta tese abordará justamente uma análise probabilística, que inclui a influência destes fatores.

Em (ABS, 2000), uma lista de problemas potenciais do processo de avaliação de risco é apresentada:

- Definição inadequada do escopo e objetivo da análise.
- Utilização de métodos quantitativos, quando seria suficiente utilizar métodos qualitativos.
- Escolha da técnica de análise não apropriada.
- Escolher obter resultados absolutos quando resultados relativos (comparativos) seriam suficientes.
- Não prover recursos ou dados suficientes.
- Estabelecer expectativas irrealistas.
- Descartar a importância das limitações do método e simplificações do problema.
- Utilizar os resultados de forma errada, como por exemplo, aplicar os resultados de uma análise para em um cenário diferente.

Ainda, é preciso também ter em mente que a análise de risco não avalia as preferências do tomador de decisão. A utilização dos resultados da análise de risco será empregada de acordo com o julgamento do tomador de decisão, ou ponderada através de uma função utilidade, quando em um contexto de um processo de tomada de decisão formal. Pode ocorrer que a análise de risco esteja desconectada das expectativas ou do perfil do tomador de decisão, e apesar de prover bons resultados e conclusões, estes podem ser questionados ou subaproveitados.

Desta forma, pode existir um paradoxo entre realizar uma análise de risco acessível e útil aos tomadores de decisão, ou realizar a análise de forma independente e sem influências no resultado, mas incorrer de receber um peso menor durante o processo de tomada de decisão.

O processo de análise probabilística de risco (PRA) possui também algumas limitações particulares. Primeiramente, muitos destes métodos foram desenvolvidos para a indústria nuclear. Embora eles sejam largamente aplicados em outras indústrias, deve-se ter o cuidado de fazer as adaptações pertinentes, ou explicitar as hipóteses adotadas. Além disso, caso não tenha sido feita a análise de risco no sistema técnico nas fases de projeto e construção, geralmente assume-se que o sistema em análise foi corretamente projetado, construído e operado. Assim, o analista irá pesquisar as falhas nas situações onde a solicitação excede a resistência descrita em projeto. Se o sistema foi corretamente projetado, este tipo de falha é raro, o que é impossível garantir. No entanto, esta suposição pode causar uma estimativa errônea da probabilidade de falha, e mascarar as oportunidades de melhoria na segurança do sistema (PATÉ-CORNELL, 2002).

Por fim, o processo de avaliação de risco também possui limitações devido às incertezas do sistema. Para expressar as incertezas, Guimarães (2003) utiliza os conceitos de domínio do conhecimento e do desconhecimento relativo ao funcionamento dos sistemas. O domínio do conhecimento compreende a região onde é possível descrever precisamente todos os estados de funcionamento e probabilidade de um modo de falha. O domínio do desconhecimento, ou ignorância, compreende a região onde não se sabe os estados de funcionamento do sistema, ou sobre seu ambiente. O domínio do conhecimento ainda é dividido em zona de certeza, onde se tem o conhecimento determinístico do sistema, e a zona de

incerteza, onde se tem apenas um conhecimento qualitativo do sistema. A Figura 8 ilustra estes conceitos.

Figura 8 – Domínios de funcionamento de um sistema
– adaptado de (GUIMARÃES, 2003)

Toda quantificação de probabilidades de risco deve ser feita sempre dentro do domínio do conhecimento. No entanto, Guimarães (2003) discute que atividades de engenharia podem ter ramificações no domínio do desconhecimento. Neste caso, o autor menciona que mais importante é a busca da melhoria dos níveis de segurança, e que nenhum método deve ser descartado “*a priori*”, mas devem-se utilizar os resultados qualitativos ou quantitativos criteriosamente, levando em conta as incertezas do processo. Isto é feito entendendo os resultados como indicadores comparativos, para hierarquizar riscos, ou priorizar os resultados qualitativos.

2.4.3. Análise de sensibilidade

Na apresentação dos resultados de uma análise quantitativa de risco, é desejável avaliar a sensibilidade da estimativa de risco associada a variações dos parâmetros críticos ou dos parâmetros que carregam alguma incerteza (por exemplo, obtidos via consulta à especialistas). A análise de sensibilidade é uma ferramenta importante neste aspecto. Esta permite avaliar o impacto de uma variável no modelo de análise como um todo, medindo a variação final do risco dada uma variação em um dos parâmetros adotados.

A sensibilidade se refere a quão sensível o modelo é em relação a pequenas variações dos parâmetros. O modo mais natural de se realizar esta análise é variar alguns parâmetros, e analisar a variação nas probabilidades posteriores do modelo. Esta irá apontar a robustez do modelo e eventualmente alguma discrepância em sua formulação.

A análise de sensibilidade é particularmente útil na investigação das incertezas de um modelo de análise probabilística de risco (REN et al., 2008). A IMO recomenda a análise de sensibilidade para se demonstrar os efeitos das incertezas em modelos envolvendo o comportamento humano (IMO, 2002a). A análise de sensibilidade também pode ser útil para demonstrar a efetividade de medidas de mitigação do risco. Por exemplo, se determinada medida de mitigação afetar a probabilidade de ocorrência de uma falha, alterando-se a probabilidade desta falha tem-se uma nova medida do risco. A análise de sensibilidade pode ajudar na decisão de aplicar ou não esta medida de mitigação, por exemplo, realizando uma análise do custo-benefício.

2.5. Análise probabilística de risco: abordagem pró-ativa

Identificar as potenciais fraquezas e eliminar as raízes das causas dos problemas antes que estes causem uma falha é o que Paté-Cornell (2002) denomina de abordagem pró-ativa de gestão de risco. Segunda a autora, é relativamente simples resolver problemas em sistemas bem conhecidos, operados por um longo tempo, com ampla informação dos mecanismos e histórico de falhas. Todavia, sistemas bem projetados, como vários sistemas concebidos para utilização na indústria naval, possuem taxas de falha muito baixas, e por isso, nem sempre existem informações estatísticas disponíveis.

Antecipar-se a problemas é algo extremamente desejável na indústria naval e de transportes marítimos devido ao grande potencial de consequências catastróficas. Na citação abaixo, a ABS menciona que não se pode suportar “aprender com os próprios erros”, e que os métodos preditivos aplicados na indústria naval, surgiram justamente da indústria nuclear.

Due to the huge perceived risks associated with accidents in the nuclear industry, it was acknowledged that more predictive methodologies must be used to set standards for the industry prior to wide-scale development of nuclear facilities. The potential consequences associated with nuclear incidents were too great to allow operators and regulators to “learn from their mistakes”. Many of the predictive risk assessment techniques applied within the marine and oil and gas industries today originated from the nuclear industry. (ABS, 2000, p 87)

Processos de avaliação de risco pró-ativos já são utilizados largamente em todo o mundo, e uma importante abordagem surgiu no campo da ergonomia e fatores humanos. Esta abordagem foca na redução pró-ativa da probabilidade de falhas. Estudos provaram que interfaces desenhadas com foco no operador, juntamente com os demais componentes e processos organizacionais aumentam a confiabilidade do sistema (WANG, 2006).

Considerando a gestão de risco na fase de projeto, Wang (2006) afirma que as decisões tomadas nos estágios iniciais de projeto exercem um impacto mais significativo no desempenho de uma embarcação, em relação àquelas decisões tomadas durante o ciclo de vida do navio. Assim, o objetivo da análise de risco pró-ativa nas fases preliminares de projeto é prover informações orientadas à segurança para o desenvolvimento do produto.

Como será apresentado nas seções seguintes, prever as probabilidades do comportamento humano e todos seus possíveis desvios não é algo que se possa realizar com precisão.

Uma das saídas para lidar com estas incertezas é a escolha de métodos qualitativos de análise e avaliação de risco. De fato, os métodos qualitativos são largamente empregados e produzem resultados satisfatórios para muitas análises. Entretanto, para fins da avaliação do risco de forma pró-ativa, os métodos qualitativos não são os mais adequados. Segundo Paté-Cornell (2002), os métodos qualitativos não permitem comparações entre cenários, avaliar as dependências entre cenários, ou classificação dos riscos.

A análise probabilística de risco (PRA), portanto, é o método mais adequado, geralmente empregando atualizações Bayesianas, incorporando as evidências disponíveis, quando informações estatísticas são inexistentes ou escassas. A abordagem Bayesiana permite a integração de diferentes fontes e a atualização das

probabilidades “*a priori*” e “*a posteriori*” utilizando o teorema de Bayes (PATÉ-CORNELL; DILLON, 2006).

Segundo a definição de NASA (2002):

Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance. (...) A foremost strength of a PRA is that it is a decision support tool. In safety applications, PRA helps managers and engineers find design and operation weaknesses in complex systems and then helps them systematically and efficiently uncover and prioritize safety improvements. (NASA, 2002, p. 1-2).

O principal objetivo da PRA é estimar as probabilidades de falha de sistemas complexos, para o qual não existem dados suficientes. A Figura 9 apresenta um fluxograma típico de uma PRA. Inicialmente, esta ferramenta foi desenvolvida para uso na indústria nuclear, mas posteriormente ganhou espaço em outras indústrias. “A PRA permite identificar as fraquezas do sistema, e é a forma mais efetiva de corrigi-las” (PATÉ-CORNELL, 2002, p.319). Será nesta linha que este trabalho abordará o problema de analisar o sistema de alarmes das embarcações, através da proposição de um modelo de análise, baseado em probabilidades condicionais.

Figura 9 – Fluxograma típico de uma PRA
– adaptado de (NASA, 2002, p. 44)

2.6. Critérios de aceitação do risco e análise custo benefício

“Segurança absoluta é uma utopia” (GUIMARÃES, 2003, p. 58)

Recapitulando o exposto anteriormente, a gestão de risco envolve a avaliação do risco aceitável e das alternativas para redução do risco associado ao sistema. Isso significa que nem sempre o risco pode ser totalmente eliminado. Neste caso, algumas estratégias para o tratamento do risco podem ser escolhidas:

- Evitar o risco (por exemplo, desistindo de um projeto).
- Controlar o risco (ou mitigar as consequências).
- Transferir o risco (por exemplo, contratando um seguro).
- Aceitar o risco (retenção do risco)³.

O risco só é dito eliminado quando não se expõe a ele. Caso contrário, deve-se reduzir-se o risco até uma condição aceitável. A aceitação de risco é um tema complexo e assunto de muitos debates (AYYUB, 2003). Todavia, determinar os níveis de risco aceitáveis é fundamental para que um sistema seja considerado seguro. A aceitação do risco depende principalmente da percepção da sociedade, e não exatamente do valor do risco.

Algumas razões para a aceitação do risco são (KRISTIANSEN, 2005):

- o risco é tão pequeno que pode ser ignorado;
- o risco é incontrollável e inevitável, e não causa nenhum impacto na sociedade;
- alguma organização com responsabilidade apropriada estabeleceu um limite aceitável de risco;
- historicamente, o nível de risco continua sendo aceitável;
- a redução do risco não é viável, no atual estado da técnica;
- o risco compensa dados os benefícios.

³ Retenção do risco é a aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco. (ABNT ISO/IEC, 2005)

Para situações fora destes casos, o conceito de critério de aceitação de risco pode ser utilizado. Critérios de aceitação de risco expressam o nível de risco tolerável de um sistema ou atividade. Podem ser tanto uma medida qualitativa quanto quantitativa. A literatura apresenta alguns métodos para se escolher o critério de aceitação de risco (AYYUB, 2003; SKJONG, 2002). Dentre elas, podem-se citar:

- Métodos de comparação (comparação de índices, comparação com outras indústrias ou outras atividades, etc.).
- Abordagem da matriz de risco.
- Curvas F-N (ver Figura 10).
- Efetividade do risco.
- Análise custo-benefício.
- ALARP.

Figura 10 – Exemplo de curva F-N
– adaptado de (KRISTIANSEN, 2005, p. 36)

Determinar o nível de segurança suficiente de um sistema não é uma questão simples. A maior parte das regulamentações existentes não menciona explicitamente os níveis de risco considerados aceitáveis ou toleráveis (ABS, 2000). Ou seja, é raro que organismos de regulamentação ou sociedade classificadora apontem quantas fatalidades ou acidentes são aceitáveis por ano em determinado tipo de embarcação, ou operação. Isso porque, surgiria campo vasto para

controvérsias e discussões morais e éticas que tirariam o foco do principal objetivo que é prevenir acidentes. Afinal, nenhum acidente é aceitável⁴.

Todavia, alguns países já publicaram valores aceitáveis para o risco para a indústria em geral (não específicos para a área naval):

Estados Unidos: A Tabela 2 apresenta valores anuais aceitáveis de risco individual e risco público.

Tabela 2 – Risco anual aceito pela sociedade nos Estados Unidos
(NASA, 2002, p. 7)

Risco Individual Anual	Risco Público Anual
Indústrias em geral: 7.0E-5	Doença do coração: 2.7E-3
Mineração: 2.4E-4	Câncer: 2.0E
Bombeiros: 4.0E-4	Veículos motorizados: 1.5E
Polícia: 3.2E-4	
Presidente dos EUA: 1.9E-2	

Holanda (KAUER, et al., 2002):

Riscos toleráveis ao indivíduo

Situações existentes: 10^{-5} fatalidades por ano

Situações novas: 10^{-6} fatalidades por ano

Riscos toleráveis à sociedade:

Uma ou mais fatalidades: 10^{-3} por ano

Inglaterra (KAUER, et al., 2002):

Trabalhadores: 10^{-3} fatalidades por ano

Público: 10^{-4} fatalidades por ano

Amplamente aceitável: 10^{-6} fatalidades por ano

Ainda na Inglaterra, o *UK Health and Safety Executive* (HSE), departamento governamental de segurança do Reino Unido, propôs valores para embarcações, conforme apresentado na Tabela 3 (HSE, 1999):

⁴ É possível encontrar na literatura autores que abordem a quantificação das consequências relacionadas à população, como fatalidades e deficiências permanentes e temporárias. Os custos associados estas consequências podem ser avaliados de acordo com parâmetros de seguros, indenizações, e encargos sociais. Também é possível encontrar métodos para cálculo de consequências relativas à poluição do ambiente. Estes temas não serão abordados neste trabalho. Para maiores detalhes, o leitor pode consultar (KRISTIANSEN, 2005).

Tabela 3 – Risco máximo tolerado para embarcações no Reino Unido
(KONTOVAS; PSARAFTIS, 2009)

Risco máximo tolerado	Frequência de fatalidades
para tripulação:	10^{-3} por ano
para passageiros:	10^{-4} por ano
para público em terra:	10^{-4} por ano
Risco desprezível	10^{-6} por ano

O conceito ALARP se mostra como sendo o mais utilizado para se buscar o equilíbrio do risco tolerável. O princípio ALARP (do inglês, *as low as reasonably practicable*) foi criado pelo *UK Health and Safety Executive* para prover uma direção na busca da redução do risco ao menor nível praticável, e, portanto, aceitável (KRISTIANSEN, 2005). A Figura 11 ilustra este princípio. Skjong (2002) menciona que, no setor naval, o R de ALARP deve significar “não desproporcional aos custos”. Neste sentido, Reason complementa o princípio ALARP com o princípio ASSIB (*And Still Stay In Business*) já que não é factível projetar um sistema ótimo em custo e segurança ao mesmo tempo (REASON, 1997).

O princípio ALARP implica realizar uma avaliação ou análise custo-benefício (CBA – *Cost-Benefit Analysis*), que é basicamente uma técnica de comparação de custos e benefícios de um projeto. A Figura 12 apresenta um exemplo de fluxograma para análise de risco e segurança, situando as funções dos critérios de aceitação de risco, e da análise custo benefício.

Figura 11 – Diagrama típico do princípio ALARP
– adaptado de (KRISTIANSEN, 2005, p. 247)

Figura 12 – Processo de análise de segurança aplicando critérios de aceitação – adaptado de (SSRC, 2003, p. 20)

Kristiansen (2005) aponta duas visões predominantes sobre a análise custo-benefício. A primeira leva em conta que, para qualquer sistema, haverá um limite econômico de quanto se pode gastar em segurança até que o sistema se torne economicamente inviável ou não competitivo. Implementar medidas de redução de risco pode aumentar a segurança e confiabilidade de um sistema, mas certamente existirá um preço financeiro a ser pago. Em determinado momento, o custo das medidas de segurança pode tornar inviável economicamente a operação de um navio. Deverá haver sempre um equilíbrio entre os custos de se implantar medidas de segurança e o nível de risco residual, o qual, não importa o esforço despendido, nunca pode ser completamente eliminado. A Figura 13 apresenta este conceito, onde o custo esperado da consequência é o valor probabilizado de determinada consequência. O custo esperado da medida de redução de risco é uma curva hiperbólica, onde um aumento marginal do custo da medida significa uma redução ainda menor da probabilidade de ocorrência. O ponto ótimo será o mínimo da curva da soma dos dois custos esperados.

A segunda visão leva em conta a ponderação entre implementar uma medida de segurança e os benefícios (redução do custo das perdas) obtidos através desta medida. Desta forma, busca-se o ponto ótimo entre os investimentos em segurança (custos) e a redução do custo das perdas. A Figura 14 ilustra este raciocínio.

Figura 13 – Equilíbrio entre custo versus consequência
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 24)

A fim de padronizar as formas de cálculo das análises custo-benefício alguns índices foram criados. Dentre estes os mais populares são: o custo por unidade de redução de risco (ou CURR – *Cost per Unit of Risk Reduction*), e o custo implícito de se evitar uma fatalidade (ou ICAF – *Implied Cost of Averting a Fatality*) (KRISTIANSEN, 2005). A Tabela 4 apresenta outros exemplos de medidas de risco utilizados no meio naval.

Figura 14 – Implementação ótima das medidas de segurança
– adaptado de (KRISTIANSEN, 2005, p. 252)

Tabela 4 – Medidas de risco no setor naval
(KRISTIANSEN, 2005, p. 33, tradução nossa)

Tipo		Nome	Definição
Acidentes ocupacionais:	LTI-Rate	Lost-Time Injury frequency rate	Número de tempo perdido devido a ausência médica por 10 ⁶ horas-homem de trabalho
	AIR	Average Individual Risk	Número de fatalidades por indivíduo exposto
	IIR	Injury Incident Rate	(Número de ferimentos)/(Número de trabalhadores) * 10 ⁵
	IFR	Injury Frequency Rate	(Número de ferimentos)/(Total de horas trabalhadas)*10 ⁵
	S-Rate	Severity Rate	Número de dias de trabalho perdido devido a ferimentos
	TRI-rate	Total Recorded Injury Rate	Número total de ferimentos registrados por 10 ⁶ horas-homem
		Número médio de dias perdidos	S-rate/LTI-rate
	FAR	Fatal Accident rate	Fatalidades por 10 ⁸ horas de trabalho
	PLL	Potential Loss of Life	
	AFR	Accident Frequency Rate	Número de acidentes / número de empregados relativos a 200.000 horas de trabalho
	ASR	Accident Severity Rate	Número de horas perdidas / número de empregados relativos a 200.000 horas de trabalho
	FSI	Frequency Severity Indicator	$FSI = \sqrt{\frac{AFR \cdot ASR}{1000}}$
Relacionados ao trabalho	WRD-rate	Work-related Diseases rate	Número de casos novos de doenças resultando em faltas por 10 ⁶ horas
		Sick leave percentage	Número de faltas por doença / número total de dias úteis
Poluição Perdas materiais		Taxa de emissão	Emissão em kg/m ³
		Taxa de perda	Acidentes por unidade de produção. Ex. colisões por 10 ⁵ milhas navegadas
		Coeficiente de perda	Navios perdidos/navios em risco
		Coeficiente de perda relativo	Coeficiente de perda / coeficiente de perda mundial

Em seu relatório sobre as diretrizes para avaliação formal da segurança, a IMO (2002a) sugere a utilização do ICAF para expressar a relação de custos com a segurança de vidas, nas formas do *Gross CAF* (*Cost of Averting a Fatality*), ou custo bruto de se evitar uma fatalidade; e do *Net CAF*, ou custo líquido de se evitar uma fatalidade (IMO, 2002). Estes podem ser definidos como:

$$Gross\ CAF = \frac{\Delta C}{\Delta R} \quad e \quad Net\ CAF = \frac{\Delta C - \Delta B}{\Delta R} \quad (5)$$

onde:

ΔC é o custo por embarcação da opção de controle de risco;

ΔB é o benefício econômico por embarcação resultante da implementação da opção de controle de risco;

ΔR é a redução do risco por embarcação, em termos de número de fatalidades evitadas, devido à opção de controle de risco.

Segundo Kristiansen (2005), a DNV (Det Norske Veritas), sociedade classificadora norueguesa, indica que medidas de redução de risco com um ICAF menor que 3 milhões de dólares podem ser consideradas eficientes pelo custo e devem ser implementadas.

O ICAF pode também ser encarado como os benefícios de se evitar uma fatalidade. De fato, conforme mencionado no início deste capítulo, vários problemas podem surgir quando se definem valores para a vida humana. Tome-se como exemplo a Figura 15, que apresenta o perfil de risco de um problema envolvendo fatalidades. Dentre várias alternativas, a fronteira das alternativas viáveis formam o que se chama de curva de Pareto. Nesta, as soluções serão equivalentes, e não é possível escolher qual delas é a melhor, por exemplo, a solução A ou B (KUMAMOTO; HENLEY, 1996).

Em outras palavras, pela eq. (1), página 13, as seguintes alternativas são matematicamente equivalentes:

- 100% de probabilidade de um acidente por ano com 1 fatalidade
(Risco = $100\% \cdot 1 = 1$)
- 10% de probabilidade de um acidente por ano com 10 fatalidades
(Risco = $10\% \cdot 10 = 1$)
- 1% de probabilidade de um acidente por ano com 100 fatalidades
(Risco = $1\% \cdot 100 = 1$)

Em casos como estes, a decisão será baseada na aversão/propensão ao risco do tomador de decisão, que levará em conta a percepção da consequência. A percepção da consequência por um indivíduo ou sociedade é estudada como “mecanismos de aversão ao risco”, que não serão abordados nesta tese. Ver (KUMAMOTO; HENLEY, 1996).

Figura 15 – Perfil de risco e curva de Pareto
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 24)

2.7. Perigos relacionados ao setor de transporte marítimo

A Figura 6 da subseção 2.4.1 mostra que o processo de análise de risco inicia com a identificação dos perigos relacionados ao sistema. A Figura 7 apresenta alguns métodos utilizados na identificação destes perigos, como o PrHA e o HAZOP. O objetivo desta sessão é apresentar alguns perigos inerentes às embarcações, à luz do que já foi publicado pela IMO e demais sociedades certificadoras.

Segundo Ayyub (2003), “perigo” é um ato ou fenômeno que impõe dano ou prejuízo a uma pessoa ou objeto e suas potenciais consequências. Outros autores definem perigo como “uma condição que é um pré-requisito para um acidente” (ERICSON, 2005). A IMO define perigo como sendo “uma ameaça à vida humana, propriedade ou ambiente” (IMO, 2002a). A norma ISO/IEC descreve perigo como sendo uma fonte potencial de dano (ISO, 1999). Para causar dano, o perigo deve interagir com pessoas ou objetos de forma prejudicial. Esta interação com pessoas ou com o sistema pode ser voluntária ou involuntária.

Outro conceito importante, que será utilizado adiante, é o de evento iniciador, que é o primeiro evento de uma sequência de eventos que conduz a uma situação de perigo ou a um acidente. A consequência será o elemento final da sequência de eventos.

Alguns exemplos relevantes relativos ao transporte marítimo são:

- Perigos a pessoas:
 - gases no ambiente, fontes térmicas, equipamentos elétricos;
 - ergonomia do espaço de trabalho;
 - erro humano.
- Substâncias perigosas em um navio:
 - roupas ou móveis, produtos de limpeza ou alimentos inflamáveis;
 - carga do navio;
 - combustíveis diversos para motores, caldeiras, aquecedores;
 - fluidos de lubrificação ou refrigerantes.
- Fontes de ignição:
 - curto-circuito, ondas eletromagnéticas;
 - faísca, fricção, superfície quente;
 - equipamentos eletrônicos, luzes;
 - equipamentos de limpeza (fero de passar, máquinas de lavar).
- Erros de projeto:
 - projeto estrutural subdimensionado.
- Perigos relacionados à navegação:
 - icebergs, mar revolto, correntes;
 - outras embarcações no mesmo canal;
 - objetos submersos e flutuantes;
 - obstáculos como pontes, boias, e estruturas *offshore*.

Esta lista contém alguns dos principais perigos citados por ABS (2000) e IMO (2002a). Esta última considera que as consequências mais graves relacionadas à atividade marítima são:

- ferimentos de pessoas ou fatalidades;
- impacto no público ou na imagem da empresa;
- impacto ambiental;
- perdas da embarcação ou danos à equipamentos;
- perdas da produção;
- impacto na operação.

A identificação dos perigos será mais eficiente quando aplicada no início do ciclo de vida do projeto. Uma vez identificados e compreendidos estes perigos, é possível seguir adiante no processo de avaliação de risco, buscando medidas e barreiras para prevenir que estes perigos encontrem um evento iniciador e propaguem para uma consequência severa.⁵

2.8. Métodos de consulta a especialistas

Na análise probabilística de risco, é comum a utilização de métodos de consulta a especialistas para suprir a falta de dados estatísticos do problema (do inglês, *Expert Elicitation Process* ou *Expert Opinion Elicitation*). O método de consulta a especialistas pode ser definido como um processo heurístico de coleta de informações, dados, ou respostas a perguntas relativas a um determinado problema ou questão (AYYUB, 2001). Trata-se de um processo formal para se obter informações sobre quantidades, probabilidades, entre outras, com passos e regras bem definidos, de forma a se ponderar os pesos de cada opinião e de cada tipo de especialista consultado.

Segundo Ayyub (2001), um especialista é uma pessoa qualificada que obteve um considerável treinamento e possui conhecimentos especiais sobre um assunto específico. A opinião de um especialista é definida por Ayyub como o julgamento formal de um especialista sobre uma questão; ou crença sobre uma questão cujas informações são incertas ou de pouco conhecimento. A opinião é sempre uma avaliação subjetiva, uma impressão sobre a quantidade ou qualidade.

A razão principal de se utilizar a consulta à especialistas é lidar com as incertezas de um sistema que se deseja avaliar. No contexto de análise de risco, especialistas podem julgar um evento utilizando um número de parâmetros sobre uma base subjetiva, e estes julgamentos podem ser sintetizados através de um processo racional (WANG et al., 2004). Os resultados, no entanto, conforme defende Paté-Cornell e Dillon (2006), não podem ser validados de forma estatística, mas

⁵ Uma lista completa e detalhada, com um *checklist* de vários perigos pode ser consultada em (ERICSON, 2005).

podem ser justificados pela boa compreensão do sistema, estrutura do estudo, e qualificação dos especialistas consultados.

Vários métodos formais podem ser encontrados na literatura, como o método de Delphi. Neste trabalho não serão discutidos estes métodos. Para maiores detalhes o leitor pode consultar Ayyub (2001).

A Figura 16 apresenta um fluxograma genérico de aplicação do processo de consulta à especialistas.

Figura 16 – Processo de consulta a especialistas
– adaptado de (Ayyub, 2001)

Os métodos de consulta à especialistas são largamente aceitos entre a comunidade naval. A IMO considera uma alternativa válida no processo de FSA, tanto para a estimativa de probabilidades relativas ao sistema como para estimativa de erros humanos (IMO, 2002a). Estes métodos são uma ferramenta importante, pois, como já comentado anteriormente, a falta de dados no setor naval é bastante comum, conforme citado por ABS: “dados de frequência de falhas de equipamentos de navegação para determinado tipo de navio são encontrados como amostras muito pequenas, resultando em um número que não é estatisticamente válido” (ABS 2000, p. 27).

Vários trabalhos sobre análise de risco para o setor naval empregaram estas técnicas, muitas delas utilizando lógica *fuzzy* para o processamento matemático das opiniões: Wang et al. (2004), Ren et al. (2008), SSRC (2003), Ward, Miles e Winterfeldt (2007), Aven, Hauge e Vinnen (2006), Celik, Lavasani e Wang (2010), Cebi et al. (2009), Celik e Cebi (2009), Sii, Wang e Eleye-Datubo (2005).

2.9. Análise de acidentes com embarcações

One reason for performing a risk analysis is to determine the accident sequences that lead to system failure and to remove, wherever possible, the weakest links of the system. Such systems changes usually lead to either improved plant availability or better protection of the capital investment in a plant. (MCCORMICK, 1981)

Safety is the sum of the accidents that do not occur. While accident research has focused on accidents that occurred and tried to understand why, safety research should focus on the accidents that did not occur and try to understand why. (WOODS; HOLLNAGEL; LEVESON, 2006)

2.9.1. Definições

Todos os esforços dos trabalhos focados em segurança são direcionados para o melhor entendimento dos acidentes, como eles ocorrem e porque eles acontecem. Como discutido até aqui, a análise de risco é uma ferramenta importantíssima, se não a mais adequada, para este fim. E principalmente a análise

probabilística de risco, a qual proporciona a obtenção de novas visões e conclusões a partir da modelagem da sequência de um acidente.

Kristiansen (2005) define acidente como “um evento indesejável que resulta em perdas ao homem, empresas ou ao ambiente.” Já IMO (2002a) define acidente como “um evento não intencional, envolvendo fatalidade, ferimentos, perda ou dano à embarcação ou a uma propriedade, ou ambiente”. Ainda segundo a IMO, um cenário de acidente é “uma sequência de eventos, desde o evento iniciador até um dos estágios finais”.

A palavra acidente pode englobar também outros conceitos. Desta forma, é importante distinguir dos conceitos:

- incidente: evento controlado antes que evolua a um acidente;
- não-conformidade: desvio das tolerâncias técnicas ou operacionais aceitáveis.

A análise de acidentes, depois de sua ocorrência ou a aplicação de modelos de análise baseados em acidentes ocorridos, pode ser vista como pouco eficaz, ou como uma medida mais reativa que pró-ativa. No entanto, os acidentes ocorridos são uma rica fonte de informações para contribuir com novos desenvolvimentos que visam à prevenção de acidentes. Kristiansen (2005) aponta que os objetivos das entidades que analisam acidentes são principalmente identificar causas e medidas potenciais de redução de risco em futuros acidente similares e identificar fraquezas nas regulamentações vigentes, de forma a continuamente aprimorar e reforçar as normas de segurança.

No setor naval, destacam-se como entidades que analisam e publicam seus relatórios de investigação (inclusive na internet):

- MAIB (*Marine Accident Investigation Branch*): localizada no Reino Unido, possui um vasto banco de dados “on-line” de relatórios de investigação, estudos e boletins sobre segurança. (MAIB, 2010)
- USCG (*United States Coast Guard*) *Office of Investigation Analysis*: departamento de análise de acidentes da guarda costeira Americana. (USCG, 2010)
- ATSB (*Australian Transport Safety Board*): órgão australiano também com extenso banco de dados on-line. (ATSB, 2010)

Os relatórios de investigação de acidentes geralmente contêm fotos e desenhos da embarcação e seus equipamentos, fontes de documentação, comunicados, documentação técnica dos sistemas, estudos especiais realizados, e transcrição de testemunhas, depoimentos, entre outras. Descrevem desde dados da embarcação, tripulação, e geografia do local, até a narrativa do acidente, sua análise, e conclusões e recomendações para o armador, tripulação e demais responsáveis.

2.9.2. Modelos de acidentes

Acidentes chegam sem aviso, e os inúmeros eventos ocorrem em espaços curtos de tempo, fazendo com que as testemunhas ou participantes tenham seus sentimentos e percepções distorcidas, dificultando a análise do que realmente aconteceu. Por conta disso, vários modelos de acidentes foram propostos e discutidos ao longo das décadas passadas.

O que se pode notar pela pesquisa na literatura é que os modelos de acidentes mais bem conceituados e citados utilizam uma abordagem sócio-técnica para explicar como os acidentes ocorrem, ou seja, os erros humanos são um aspecto chave no entendimento da sequência de um acidente ou propagação de uma falha.

Kumamoto e Henley (1996) propõem um modelo genérico de acidentes chamado de MACHINE (*Model of Accident Causation Using Hierarchical Influence Network Elicitation*). Esse modelo genérico, apresentado na Figura 17, assume que as causas diretas dos acidentes, apresentadas na camada de eventos, são combinações de erros humanos, falhas de equipamentos e eventos externos.

Kristiansen (2005) também apresenta alguns modelos de acidentes e de reconstrução de eventos. Dentre eles, o *Loss Causation Model* (LCM), cujo princípio é que todas as perdas ou problemas de segurança podem ser rastreados até a perda do controle pela gerência. Esse modelo foi desenvolvido por Bird e Germain (1992) do *International Loss Control Institute Inc.* (ILCI), e é a abordagem de gerenciamento de segurança promovida pela DNV (*Det Norske Veritas*). Os componentes do modelo, apresentados na Figura 18, são: perda do controle pela gerência, causas básicas e imediatas, incidente e perdas de pessoas ou de

propriedade. O primeiro elemento da cadeia é o que os autores chamam de “controle inadequado”, o que é uma inovação do modelo, pois coloca mais peso sobre a gerência que sobre os operadores.

Figura 17 – Modelo genérico de acidente
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 69)

Figura 18 – Modelo de acidente LCM
– adaptado de (KRISTIANSEN, 2005, p. 378)

Ren et al. (2008) também apresentam um modelo para avaliação de segurança baseado em fatores humanos e organizacionais. Eles propõem que as seguintes premissas podem ser consideradas sobre acidentes:

- Acidentes não ocorrem devido a uma causa única, mas são o resultado de uma combinação de falhas ou erros, ou uma cadeia de erros.

- Acidentes não são causados por uma ocorrência súbita de uma condição desfavorável, mas frequentemente são causados por fatores humanos e organizacionais que disparam um evento iniciador.
- Todos os acidentes possuem uma causa iniciadora e uma causa raiz.
- Os fatores de risco possuem uma natureza dinâmica, e a análise de risco deve ser capaz de refletir estas propriedades dinâmicas e lidar com informações dinâmicas.

O entendimento de Reason sobre acidentes organizacionais também é muito bem aceito nos trabalhos da área de análise de risco e confiabilidade, sendo uma literatura quase obrigatória no meio acadêmico. Reason (1997) afirma que os acidentes podem ser divididos em dois tipos:

- Acidentes individuais: são frequentes, com consequências limitadas, com poucas ou nenhuma barreira. Suas causas são limitadas e podem ser simplesmente um deslize, lapso ou um engano.
- Acidentes organizacionais: são raros, mas com consequências amplas. Podem ter várias causas e barreiras, envolvendo julgamento e decisão.

O modelo de acidentes de Reason é chamado de “modelo do queijo suíço”, onde as barreiras são as medidas que impedem que um perigo se propague para um incidente. Estas barreiras não são perfeitas, e possuem vários “buracos”, que são as falhas ativas ou latentes do sistema. Quando um perigo encontra um caminho entre buracos de todas as barreiras, o incidente ocorre.

Vários autores utilizam este modelo como base para modelos mais específicos, como, por exemplo, Mosleh e Dias (2004 apud DIAS et al., 2007b). Estes expandiram o modelo do queijo suíço de forma a explicitar o evento iniciador (ou evento gatilho), e as barreiras entre a causa e a condição perigosa, entre a condição perigosa e incidente, e entre incidente e consequências. Este modelo, ilustrado na Figura 19, se preocupa tanto com a prevenção do acidente, evidenciando as barreiras anteriores ao incidente, quanto com as medidas de contingência, as quais se referem à gestão do incidente, tanto no caso da perda da função simplesmente, quanto diante da ocorrência de danos.

Figura 19 – Modelo da corrente causal para análise de perigo e trajetória de incidentes através de barreiras – adaptado de (DIAS et al., 2007b, p. 9)

Nem sempre é óbvio introduzir barreiras que evitam que um perigo evolua para um acidente. Na realidade, as falhas acopladas estão entre as deficiências que mais requerem uma análise sistemática do risco para serem descobertas. Estes acoplamentos podem ser:

- Acoplamento funcional: quando o sistema A fornece as condições sob as quais o sistema B deve funcionar. Se A falha, B pode não atingir seu funcionamento, pois as condições de operação estão fora do limite de projeto de B. Se A falha, B falha em sequência.
- Acoplamento por unidade comum: os sistemas A e B possuem uma mesma unidade que permite o funcionamento de ambos, por exemplo, mesma alimentação elétrica.
- Acoplamento por proximidade: o elemento A falha, e por consequência, B também falha por estar perto de A. Por exemplo, uma bomba d'água de emergência pega fogo durante um incêndio, e a bomba reserva, no mesmo compartimento, também falha.

- Acoplamento humano: são dependências introduzidas por atividades humanas, como erros de omissão ou comissão. Exemplo, um operador interpreta um alarme erroneamente, e por isso realiza um comando que não deveria.

O modelo de Reason aborda vários aspectos relacionados aos fatores humanos e organizacionais, e por isso, será discutido em maior profundidade no capítulo seguinte.

3. ERROS E FATORES HUMANOS

“Errar é humano...”
Alexander Pope – poema “Ensaio sobre a crítica”

“...entender as razões pelas quais o ser humano erra é ciência.”
(HOLLNAGELL, 1993b, p. 1)

Tendo-se o conhecimento técnico adequado, o projeto em si de um sistema ou equipamento nem sempre é uma tarefa complexa. E mesmo nestas situações, após o produto construído, há casos em que se percebe que nem todos os requisitos de projetos são atendidos. Dentre as inúmeras causas que este problema pode ter, uma delas, em especial, é não prever a interação do ser humano com o equipamento, ou não considerá-lo como uma parte integrante do sistema. A abordagem sócio-técnica defende que o ser humano também deve ser objeto de requisitos de projeto (HOLLNAGEL, 1998).

Considerando que o objetivo de uma embarcação é realizar uma missão, seja esta o transporte de carga ou passageiros, o sistema em questão é, portanto, um sistema sócio-técnico, do qual o homem é um componente. E ainda, sob o aspecto do número de falhas é talvez o componente mais importante, conforme já apresentado na introdução desta tese.

Este capítulo irá abordar conceitos gerais e fundamentais para a composição do modelo de análise de risco a ser apresentado posteriormente. Serão introduzidos os conceitos de erro humano, sistema sócio-técnico, e a base teórica para o entendimento dos modelos do comportamento humano. Também serão discutidos os motivos para se considerar o ser humano como peça chave para uma análise de risco abrangente, e apresentadas algumas técnicas para classificar e quantificar a probabilidade de ações humanas errôneas.

3.1. Conceitos básicos

3.1.1. Sistemas sócio-técnicos

A abordagem sócio-técnica é importante no sentido de considerar tanto o sistema técnico quanto as questões relacionadas aos fatores humanos, uma vez que o foco desigual em uma ou outra parte pode conduzir a um resultado irreal de uma análise de risco. Trata-se de uma visão bastante aplicável para os problemas relacionados às análises de risco na área naval, uma vez que o sucesso da missão de um navio depende tanto das máquinas quanto da tripulação.

A noção de sistema sócio-técnico teve origem no final da década de 1950, no contexto de estudos laborais, no Instituto Tavistock de Londres (TRIST; EMERY, 1960). Um sistema sócio-técnico pode ser definido como tendo duas partes (ou dois subsistemas): a parte técnica, que são as máquinas, processos e arranjos físicos; e a parte social, que inclui as pessoas, seus hábitos, valores, estilos e relações comportamentais (ROPOHL, 1999). Teorias e estudos organizacionais se concentram na área de administração, e um dos princípios da Escola Sócio-Técnica é que a organização é um sistema que interage com o meio ambiente e busca a melhor combinação entre os sistemas técnicos e sociais, a inter-relação entre a empresa e o seu ambiente (GOMES; BORELLI; NAZARÉ, 2009). Este princípio pode ser visto como bastante aplicável ao setor de construção naval e transporte marítimo, já que a abordagem técnica considera apenas que o ser humano é um usuário do sistema.

Hollnagel (1998) considera que, em um sistema sócio-técnico, o desempenho humano é um compromisso entre as demandas da tarefa a ser executada e os recursos e restrições do ambiente de trabalho, ou seja, do contexto organizacional. Em outras palavras, a tarefa executada pelo operador impõe uma demanda de desempenho, e este desempenho é influenciado pela organização. Surge então a divisão das pessoas no “*sharp end*” e no “*blunt end*”. As primeiras são as pessoas que trabalham interagindo com o processo, como a tripulação de um navio. Estas pessoas estão diretamente expostas aos perigos existentes na planta; as pessoas no “*blunt end*” são as pessoas responsáveis pelas condições de trabalho das

peessoas do “*sharp end*”, mas ficam isoladas do processo, como gerentes, projetistas, fornecedores, e fiscais.

Apesar de esta abordagem ter contribuído para o avanço do estudo do erro humano, ainda existem lacunas a serem preenchidas com novos desenvolvimentos nesta área, como será tratado adiante neste capítulo.

3.1.2. Fatores Humanos

The maritime system is a people system. (ROTHBLUM, 2000, p. 1)

O termo fatores humanos, também conhecido como engenharia humana, ou engenharia dos fatores humanos é a aplicação das ciências comportamentais e biológicas ao projeto de máquinas e sistemas homens-máquina (SHERIDAN, 2002). Em outras palavras, fatores humanos compreendem o conjunto de interações entre pessoas e máquinas, pessoas e procedimentos, pessoas e o meio ambiente e entre pessoas e pessoas.

Não raro o termo ergonomia é utilizado como sinônimo de fatores humanos, no entanto, o estudo da ergonomia aborda mais aspectos biomecânicos e cinemáticos do corpo, ao passo que os fatores humanos lidam primordialmente com aspectos cognitivos e sensoriais.

A aplicação do conceito de fatores humanos no projeto e operação de um navio significa levar em consideração as habilidades e capacidades humanas, bem como suas limitações e necessidades. Squire (2005) considera que a disciplina de Fatores Humanos possui três subdomínios:

- engenharia de Fatores Humanos: que aborda a integração do ser humano na especificação, projeto e análise de um sistema, a fim de otimizar o desempenho do sistema homem-máquina;
- segurança de Sistemas: que estuda a contribuição humana ao risco do sistema;
- perigos à saúde: que envolve a identificação, avaliação e remoção ou redução de perigos relacionados à saúde das pessoas.

A norma ISO/DIS 8468, que trata do projeto de pontes de comando de navios, reconhece a importância de levar em consideração os fatores humanos e ergonomia. No entanto, propõe que a técnica FMEA (*Failure Mode and Effect Analysis*), uma técnica de análise de risco de sistemas, seja utilizada para documentar as limitações do projeto, incluindo o elemento humano (ISO, 2006).

Squire (2005) e Kristiansen (2005) listam os seguintes fatores humanos relacionados à área naval:

- Habilidades pessoais: competência, experiência, liderança, consciência situacional⁶.
- Diferenças Culturais: religião, tradições culturais, linguagem.
- Motivação: carga de trabalho, remuneração, benefício, ambiente de trabalho.
- Conhecimento: educação, treinamento.
- Estado físico: saúde, higiene, estresse, alimentação, fadiga.
- Capacidade física: força, fadiga, vibração, visão noturna, vigilância.
- Estado psicológico: Carga de trabalho, tédio, distrações, ameaças.
- Capacidade psicológica: Percepção, memória, carga de informações.
- Equipamentos e projeto do espaço de trabalho: usabilidade, interfaces homem-máquina, iluminação, vibração, ruídos, projeto do espaço de trabalho, ferramentas, equipamentos, acessibilidade,
- Gerência: políticas de segurança, alocação de recursos, planejamento financeiro.
- Empregados: seleção de trabalhadores, supervisão, clima social, treinamento.
- Operacional: métodos de inspeção, manutenção, documentação.
- Técnico: monitoramento, automação, interface homem-máquina.
- Gerência de Segurança: rotinas, manutenção, auditorias, políticas.

Por esta lista, vê-se que a automação (que engloba o sistema de alarmes) também está relacionada com os fatores humanos, uma vez que aspectos como a

⁶ Consciência situacional, do inglês *situation awareness*, é uma expressão comum na área de fatores humanos, e significa a habilidade de um indivíduo de estabelecer um modelo mental de algo ocorrendo em um determinado período, e também fazer projeções sobre como a situação se desenvolverá (HETHERINGTON; FLIN; MEARNES, 2006).

interface, grau de automação, necessidade de qualificação para operar o sistema devem prever a interação com o operador.

Squire (2005) ainda lista seis fatores humanos considerados fundamentais para a operação segura e efetiva de um navio:

- Habitabilidade (*Habitability*): provisão de acomodações adequadas e confortáveis;
- Manutenibilidade (*Maintainability*): provisão de condições adequadas para ações de manutenção rápidas, seguras e efetivas;
- Trabalhabilidade (*Workability*): ou capacidade para o trabalho – considera a provisão de condições para que os recursos, como equipamentos e ferramentas, possam ser utilizados adequadamente;
- Controlabilidade (*Controllability*): considera que o projeto do sistema de controle, comando, e maquinários permitam a apropriada capacidade de controle do navio;
- Manobrabilidade (*Manoeuvrability*): considera que os equipamentos de propulsão e timoneria permitem uma capacidade de manobras adequada;
- Sobrevivenciabilidade (*Survivability*): provisão de sistemas adequados de combate a incêndio e salvação para garantir a segurança da tripulação e passageiros.

Em suma, a aplicação do conceito de fatores humanos envolve a compreensão das capacidades e limitações humanas, e estes fatores devem ser considerados no projeto e na operação de um sistema, assim como políticas e procedimentos organizacionais. A IMO reconhece que os fatores humanos são um dos fatores contribuintes mais importantes em acidentes marítimos, e recomenda sempre incorporar seus princípios nas análises formais de risco (IMO, 2002a).

3.1.3. Erro Humano

Human errors are diverse and no single model can deal with every possible aspect of human behaviors. (KUMAMOTO; HENLEY, 1996, p. 498)

O estudo das ações humanas errôneas segue tradicionalmente duas linhas de abordagem (HOLLNAGEL; KAARSATD; LEE, 1999). A primeira se concentra na área de “psicologia do erro”, e busca estudar, através de análises retrospectivas, as prováveis causas do erro humano. Esta abordagem utiliza modelos derivados dos fatores humanos clássicos, modelos de processamento de informações, engenharia cognitiva e modelos sócio-técnicos, como o modelo de Reason (REASON, 1997).

A segunda linha de abordagem se preocupa com a predição das ações humanas errôneas, tanto na forma qualitativa quanto na forma quantitativa. Esta abordagem se encaixa no domínio da Análise da Confiabilidade Humana (ACH). Hollnagel, Kaarsatd e Lee (1999) apontam que a abordagem retrospectiva é mais utilizada no meio acadêmico, onde se formulam teorias, modelos e experimentos sobre o erro humano. A abordagem preditiva é de natureza mais pragmática, enfatizando dados e métodos. Para os problemas práticos de projeto, operação e manutenção, Hollnagel, Kaarsatd e Lee (1999) consideram que a grande necessidade é de métodos aplicáveis em vez de teorias elegantes.

O primeiro passo do estudo do erro humano é definir precisamente alguns termos e conceitos, para que estes não sejam confundidos com seu significado popular.

Formalmente, Reason (1990a) define erro humano como “um termo genérico para englobar todas as ocasiões em que uma sequência mental planejada ou atividade física falha em atingir o resultado esperado.” Hollnagel (1993) prefere distinguir uma ação errônea de um erro humano. A ação errônea é uma ação que não produz um resultado esperado, e que produz uma consequência indesejada. Uma ação errônea pode ocorrer mesmo quando a intenção da ação for adequada, mas falha em atingir o resultado esperado. Já erro humano pode ser utilizado para significar a ação, a intenção e o resultado. Em outras palavras, erro humano é uma ação que não atende a algum limite de aceitabilidade conforme definido para um sistema. Pode ser uma ação física (abrir uma válvula); ou uma ação cognitiva (diagnóstico de falha ou tomada de decisão).

Filgueiras (1996) comenta que a definição de Hollnagel é mais abrangente, pois define erro não apenas olhando para o resultado da ação (certo ou errado), mas também para sua consequência (desejada ou indesejada).

Apesar de concordar com a visão de Hollnagel (1993), nesta tese utilizar-se-á apenas o termo “erro humano”, termo mais usual nas publicações sobre o assunto.

3.1.3.1. Modelos do comportamento humano

Com o objetivo de se prever o comportamento humano, avaliar seu desempenho, simular situações e mesmo compreender o funcionamento da mente humana, foram criados modelos de atividade humanas (FILGUEIRAS, 1996). Alguns destes modelos são baseados em dados empíricos de experimentos realizados em laboratórios de psicologia. Outros são baseados em observações de atividades reais. Estes modelos serviram como alicerce para a criação das técnicas de análise da confiabilidade humana:

- Modelo GOMS – *Goal, Operators, Methods, Slection, Rules*: que é um modelo do processador humano. (CARD; MORAN; NEWELL, 1983)
- Modelo COCOM – *Contextual Control Model*: é o modelo utilizado no método CREAM, e será apresentado mais adiante neste capítulo. (HOLLNAGEL, 1993a)
- Modelo de Rasmussen ou SRK (*Skill-Rule-Knowledge*). (RASMUSSEN, 1983)

O modelo de Rasmussen é um dos modelos de cognição humana mais citados na literatura. Este modelo cognitivo de resolução de problema nasceu em 1974 de estudos de protocolos verbais de técnicos, que trabalhavam com resolução de problemas em equipamentos eletrônicos, e é capaz de modelar o conhecimento usado pelo operador quando ele está tentando resolver um problema. Os três níveis de desempenho propostos por Rasmussen acabaram se tornando um padrão de referência dentro da comunidade que estuda confiabilidade humana (REASON, 1990a). Cada nível de desempenho corresponde ao nível de familiaridade do operador com o ambiente ou tarefa:

- Nível baseado em habilidades (*skill-based*): corresponde ao desempenho governado por padrões armazenados pré-programados. A ação se dá automaticamente após o reconhecimento da situação, de forma inconsciente e sem envolvimento de raciocínio. O comportamento é derivado da repetição da atividade, o que gera a habilidade de responder rapidamente na presença de um estímulo. Erros, neste nível, estão relacionados com a coordenação da variabilidade de força, espaço e tempo.

- Nível baseado em regras (*rule-based*): corresponde ao desempenho na resolução de problemas familiares, governados por regras armazenadas do tipo “se-então” (*if-then*). A ação é determinada após o diagnóstico do estímulo. Este nível é ativado quando o estímulo não é suficientemente simples para uma ação reflexa. Erros neste nível são associados a classificação errada das situações implicando a aplicação da regra errada ou a lembrança errada dos procedimentos.
- Nível baseado em conhecimento (*knowledge-based*): compreende ao que se entende por resolução de problemas. Este nível se torna ativo frente novas situações ações que precisam ser planejadas, e requerem análise ou tentativa e erro. A análise consciente dos processos, os conhecimentos pré-existentes, experiência e criatividade são utilizados. Os erros surgem devido à limitação de recursos: conhecimento incompleto ou incorreto.

A Figura 20 apresenta uma visão simplificada dos níveis de desempenho humano. Segundo Filgueiras (1996), este modelo é interessante para a análise de confiabilidade humana, pois estabelece uma forma de se compreenderem as causas de erro humano, já que elas estão relacionadas às fases do processamento humano de informações.

É válido observar que em processos de risco, quando existem procedimentos que prevêm situações de acidentes, o operador bem treinado pode utilizar o atalho de associar o estado com a tarefa, e as fases de identificação, decisão e planejamento são simplificadas. Outro atalho possível é entre a percepção (extrair características) e ação, no nível do desempenho baseado em habilidades. Um exemplo comum deste atalho é quando um motorista pisa no freio ao visualizar um farol vermelho.

Tipicamente, um sistema de alarmes nas embarcações auxiliará nos processos do lado esquerdo da Figura 20: percepção, reconhecimento e avaliação. Desta maneira, contribui com informações para a tomada de decisão do operador.

Figura 20 – Três níveis de desempenho do operador humano
– adaptado de (RASMUSSEN, 1983, p. 258)

3.1.3.2. Classificação dos erros humanos

O termo **erro**, de forma genérica, é empregado para designar um estado que se desvia do esperado. Já o termo **falha** se refere a uma causa hipotética do erro. Uma falha pode ser classificada como ativa, quando esta pode causar um erro, ou dormiente (latente) quando esta não causa erros. Já uma **disfunção** (do inglês, *service failure*) ocorre quando o sistema entrega um serviço diferente do esperado, ou seja, o sistema não cumpre sua função ou sua especificação não descreve adequadamente a função do sistema. A Figura 21 apresenta a sequência de propagação de uma falha.

Figura 21 – Sequência de propagação de uma falha

Os erros humanos são ações humanas que podem levar a uma disfunção do sistema, e podem se tratar tanto de uma omissão (a pessoa não faz o que deve)

quanto de uma comissão (a pessoa faz o que não deve)⁷. A Tabela 5 apresenta a classificação de três tipos primários de erro humano, conforme a classificação de Reason (1990a), denominada GEMS (*Generic Error-Modeling System*). Para cada tipo primário de erro, associam-se o respectivo estágio cognitivo e o nível de desempenho segundo o modelo de Rasmussen.

Tabela 5 – Classificação dos tipos primários de erro (REASON, 1990a)

Estágio cognitivo	Tipo de erro primário	Nível de Desempenho
Planejamento	Engano	Nível de conhecimento
Planejamento	Engano	Nível de regras
Memória	Lapso	Nível de habilidade
Execução	Deslize	Nível de habilidade

Enganos são ações intencionais não apropriadas às circunstâncias, ou seja, são erros que ocorrem como resultado de ignorância da tarefa correta ou da maneira correta de realizá-la. Deslizes e lapsos são erros que ocorrem como resultado de esquecimentos, hábitos, fadiga ou causas psicológicas similares. Comparado com enganos, a intenção é correta, mas não é atendida.

A Figura 22 apresenta uma curva, posicionando os tipos de erros de acordo com a classificação de Reason (1990a).

Figura 22 – Tipos de erros de acordo com GEMS de (REASON, 1990a)

⁷ Não existe disfunção humana nas concepções sócio-técnicas.

A Figura 23 apresenta um diagrama resumindo as definições de enganos, lapsos, deslizes e violação. Uma violação ocorre quando intencionalmente não se executa uma ação prevista no regulamento, ou seja, existe a intenção de errar. Violações (sabotagens) são sempre intencionais, de origem motivacional e só podem ser entendidas no contexto social. Para se reduzir erros por violação, o foco deve ser adequar a cultura de segurança da empresa. Erros por violação não serão tratados neste trabalho.

Figura 23 – Fontes do erro humano
– adaptado de (REASON, 1990a)

3.1.3.3. Classificação dos erros humanos para a PRA

Kumamoto e Henley (1996) propõem uma divisão dos erros humanos à luz de um processo de análise probabilística de risco. Esta classificação é útil para o levantamento dos erros humanos, antes e depois do evento iniciador.

Quando ocorridos antes dos eventos iniciadores, os erros humanos podem ser (i) erros de teste e manutenção, que ocorrem em condições controladas, antes do evento iniciador; ou (ii) a causa do evento iniciador, ocorrendo nos momentos de maior intervenção humana, como durante partidas e paradas de equipamentos.

Para os erros durante um acidente, os erros humanos podem ser relacionados a procedimentos de emergência e de recuperação do sistema. A Figura 24 apresenta uma árvore de eventos (do inglês, *Event Tree*, ou ET), chamada de árvore de ação do operador (OAT – *Operator Action Tree*) durante um acidente,

relacionando as possíveis tarefas do operador aos tipos básicos de erro (lapso, deslize, engano).

Figura 24 – Árvore de ação do operador
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 473)

Uma árvore de eventos, como a da Figura 24, é logicamente equivalente a um diagrama de sequência de eventos (ESD – *Event Sequence Diagram*). Segundo NASA (2002), a árvore de eventos relaciona mais diretamente a quantificação dos cenários de acidentes. No entanto, o diagrama de sequência de eventos facilita o pensamento e entendimento do problema.

3.1.4. Fatores organizacionais

O termo “Fatores Humanos e Organizacionais” (FHO) ou HOF (*Human and Organizational Factors*) é frequentemente encontrado na literatura e agrupa em um só termo tanto os aspectos relacionados aos fatores humanos, já discutidos anteriormente, quanto aos aspectos relacionados à organização. O termo “fatores humanos e organizacionais” também pode ser encarado como uma expansão do termo “fatores humanos”, pois ao longo do tempo percebeu-se que não apenas o

estudo do comportamento do indivíduo era suficiente, mas que a organização tinha um papel igualmente importante, influenciando diretamente este comportamento e o sistema técnico em si.

Ren et al. (2008) consideram que as causas de acidentes marítimos residem na complexidade das relações entre o projeto, procedimentos, equipamentos, ambiente, operação, etc. Esta complexidade de relações exige uma abordagem ampla que contemple todas as entidades que compõem o sistema e suas inter-relações, incluindo as organizações e empresas envolvidas.

Assim, o conceito de FHO é extremamente amplo, e abrange as pessoas não apenas da tripulação, mas também projetistas, fornecedores, gerentes, equipes de manutenção, pessoal de suporte, recursos humanos, e assim por diante. Ou, conforme Hollnagel (1998), os que ficam no “*sharp end*” e no “*blunt end*”.

Especificamente na área naval, o número de tripulantes, qualidade e quantidade de treinamentos, políticas organizacionais, turnos de trabalho, estilo de gerência, cultura de segurança, e comunicação interna são exemplos de fatores organizacionais.

No entanto, a análise de risco de forma holística de um sistema como um navio, principalmente avaliando os FHO, apresenta algumas dificuldades (REN et al., 2008):

- ainda não existe uma definição exata de FHO, portanto, pode ser discutível o limite dos inúmeros fatores que se encaixam sob o termo FHO.
- a mensuração dos FHO é complexa, pois o que medir e determinar como estes fatores se inserem em uma metodologia de análise não é trivial.
- não existem dados empíricos disponíveis, e é extremamente difícil obtê-los da indústria.
- a elaboração de uma metodologia genérica e uniforme que avalie os FHO é igualmente complexa, e não é possível abordar a influência dos FHO com as técnicas de análise convencionais.

Apesar dessas dificuldades, sob o ponto de vista do resultado da análise de risco, a análise dos fatores organizacionais é extremamente importante e útil, pois permite aos gestores avaliar quais fatores especificamente exercem maior influencia

sobre este ou aquele desempenho. Controlar ou ajustar estes fatores organizacionais, na forma de políticas internas e medidas de segurança, permite influenciar os operadores e modificar o risco de determinado sistema.

Para maiores detalhes sobre fatores organizacionais, o leitor pode consultar (SCHÖNBECK, 2007), onde é apresentada uma extensa e detalhada revisão bibliográfica sobre modelos de análise de risco que incorporam os fatores humanos e organizacionais.

3.1.4.1. O modelo de Reason

O modelo de Reason teve sua origem em 1987 durante a redação do livro *“Human Error”* (REASON, 1990a). A intenção original deste livro era discorrer sobre a natureza, variedades e fontes mentais do erro humano, sob a perspectiva da psicologia cognitiva (REASON; HOLLNAGEL; PORIES, 2006). Baseado na teoria do comportamento humano e das organizações, James Reason (1990a), professor de psicologia na Universidade de Manchester, propôs o modelo do “queijo suíço”, apresentado na Figura 25, que demonstra quão genericamente os FHO podem se apresentar, decompondo-se em categorias lógicas, mutuamente exclusivas, cada qual influenciando a próxima. No modelo de Reason, cada fatia de queijo representa uma barreira de segurança relevante para um determinado perigo. Os buracos representam as falhas latentes, que quando se alinham, significam que todas as defesas falharam e as vulnerabilidades do sistema são expostas, e, neste momento, os incidentes ocorrem. Uma contribuição importante deste modelo é corroborar com a ideia de que cada fator que contribui para o incidente é necessário, mas não suficiente, sendo que um incidente nunca possui uma causa única, mas uma combinação delas.

Um acidente organizacional pode ser definido como “a falha simultânea de várias barreiras, facilitada por características não ótimas da organização” (REASON; HOLLNAGEL; PORIES, 2006). Uma variação posterior do modelo foi proposta por Reason (1997), conforme apresentado na Figura 26. A parte superior é equivalente ao modelo da Figura 25. A parte inferior da Figura 26 mostra o desenvolvimento de um acidente organizacional, sendo que os fatores organizacionais, os fatores do local de trabalho e ações inseguras podem criar os buracos nas barreiras.

Figura 25 – Modelo do queijo suíço de Reason (1990a) - adaptado

Figura 26 – Modelo do acidente organizacional
– adaptado de (REASON, 1997)

O modelo de Reason serviu e serve como base para a elaboração de outros modelos, tendo o papel de ser um modelo de alto nível, para os modelos mais específicos como apresentados, por exemplo, em Dias et al. (2007), Ren et al. (2008) e Schönbeck (2007). O modelo do queijo suíço demonstrou que o surgimento de novos modelos não necessariamente invalida ou torna obsoletos os modelos

existentes. Historicamente, o modelo do queijo suíço teve uma importância ímpar como uma via didática e no entendimento de como acidentes acontecem. Recentemente, porém, o modelo de Reason foi objeto de críticas em um relatório escrito pelo próprio autor e por Hollnagel e Paries (REASON; HOLLNAGEL; PARIES, 2006). Neste relatório, são apontadas as principais críticas publicadas ao longo dos anos como:

- o modelo não leva em conta as inter-relações entre as causas, e sem estas, os resultados são vagos ou sem utilidade;
- as barreiras não são sempre estáticas ou constantes, e não são também independentes uma das outras (ver acoplamentos na seção 2.9.2);
- trata-se de uma teoria simples, com poucos detalhes de como aplicá-la em uma situação real;
- nem sempre um acidente pode ser a consequência de um erro. Acidentes podem acontecer mesmo quando todas as pessoas envolvidas acreditam que estão tomando as ações corretas, e acidentes podem decorrer de um comportamento normal ou um evento normal.

Os autores concluem que o modelo de Reason tem menos ambição que os modelos que vieram a seguir, os quais estudam as probabilidades do erro humano, e tentam alcançar maior eficiência na predição de acidentes:

The Swiss Cheese Model (SCM) does not provide a detailed accident model or a detailed theory of how the multitude of functions and entities in a complex socio-technical system interact and depend on each other. That does not detract from its value as a means of communication, but may limit its use in analysis and as a support for proactive measurements. On the other hand, the SCM was never developed to be a detailed model in this sense, and it is therefore hardly justified to criticize it for that. Indeed, as most of the criticisms fail to distinguish among the three primary uses of the SCM, they may be accusing it for failing to achieve something it never intended. (REASON; HOLLNAGEL; PARIES, 2006, p. 20)

3.1.4.2. Fatores organizacionais na área naval

Fatores organizacionais estão diretamente relacionados à maneira com que as embarcações são gerenciadas e operadas. Abaixo estão listados resumidamente

alguns exemplos de fatores organizacionais presentes no setor naval (IMO, 2002b). Para o melhor entendimento e para a aplicação destes fatores na metodologia de análise de risco que será proposta, foi sugerida uma classificação destes fatores segundo sua relação com a tripulação, sistema físico ou níveis de perda e consequência. Os fatores a. e b. estão relacionados à prevenção do incidente. Os fatores c. estão relacionados à gestão do acidente.

a. Fatores organizacionais relacionados à tripulação:

- Políticas de recursos humanos (ex.: seleção da tripulação)
- Funções dos tripulantes e pessoal de terra
- Requisitos de relatórios
- Agenda de turnos e carga de trabalho, horas-extras, intervalos de folga
- Cultura organizacional e estilo de gerência
- Incentivos a comprometimento com processos
- Política de treinamento técnico e reciclagem
- Comprometimento com normas SMS, IMO e certificadoras.
- Filosofia orientada à segurança
- Cumprimento de funções e hierarquia
- Políticas de segurança em relação a abortar uma missão (mau tempo, tripulação incompleta, etc.)
- Insegurança em relação ao emprego
- Ambiente de trabalho adequado
- Falta de estímulo financeiro
- *Job rotation* da tripulação para disseminação do conhecimento
- Pressão para resultados

b. Fatores organizacionais relacionados ao sistema técnico:

- Especificação do armador
 - Projeto do navio, escolha da confiabilidade dos equipamentos
 - escolha do nível de automação, escolha das redundâncias
 - Ergonomia (postos de trabalho, acomodações e máquinas)
 - Escolha de certificadoras
- Política de manutenção e inspeção
- Alteração da planta durante fase operacional, em desacordo com critérios adotados no projeto inicial (ampliações de instalações, trocas de equipamentos causando mudanças das cargas previstas no projeto elétrico, layout de salas, diminuição de espaço para evacuação, etc.)

c. Fatores organizacionais relacionados aos níveis de perda e consequências:

- Treinamento para situações de acidentes
- Treinamento da tripulação na mitigação das consequências
- Contratação de funcionários com perfil de resiliência
- Procedimentos e regras para situações de emergência

- Instalação de sistemas para mitigar perdas (barreiras de contenção de óleo, barcos salva-vidas, etc.)
- Políticas de manutenção
- Job rotation
- Políticas para mitigação de:
 - Impacto no público
 - Impacto em operações associadas
 - Impacto na reputação e imagem da empresa

Assim como o tema fatores humanos e organizacionais é amplo, a lista de fatores que podem ser relacionados a um sistema também será extensa. A lista acima apresentada, portanto, não esgota todos os fatores presentes em uma embarcação, podendo existir outros fatores e outras possíveis classificações. No entanto, esta lista, baseada na diretriz de (IMO, 2002b), é uma referência importante e um ponto de partida fundamental para as análises de risco.

3.1.4.3. Cultura de segurança como fator organizacional

It therefore becomes evident that an effective safety culture requires the active collaboration between management and the workforce. (IMO, 2002c, p. 2)

A cultura de segurança mereceu uma subseção dedicada por se tratar de um fator organizacional chave nas causas de acidentes com embarcações, conforme analisado em detalhe por (HETHERINGTON; FLIN; MEARNS, 2006), e por ser considerada como sendo o maior fator contribuinte em acidentes (LUNDBERG; ROLLENHAGEN; HOLLNAGEL, 2009). A cultura de segurança em diversas indústrias, incluindo a indústria naval e de transportes marítimos, sofreu algumas mudanças nos anos passados (WANG et al., 2004). Isso pode ser demonstrado pela implementação do ISM Code e a introdução das avaliações formais de segurança (FSA) pela IMO no processo de elaboração de regras.

Segundo Ayyub (2003), segurança (do inglês, *safety*), pode ser definida como o julgamento da aceitabilidade do risco para determinado sistema. A cultura de segurança se refere à dedicação pessoal e à responsabilidade de todos os indivíduos engajados em uma atividade, que tem relação com a segurança de uma planta. Também deve se referir à mudança de postura frente aos erros humanos e acidentes, fazendo com que a identificação de riscos seja uma rotina, que os

projetos dos sistemas sejam centrados no homem, de forma a considerar os fatores humanos.

A cultura de segurança está fortemente relacionada à gerência de uma organização, a qual estabelece políticas, incentivos, responsabilidades para a operação da empresa. A comunicação interna também é um fator chave, pois as informações relevantes à segurança devem ser abertamente disseminadas, de forma a se criar um ambiente onde se questionem atitudes de risco e evitem a complacência a normas, priorizando o compromisso com as questões de segurança.

A IMO também reconhece a importância da cultura de segurança, enfatizando que o cumprimento das normas só é efetivo com atitudes orientadas à segurança, intrínsecas no dia a dia daqueles envolvidos na operação do navio (IMO, 2002c).

3.1.5. Análise da confiabilidade humana

O estudo da confiabilidade humana pode ser visto como uma área híbrida que abrange os temas de psicologia, ergonomia, confiabilidade de sistemas e análise de sistemas. A hipótese inicial nas análises de segurança era que o operador humano poderia ser descrito da mesma maneira que uma máquina, o que acabou por se provar inválido. Assim, surgiu a necessidade de se desenvolver métodos mais realistas que descrevessem as ações humanas de forma adequada (HOLLNAGEL, 1998).

Conforme já exposto anteriormente, a atuação humana é um fator de risco e um fator de degradação da própria confiabilidade do sistema. Isto posto, fica evidente que a confiabilidade total do sistema deve ser composta pela confiabilidade dos equipamentos e pela confiabilidade da operação destes equipamentos. Filgueiras (1996) enfatiza este papel dual do ser humano, contribuindo e comprometendo a segurança dos sistemas:

Por outro lado, é exatamente a existência do elemento humano que tem evitado um número muito maior de falhas de sistema, já que sua capacidade de adaptação e solução de problemas mitiga as consequências destas falhas. Na verdade, a análise dos grandes acidentes industriais revela que os operadores de sistemas de controle são apenas a ponta de uma cadeia de problemas, muitas vezes latentes, que apenas se mostram quando combinados em alguma situação catastrófica. (FILGUEIRAS, 1996, p. 4)

O objetivo da Análise da Confiabilidade Humana (ACH) é caracterizar como as ações humanas podem levar o sistema a estados diferentes dos estados esperados ou desejados (HOLLNAGEL, 1998). Segundo Kumamoto e Henley (1996), é difícil prover uma descrição unificada e quantitativa dos aspectos positivos e negativos do ser humano na confiabilidade e segurança dos sistemas. Mas uma visão unificada é, todavia, necessária.

Swain e Guttman (1983) definem formalmente a confiabilidade humana como:

"the probability of successful performance of the human activities necessary for either a reliable or an available system; specifically, the probability that a system-required human action, task or job will be completed successfully within a required time period" (SWAIN; GUTTMANN, 1983).

Filgueiras (1996) aponta algumas observações interessantes sobre esta definição:

- a confiabilidade humana é definida como uma probabilidade, assim como a confiabilidade de sistemas
- a confiabilidade humana implica a definição de uma missão, sem a qual a confiabilidade humana não pode ser avaliada
- a missão possui um tempo determinado para ser cumprida

A ACH é, portanto, relacionada à predição das probabilidades de uma ação humana falhar. Sua origem é ligada às disciplinas de engenharia, que fizeram uso de conceitos de psicologia para aplicação prática nas análises. A literatura especializada comumente utiliza a distinção entre os métodos de primeira geração (métodos clássicos) e de segunda geração (métodos modernos). As técnicas pertencentes a cada uma das gerações da ACH serão tratadas nas seções seguintes desta tese.

3.2. Visão teórica versus visão prática

O objetivo desta seção é justificar algumas simplificações adotadas neste trabalho, antes de discorrer sobre as técnicas de ACH.

Segundo Hollnagel (1998) a própria natureza e a origem do termo “erro humano” é entendida sob diferentes pontos de vista, de acordo com as análises de diferentes profissionais. Um engenheiro prefere enxergar um operador como um componente do sistema que pode falhar ou ter sucesso, e que seu comportamento pode ser descrito da mesma maneira que uma máquina. Psicólogos partem do princípio que o comportamento humano é sempre intencional, e só pode ser compreendido analisando-se seus objetivos e intenções. Sociólogos, por sua vez, se referem aos modos de erro humano como características de um sistema sócio-técnico, e em uma análise sociológica, fatores como estilo de gerência e estrutura organizacional são vistas como influenciadores das taxas de erro.

O erro humano também pode ser avaliado conforme o resultado da ação ou intenção, segundo um critério de resposta (HOLLNAGEL, 1998). Duas categorias de critérios de resposta são utilizadas: modelos verificáveis externalizados ou internalizados. A Figura 27 apresenta estes dois modelos.

Figura 27 – Categorias do erro segundo critério de resposta
– adaptado de (HOLLNAGEL, 1998, p. 25-26)

O erro como uma categoria externalizada é definido conforme o objetivo e resultado da ação. Nas análises de confiabilidade humana, o erro é encarado desta forma, sendo uma resposta que excede algum limite de aceitabilidade. Por outro lado, analistas que trabalham sob o ponto de vista da psicologia, preferem utilizar os modelos internalizados, cujo critério de resposta está relacionado com as intenções temporárias e objetivos da ação do indivíduo. Para fins de análise da confiabilidade humana, o estudo dos erros sob o ponto de vista dos psicólogos não é significativo,

pois é impossível, na prática, fazer suposições concretas sobre o estado da mente do operador e avaliar suas intenções reais.

Conforme citado nos capítulos anteriores, a análise de confiabilidade humana se originou das disciplinas da engenharia, e possui uma visão muito prática em relação ao comportamento humano. Segundo Hollnagel (1998), existe ainda um abismo entre esta visão prática da ACH e estudos psicológicos, o que é extremamente ruim, pois a ACH pode sempre tirar vantagens dos estudos teóricos da psicologia sobre os erros humanos, e vice versa.

A visão teórica enxerga que existe até uma desvantagem em se utilizar a abordagem tradicional de fatores humanos, que é a possibilidade limitada de caracterizar os eventos em termos das características psicológicas do operador e de suas funções cognitivas. Isso porque, os modelos não foram desenvolvidos para considerar as teorias de psicologia. Por outro lado, os modelos de processamento de informações não possuem validações, carecem de explicações válidas e permeiam no campo das teorias e hipóteses (HOLLNAGEL, 1998). Filgueiras (1996) destaca a oposição entre as correntes de pensamento preditivas e psicológicas:

Esta corrente foi denominada, mais tarde, de preditiva, pois o objetivo principal é prever a confiabilidade humana em uma nova tarefa, a partir da experiência de tarefas anteriores. Em algumas publicações, estas técnicas são chamadas de técnicas de engenharia - já que se destinam a contabilizar e contornar os erros - em oposição a uma outra corrente, denominada psicológica, cujo objetivo é compreender os mecanismos de erro. (FILGUEIRAS, 1996, p. 37)

Neste trabalho, dar-se a preferência para a visão prática (externalizada) do erro humano e da confiabilidade humana. Os conceitos relacionados à parte da psicologia cognitiva serão tratados no mesmo nível de detalhes da bibliografia apresentada dentro do campo da engenharia. Este trabalho não tem a pretensão de discutir ou criticar os métodos de ACH à luz dos fundamentos teóricos sobre a mente humana, mas sim, avaliá-los sob o ponto de vista de sua aplicabilidade, uma vez que os supostos usuários do método a ser proposto posteriormente serão também da área técnica.

3.3. Técnicas de Análise da Confiabilidade Humana

3.3.1. Histórico

As técnicas de análise da confiabilidade humana se originaram do estudo do comportamento e desempenho humano em ambientes industriais, provavelmente durante a Revolução Industrial no final do século XIX. A principal motivação do surgimento desta disciplina foi a necessidade de avaliação do impacto dos erros humanos nos sistemas. A partir da Segunda Guerra Mundial, a análise das atividades humanas se tornou uma exigência, já que a evolução tecnológica aumentou o grau de complexidade dos sistemas. As análises de confiabilidade humana, então, nasceram baseadas nos conceitos da Teoria de Confiabilidade de Sistemas, os quais ganharam popularidade após seu sucesso nas aplicações em sistemas eletrônicos (FILGUEIRAS, 1996).

O acidente da usina nuclear de Three Mile Island, no estado da Pensilvânia nos Estados Unidos, em 28 de março de 1979 foi um divisor de águas na disciplina de Confiabilidade Humana. As causas do acidente foram atribuídas ao mau estado do sistema técnico, mas principalmente aos erros humanos, com ações e decisões erradas tomadas por operadores despreparados. Esta tragédia despertou a necessidade do melhor entendimento e modelagem do comportamento humano em tarefas cognitivas, a fim de se poder aplicar esse conhecimento em engenharia.

Filgueiras (1996) destaca alguns resultados positivos em termos científicos devido aos esforços de se evitar acidentes semelhantes:

- O modelo do comportamento humano de Rasmussen. (RASMUSSEN, 1983).
- Os trabalhos de Swain e Guttman, que ficaram conhecidos como o Manual da Confiabilidade Humana. (SWAIN; GUTTMANN, 1983).
- A norma NUREG-0700 da *Nuclear Regulatory Commission*, agência americana de regulamentação nuclear, que incluía instruções sobre ergonomia e das interfaces homem-máquina (NUREG, 1981b apud FILGUEIRAS, 1996).

A primeira metade da década de 1980 foi o ápice do surgimento de técnicas de confiabilidade humana, a maioria desenvolvida e utilizada nos Estados Unidos. O final da década de 1980 teve um número reduzido de publicações de novas técnicas, surgindo novos desenvolvimentos apenas no início da década seguinte, após um artigo de Dougherty (1990), fazendo uma “segunda chamada” para novas pesquisas. Dougherty (1990) foi quem estabeleceu a distinção entre os métodos de primeira e segunda geração. Para um aprofundamento sobre estas técnicas, o leitor pode consultar Hollnagel (1998), onde uma síntese das principais técnicas no campo da ACH é apresentada. Segundo este trabalho, podem ser identificadas na literatura de 35 a 40 técnicas distintas de ACH.

Serão apresentadas a seguir algumas técnicas e críticas referentes à primeira e segunda geração. As técnicas foram selecionadas ou por serem muito difundidas e utilizadas em trabalhos da área, ou por serem relevantes ao entendimento ou aplicação no modelo a ser apresentando neste trabalho.

3.3.2. Fatores de condicionamento de desempenho

Antes de se apresentar as técnicas de análise de confiabilidade humana, apresentar-se-á o conceito de fatores de condicionamento de desempenho, o qual será abordado em várias técnicas.

Pesquisas sobre análise da confiabilidade humana naturalmente se preocuparam com a variabilidade do desempenho humano, uma vez que a variabilidade imprevisível e incontrolável pode se tornar uma das causas de um incidente ou acidente. Ainda que o desempenho humano tenha uma variabilidade inerente, assume-se que os principais fatores que afetam o desempenho são externos. O conceito de Fatores de Condicionamento de Desempenho, mais conhecido como *Performance Shaping Factors* (PSF), surgiu para classificar todos os fatores que influenciam o desempenho humano. Os PSF são normalmente vistos como um fator contribuinte, nunca como uma causa de um erro. Segundo Hollnagel (1998), se encontram na literatura listas de diferentes tamanhos sobre os PSF, e existe até um entendimento geral de uma lista dos principais fatores que influenciam o desempenho humano. Todavia, ainda não há consenso sobre como esses fatores efetivamente exercem sua influencia.

Nos métodos clássicos de ACH, como o método THERP (que será apresentado adiante), parte-se do princípio que os PSF alteram as probabilidades de erro humano (do inglês, HEP – *Human Error Probability*). A influência dos PSF é contabilizada multiplicando um HEP pela ponderação de todos os PSF envolvidos, conforme demonstrado na eq. (6).

$$P_{EA} = HEP_{EA} \cdot \sum_{k=1}^n PSF_k \cdot W_k + C \quad (6)$$

onde:

P_{EA} é a probabilidade de uma ação errônea específica;

HEP_{EA} é a probabilidade do erro humano correspondente;

PSF_k é a valor numérico do k-ésimo PSF;

W_k é o peso do k-ésimo PSF;

n é o número total de PSF;

C é uma constante numérica.

Sob o ponto de vista psicológico a eq. (6) é vazia, mas não pode ser descartada, pois é possível estabelecer seus parâmetros empiricamente. Hollnagel (1998) critica esta abordagem, pois a influência dos fatores externos é muito mais complexa, apesar de admitir que quando o THERP foi concebido, a psicologia cognitiva estava no início de seu desenvolvimento, e o método não pretendia descrever apropriadamente a mente humana.

Swain e Guttman (1983 apud HOLLNAGEL, 1998) apresentaram uma divisão dos PSF: externos, subdivididos em características situacionais, instruções da tarefa, e características do equipamento; internos, que atuam no indivíduo, e relativas ao estresse (ver Tabela 6).

Hollnagel (1998) classifica essa divisão como autoritária, e que peca em não considerar a dependência entre os PSF. Hollnagel propõe a utilização de uma nova abordagem de fatores chamados de Condições de Desempenho Comum (*Common Performance Conditions* - CPC), que se preocupa em utilizar os PSF fazendo uma ligação entre as condições e o desempenho, ou seja, os caminhos pelos quais uma ação pode dar errada (chamados de modos de erro). Os CPC são uma adaptação

dos PSF para o método CREAM (que será apresentado adiante). A diferença entre os dois não está na nomenclatura, mas como são utilizados. Para facilitar a prática, os CPC são mais resumidos, no total de nove condições, e possuem uma dependência entre si. A Tabela 7 apresenta os nove CPC e sua relação com a confiabilidade do desempenho.

A classificação apresentada na Tabela 7 é baseada na teoria dos fatores humanos e experiências com a ACH. A Tabela 8 reproduz a tabela de Hollnagel (1998) resumindo as dependências entre os CPC.

Tabela 6 – Classificação dos PSF segundo (SWAIN; GUTTMANN, 1983)

PSF Externas		PSF Relativas ao estresse	PSF Internas
Características situacionais	Características da tarefa e equipamentos	Psicológicas	Características da pessoa devido às influências externas e internas
<ul style="list-style-type: none"> ▪ Fatores arquitetônicos ▪ Qualidade do meio ambiente (iluminação, barulho, limpeza, umidade, temperatura, etc) ▪ Horas de trabalho e intervalos ▪ Rotatividade ▪ Disponibilidade de ferramentas necessárias ▪ Estrutura organizacional ▪ Atitude de supervisores, sindicatos, agencias reguladoras ▪ Prêmios, reconhecimento, benefícios 	<ul style="list-style-type: none"> ▪ Percepção requerida ▪ Exigência do equipamento ▪ Relação entre controles de mostradores ▪ Interpretações ▪ Complexidade ▪ Frequência e repetitividade ▪ Memória de longo ou curto prazo ▪ Cálculos requeridos ▪ Feedback ▪ Dinâmica x atividade passo a passo ▪ Equipe e comunicação ▪ Interface homem-máquina 	<ul style="list-style-type: none"> ▪ Duração do estresse ▪ Velocidade da tarefa ▪ Quantidade de trabalho ▪ Riscos ▪ Tratamento (a falha, demissão) ▪ Trabalho monótono ▪ Longos períodos sem ação ▪ Conflitos a respeito dos motivos da obtenção do melhor resultado ▪ Distrações ▪ Falta de avisos 	<ul style="list-style-type: none"> ▪ Experiência e treinamento ▪ Estado atual desta prática ▪ Variáveis de personalidade e inteligência ▪ Motivação e atitude ▪ Estado emocional ▪ Estresse (mental ou físico) ▪ Conhecimento do rendimento exigido ▪ Diferenças de sexo; ▪ Condição física; ▪ Atitudes baseadas na influência de grupos familiares ou outras pessoas; ▪ Identificação com a equipe.
Instruções de trabalho e tarefas		Fisiológicas	
<ul style="list-style-type: none"> ▪ Procedimentos requeridos ▪ Comunicação oral ou escrita ▪ Avisos de perigo ▪ Método de trabalho ▪ Política de trabalho 		<ul style="list-style-type: none"> ▪ Duração dos níveis de estresse ▪ Fadiga ▪ Dor e desconforto ▪ Fome e sede ▪ Temperaturas extremas ▪ Radiação ▪ Pressão atmosférica ▪ Insuficiência de oxigênio ▪ Vibração ▪ Movimentos restritos ▪ Falta de exercícios físicos 	

Tabela 7 – CPC e a confiabilidade do desempenho
– adaptado de (HOLLNAGEL, 1998, p. 114)

Nome do CPC	Nível	Efeito esperado na confiabilidade do desempenho
Adequação à organização	Muito eficiente	Melhora
	Eficiente	Não significativo
	Ineficiente	Reduz
	Deficiente	Reduz
Condições de trabalho	Vantajosa	Melhora
	Compatível	Não significativo
	Incompatível	Reduz
Adequação a MMI (<i>Man-Machine Interface</i>) e suporte operacional ⁸	Apoiadora	Melhora
	Adequada	Não significativo
	Tolerável	Não significativo
	Inapropriada	Reduz
Procedimentos disponíveis	Apropriado	Melhora
	Aceitável	Não significativo
	Inapropriado	Reduz
Número de objetivos simultâneos	Menor que a capacidade	Não significativo
	De acordo com capacidade	Não significativo
	Maior que a capacidade	Reduz
Tempo Disponível	Adequado	Melhora
	Temporariamente inadequado	Não significativo
	Continuamente inadequado	Reduz
Horário	Diurno	Não significativo
	Noturno	Reduz
Treinamento e experiência	Adequados	Melhora
	Adequados	Não significativo
	Inadequados	Reduz
Colaboração da equipe	Muito eficiente	Melhora
	Eficiente	Não significativo
	Ineficiente	Não significativo
	Deficiente	Reduz

⁸ Modelo proposto por (SHERIDAN; HENNESSY, 1984). Relacionado com a devida apresentação das informações em interfaces e indicadores

Tabela 8 – Dependência entre CPC
– adaptado de (HOLLNAGEL, 1998, p. 115)

	Adequação à organização	Condições de trabalho	Adequação a MMI	Procedimentos disponíveis	Número de objetivos simultâneos	Tempo Disponível	Horário	Treinamento e experiência	Colaboração da equipe
Adequação à organização									
Condições de trabalho	+		+			+	+	+	
Adequação a MMI	+								
Procedimentos disponíveis	+								
Número de objetivos simultâneos		-	-	-					
Tempo Disponível		+	+	+	-		+		+
Horário									
Treinamento e experiência	+								
Colaboração da equipe	+							+	

3.3.3. Técnicas de primeira geração

3.3.3.1. Matriz de Confusão

A matriz de confusão ou matriz confusão (do inglês, *confusion matrix*) é uma técnica utilizada para estimar a probabilidade de um operador não diagnosticar corretamente um evento iniciador. Devido ao fato do comportamento humano ser imprevisível, as análises de árvores de eventos se tornam complexas, uma vez que se baseiam em lógica binária e a inclusão de todas as possíveis ações humanas implica um número grande de ramos.

Nesta subseção, será apresentada resumidamente a abordagem para estimativa de erro de diagnóstico de Wakefield (1988 apud KUMAMOTO; HENLEY, 1996). O método inicia com a construção da matriz de confusão apresentada na Tabela 9. A letra P na linha i e coluna j indica a probabilidade de o evento E_i ser diagnosticado como evento E_j . A severidade ou impacto deste erro de diagnóstico é dado pela consequência C_{ij} .

Tabela 9 – Matriz de confusão

	E1	E2	E3	E4	E5
E1		P12,C12	P13,C13	P14,C14	P15,C15
E2	P21,C21		P23,C23	P24,C24	P25,C25
E3	P31,C31	P32,C32		P34,C34	P35,C35
E4	P41,C41	P42,C42	P43,C43		P45,C45
E5	P51,C51	P52,C52	P53,C53	P54,C54	

As informações para a construção da matriz de confusão são obtidas da matriz de resposta da planta, mostrada na Tabela 10. Cada linha corresponde a um evento iniciador e as colunas correspondem a um indicador da planta, como um alarme. Os símbolos usados neste exemplo correspondem a: ON – início de um alarme; OFF – final de um sinal; U – aumento; D – redução; X – aumento ou redução; 0 – nível zero.

Tabela 10 – Matriz de resposta da planta

	R1	R2	R3	R4	R5	R6
E1	ON	OFF	U	D	X	0
E2	ON	ON	X	U	D	D
E3	ON	OFF	D	D	0	U
E4	OFF	ON	0	X	0	0
E5	OFF	OFF	D	X	U	D

Desta matriz, as probabilidades de erro de diagnóstico podem, então, ser avaliadas. Por exemplo, pode-se estimar a probabilidade de o operador diagnosticar E1(ON, OFF, U, D, X, 0), como sendo E2(ON, ON, X, U, D, D), conhecendo-se o significado destas respostas na planta, e as possíveis reações do operador.

A matriz de procedimentos para o evento iniciador da Tabela 11 mostra os procedimentos a serem adotados para cada evento iniciador, e sua ordem correta. Esta matriz mostra os erros de sequência de procedimentos devido ao erro de diagnóstico. Como exemplo, dado um evento iniciador E1 diagnosticado como E2, o

operador irá executar a sequência de procedimentos p1-p5-p3, ao invés de executar a sequência p1-p2-p3.

Tabela 11 – Matriz de procedimentos para o evento iniciador

	p1	p2	p3	p4	p5	p6	p7
E1	1	2	3				
E2	1		3		2		
E3	1			2	3		
E4	1		2		3	4	
E5	1	2		3			

Para identificar as probabilidades de um operador utilizar um procedimento incorreto, após um erro de diagnóstico, se constrói a matriz de entradas e procedimentos. A Tabela 12 mostra quando um procedimento deve ser iniciado. Cada linha mostra um procedimento, e cada coluna um indicador da planta. Os símbolos entre parêntesis significam que somente este estado é suficiente para o operador iniciar o procedimento correspondente. Como exemplo, a condição para se iniciar o procedimento p1 é quando os indicadores R1 e R2 estiverem em ON e OFF respectivamente.

Destas matrizes de resposta da planta (Tabela 10) e de entradas e procedimentos (Tabela 12) podem-se avaliar os procedimentos e ações que podem ser confundidos.

Tabela 12 – Matriz de entradas e procedimentos

	R1	R2	R3	R4	R5	R6
p1	ON	OFF				
p2	ON		U			
p3	ON	(OFF)		(D)	0	
p4	ON	ON				
p5		OFF	D		0	
p6	OFF	ON				0
p7	OFF	OFF		X		D

Usualmente, as análises via matriz de confusão são feitas para estimar as probabilidades de fases diferentes do acidente, por exemplo, até 15 minutos após a ocorrência do evento iniciador e até 1 hora após a ocorrência do evento iniciador. O principal ponto positivo deste método é que ele fornece uma estrutura simples para ajudar os analistas a identificar situações não facilmente modeladas por outros métodos. Por outro lado, segundo Hollnagel (1998), o método de matriz de confusão apresenta a estimativa de erro de diagnóstico sem considerar as questões cognitivas ou os fatores de condicionamento de desempenho.

3.3.3.2. Estimativa de especialistas

Esta abordagem ACH considera que especialistas estimem diretamente a probabilidade de ocorrência de determinado erro humano baseados em sua própria experiência (ver seção 2.8). Isso pode ser alcançado de diversas maneiras, com métodos estatísticos, classificando os especialistas, atribuindo pesos distintos a cada estimativa, entre outros. Este método não considera nenhum modelo de comportamento do operador, e os fatores de condicionamento de desempenho são presumidamente embutidos nos julgamentos dos especialistas (HOLLNAGEL, 1998).

3.3.3.3. Success Likelihood Index Method (SLIM)

O método SLIM (*Success Likelihood Index Method*, ou Método do Índice de Probabilidade de Sucesso) é um método de avaliação quantitativa da probabilidade de erro humano, desenvolvido por Embrey et al. (1984). Assim como os métodos de matriz de confusão e estimativa de especialistas o método SLIM não é em sua essência um método de ACH, mas uma ferramenta utilizada para contornar o problema de falta de dados sobre os erros humanos. O método utiliza os fatores de condicionamento de desempenho de forma quantitativa, ou seja, por não propor também um modelo de comportamento do operador, não há descrição de como os PSFs exercem sua influência (HOLLNAGEL, 1998).

Filgueiras (1996) destaca que o SLIM é interessante, pois atua em um nível macroscópico de análise, por considerar a opinião de especialistas, e, portanto é um método mais acessível.

Para a determinação de uma probabilidade de erro humano, convoca-se certo número de especialistas, para os quais são apresentados critérios pertinentes chamados de influências, pois estas influenciam a probabilidade de ocorrência do erro humano. Essas influências são semelhantes aos fatores de condicionamento de desempenho, como nível de estresse, complexidade da tarefa, fatores ambientais, qualidade da equipe, etc.

Cada especialista avalia esta influência com um fator entre 0 e 1, que quantifica a influência sobre o erro r_i . Influências entre 0 e 0,5 favorecem o erro humano, e entre 0,5 e 1 significam que sua presença ajudam a evitar o erro. Cada influência também recebe um peso relativo à sua importância, denominado índice de qualidade q_i . A menos significativa recebe peso 10, e as demais múltiplos desse valor. O índice de probabilidade de sucesso SLI é calculado da seguinte maneira (FILGUEIRAS, 1996):

$$SLI = \sum_i \frac{r_i}{\sum_i r_i} \cdot q_i \quad (7)$$

Para um dado SLI , a probabilidade de erro humano (HEP – *Human Error Probability*) para determinada tarefa é estimada por:

$$HEP = 10^{a \cdot SLI + b} \quad (8)$$

onde a e b são constantes determinadas por duas ou mais tarefas para as quais os HEP são conhecidos. Não havendo dados sobre a e b , estes devem ser estimados por especialistas (KUMAMOTO; HENLEY, 1996).

3.3.3.4. Correlação Tempo-confiabilidade

Dougherty e Fragola (1988) introduziram o método chamado de Correlação Tempo-Confabilidade, ou *Time-Reliability Correlation* (TRC). O método visa estimar

a probabilidade de um operador efetuar um diagnóstico ou tomar uma decisão correta, dentro de um tempo t , matematicamente, expressa por:

$$R_H = P(T \leq t) \quad (9)$$

onde R_H é a confiabilidade humana, e T é o tempo decorrido até o diagnóstico. Quando o limite de tempo tende para o infinito, a probabilidade do diagnóstico correto é 100%:

$$\lim_{t \rightarrow \infty} R(t) = 1 \text{ (sucesso)} \quad (10)$$

Fazendo-se uma analogia à confiabilidade de sistemas, considerando a variável independente como sendo o tempo necessário para se realizar o diagnóstico correto, experimentos podem ser realizados em um cenário específico, e a confiabilidade humana R_H pode ser calculada por (DOUGHERTY; FRAGOLA, 1988):

$$R_H(t_i) = \frac{N_i}{N + 1} \quad (11)$$

onde:

N_i é o número de respostas corretas até o tempo t_i ;

N é o número total de respostas.

As curvas TRC, como são chamadas, são obtidas através de experimentos em simuladores. Aos dados são então ajustadas distribuições de Weibull, normal ou log-normal. Fragola e Dougherty (1988) sugerem que os experimentos em simuladores apontam que a distribuição log-normal é suficiente para a modelagem das curvas TRC. Para uma distribuição log-normal, a probabilidade do erro humano (HEP) associada ao intervalo de tempo T_w pode ser calculada por (FILGUEIRAS, 1996):

$$HEP = P(T_{resposta} > T_w) = 1 - \Phi\left(\frac{\ln(T_w - T_m)}{\varepsilon}\right) \quad (12)$$

onde:

T_m é o tempo medido de resposta dos operadores;

ε é o desvio padrão logarítmico;

Φ é a distribuição log-normal acumulada.

O método TRC sofre algumas críticas por causa da imprecisão dos dados e por ter sua utilidade questionável em projeto, já que nem sempre é possível construir simuladores para avaliar a confiabilidade de um sistema. Além disso, utilizar curvas de situações semelhantes também pode ser uma aproximação grosseira dos resultados. Hollnagel (1998), por sua vez, considera o método TRC como uma “caixa preta”, já que não se preocupa com o que ocorre entre o evento e a resposta.

3.3.3.5. Confiabilidade Cognitiva Humana

O método Confiabilidade Cognitiva Humana, mais conhecido como HCR (*Human Cognitive Reliability*), foi criado por Hannaman, Spurgin e Lukic (1984), e se propõe a estimar a probabilidade de um operador não responder a um evento durante um acidente. A parte cognitiva do nome do método faz alusão ao modelo baseado em habilidades, regras e conhecimento de Rasmussen (ver subseção 3.1.3.1).

O método utiliza três curvas TRC, uma para cada tipo de comportamento, modeladas através da distribuição de Weibull. A probabilidade de o operador não responder até o tempo t é dada por (KUMAMOTO; HENLEY, 1996):

$$P(t) = \exp \left\{ - \left[\frac{\left(\frac{t}{T_{1/2}} \right) - B}{A} \right]^c \right\} \quad (13)$$

onde:

t é o tempo disponível para completar o diagnóstico ou ação após o estímulo;

$T_{1/2}$ é a média estimada de tempo para completar a ação;

A , B , C são os coeficientes de correlação associados ao tipo de processamento mental, como habilidade, regra ou conhecimento.

O modelo HCR assume que o tempo médio é afetado pelos fatores de condicionamento de desempenho da seguinte maneira:

$$T_{1/2} = (1 + K_1) \cdot (1 + K_2) \cdot (1 + K_3) \cdot \overline{T}_{1/2} \quad (14)$$

As constantes K_1 , K_2 e K_3 são coeficientes extraídos de tabelas de PSF, como, por exemplo, é apresentado na Tabela 13. E $\overline{T}_{1/2}$ é o tempo de resposta médio nominal correspondente à probabilidade de 0,5.

Tabela 13 – Tabela de PSF para HCR
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 493)

PSF	Coeficiente	Critério
Experiência	K_1	
1. Especialista	-0,22	Treinado com mais de 5 anos de experiência
2. Médio	0,00	Treinado com mais de 6 meses de experiência
3. Novato	0,44	Treinado com menos de 6 meses de experiência
Nível de estresse	K_2	
1. Grave	0,44	Situação de alto estresse, emergência, ameaça
2. Alto	0,28	Situação de alto estresse, alta carga de trabalho
3. Normal	0,00	Situação ótima
4. Baixo	0,28	Problema com vigilância
Interface	K_3	
1. Excelente	-0,22	Ajuda ao operador disponível para ajudar em acidentes
2. Boa	0,00	Display bem projetado, com integração de informação
3. Normal	0,44	Display bem projetado, sem integração de informação
4. Ruim	0,78	Display disponível, mas projeto não foca o indivíduo
5. Muito Ruim	0,92	Display não visível diretamente pelo operador

O HCR é um dos únicos métodos da primeira geração que se refere a modelos cognitivos, mas também não explica como esses fatores de condicionamento de desempenho afetam o desempenho do operador.

3.3.3.6. THERP

O método THERP (*Technique for Human Error Rate Prediction*) é certamente a técnica de ACH mais conhecida e mais utilizada. O método, desenvolvido por Swain e Guttman (1983) no Sandia National Laboratories para a US Nuclear Regulatory Commission, tem o objetivo de prover dados para as análises probabilísticas de risco. Os cálculos são baseados em taxas de erros pré-definidas, chamadas de Probabilidades de Erro Humano (HEP – *Human Error Probability*). O método envolve realizar uma análise das tarefas, a fim de prover a descrição das características de desempenho do indivíduo a ser analisado. Esses resultados são apresentados graficamente através de uma árvore de eventos, que é uma representação formal da sequência de ações. A probabilidade nominal calculada é então modificada pelos fatores de condicionamento de desempenho.

De forma sucinta, os passos de aplicação do THERP são:

1. Definir disfunções do sistema que são influenciadas por erros humanos, os quais terão suas probabilidades estimadas.
2. Analisar as operações humanas correspondentes, decompondo-se cada tarefa em uma árvore de eventos, onde se representam as ações, modos de erro, e recuperações (ver Figura 28).
3. Cada elemento na tarefa é quantificado, segundo as tabelas de probabilidade de erro humano, levando-se em conta os fatores de condicionamento de desempenho, conforme a eq. (6).
4. Determinar os efeitos dos erros humanos nos eventos de disfunção do sistema.
5. Recomendar e avaliar mudanças no sistema para reduzir a taxa de falha para o nível aceitável.

A Tabela 14 apresenta um exemplo de probabilidade de erro humano para erros na verificação e checagem de monitores (SWAIN; GUTTMANN, 1983 apud KUMAMOTO; HENLEY, 1996). A Tabela 15 apresenta como um fator de condicionamento de desempenho, no caso o estresse, afeta as probabilidades de erro humano tabeladas.

Figura 28 – Árvore de eventos do THERP

Tabela 14 – Erros na verificação e leitura de monitores

Tarefa de verificação e leitura	HEP	Intervalo
1. Indicadores digitais	0,001	(0,0005 a 0,005)
2. Medidores analógicos com marcações de limites de fácil visualização	0,001	(0,0005 a 0,005)
3. Medidores analógicos com marcações de limites de difícil visualização	0,002	(0,001 a 0,01)
4. Medidores analógicos sem marcações de limites	0,003	(0,001 a 0,01)
5. Registros gráficos analógicos com limites	0,002	(0,001 a 0,01)
6. Registros gráficos analógicos sem limites	0,006	(0,002 a 0,02)
7. Confirmar uma mudança de status de uma luz	Desprezível	-
8. Verificar uma luz com indicador errado	0,003	(0,001 a 0,01)
9. Interpretar errado a indicação dos indicadores luminosos	0,001	(0,0005 a 0,005)

Dos métodos de análise de confiabilidade humana, o THERP é sem dúvida o mais detalhado e documentado. É um método que não necessita de um “software” específico, e os valores tabelados dispensam os trabalhos de coleta de dados. As recomendações das mudanças para aumentar a confiabilidade são direcionadas às manipulações dos fatores de condicionamento de desempenho e às implementações de redundâncias.

Tabela 15 – Probabilidade de erros humanos para nível de estresse
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 491)

Nível de estresse	HEP
Operador experiente	
Muito baixo	2x tabela do HEP
Ótimo	Tabela do HEP
Moderadamente alto	
Tarefas passo a passo	2x tabela do HEP
Tarefas dinâmicas	5x tabela do HEP
Muito alto	0,25
Operador novato	
Muito baixo	2x tabela do HEP
Ótimo	Tabela do HEP
Moderadamente alto	
Tarefas passo a passo	4x tabela do HEP
Tarefas dinâmicas	10x tabela do HEP
Muito alto	0,25

Entretanto, a técnica THERP é relativamente ruim para avaliar processos cognitivos dependentes de tempo, como o diagnóstico de um monitor de sistema de alarmes durante um acidente. Diante das dificuldades em modelar ações humanas utilizando árvores binárias de eventos, este método não considera a dependência entre eventos e entre fatores de desempenho, que constituem suas principais deficiências. Isso porque, como o comportamento humano é imprevisível, faz-se necessário identificar todas as possíveis ações erradas causadas por um evento iniciador. Como as árvores de eventos são baseadas em lógica binária, esta acaba por possuir muitos ramos, fazendo a análise demasiadamente complexa (KUMAMOTO; HENLEY, 1996).

Outra deficiência do THERP é que as tabelas de probabilidade de erro humano foram construídas a partir de estudos e para a utilização na indústria nuclear. Para utilização em outras situações, como em análises na área naval (ver (MATURANA; MARTINS, 2008)), deve-se fazer uma associação entre as tarefas, assumindo que tarefas semelhantes terão probabilidades de erro parecidas, ou pelo menos, de mesma ordem de grandeza. Dependendo da atividade, essa aproximação pode ser por demais grosseira. Uma alternativa é reavaliar as probabilidades tabeladas através da consulta a especialistas, ou apenas utilizar os resultados do THERP para fins de comparação e classificação das alternativas de redução do risco.

3.3.3.7. Seleção dos métodos

A seleção de uma técnica de análise de confiabilidade humana para uma aplicação segue o mesmo princípio da seleção das técnicas de análise de risco, comentada anteriormente. O analista deve ponderar a quantidade de dados disponíveis, recursos humanos e tempo de análise. Resumidamente, e de forma simplista e simplificada, porém útil, Kumamoto e Henley (1996) propõem alguns critérios para a seleção das técnicas apresentadas nas seções anteriores, conforme exposto na Tabela 16.

Tabela 16 – Métodos de ACH e tipos de erro
– adaptado de (KUMAMOTO; HENLEY, 1996, p. 499)

Tipo de erro	Método
Antes do evento iniciador	
Erro de teste e manutenção	THERP
Para o evento iniciador	
Causa do evento iniciador	Experiência Estimativa de especialistas
Durante o acidente	
Operador não responde	HCR
Ações erradas	Matriz de confusão
Deslize e lapso	THERP, SLIM
Falhas na recuperação	THERP, SLIM, HCR

3.3.3.8. Críticas aos métodos da primeira geração

Em seu livro denominado “*Cognitive Reliability and Error Analysis Method*”, Erick Hollnagel (1998) apresenta críticas severas e sensatas sobre os métodos da primeira geração de ACH.

A primeira delas é que a maioria dos métodos de análise de confiabilidade humana da primeira geração é baseada nos princípios da análise probabilística de segurança, sem se preocupar com as implicações deste fato, como as limitações da aplicação dos métodos ao ser humano. Nenhum dos métodos apresenta uma teoria bem fundamentada em termos dos modelos de cognição humana, ou apresenta tratamento adequado sobre os “erros cognitivos”. Tampouco, os fatores de

condicionamento de desempenho possuem uma explicação bem definida de sobre como exercem influência no desempenho do indivíduo.

Além disso, existem casos onde o comportamento humano é uma função cognitiva, e o uso de árvore de eventos acaba por não fazer sentido. O comportamento humano não deve ser simplesmente modelado como um resultado binário de sucesso ou insucesso, assim como é feito nas análises de confiabilidade de sistema. Os métodos de primeira geração também pecam no tratamento dos erros de comissão. Existe diferença entre falhar em realizar a ação correta, e falhar em realizar uma ação corretamente. Ações bem intencionadas com resultados indesejados ainda não possuem um tratamento apropriado.

A escassez de dados para a predição quantitativa do comportamento humano também é uma limitação, assim como a inexistência de demonstrações sobre a acurácia das estimativas no mundo real. Os dados existentes, como as tabelas de HEP, contém alto nível de incertezas, além de terem sido desenvolvidas para uma aplicação específica, a indústria nuclear, a qual não é sempre semelhante às aplicações das outras indústrias.

Todavia, isso não significa que nenhum método não tenha seu valor, já que cada método foi desenvolvido para uma necessidade prática específica, e vários deles já foram largamente utilizados. Novamente, muitas destas críticas giram em torno das visões distintas (prática ou teórica, preditiva ou psicológica) a cerca do estudo do comportamento humano.

3.3.4. Técnicas da segunda geração

A introdução do conceito de técnicas de primeira geração criou o problema de definir o que seriam métodos de segunda geração. Hollnagel (1998) propõe utilizar o critério cronológico, estabelecendo o ano de 1991 como divisão entre a primeira e segunda geração. Os principais métodos de segunda geração são:

- CES – *Cognitive Enviroiment Simulator*: uma ferramenta de simulação, que analisa a formação de intenção do operador, através da geração de dados via simulador.
- INTENT: uma extensão do método THERP para a análise de erros de intenção.

- COGENT – *Cognitive Event Tree System*: também uma extensão do método THERP, que aperfeiçoa a construção da árvore de eventos
- HITLINE – *Human Interaction Timeline*: baseia-se em um programa de computador que gera sequências de ações humanas, incluindo erros, ao longo do tempo. A simulação utiliza um modelo lógico da planta e múltiplas árvores de eventos, correspondendo às diferentes condições iniciais.
- ATHEANA – *A Technique for Human Error Analysis*: método desenvolvido por Cooper, Ramey-Smith e Wreathall (1996) para a U.S. Nuclear Regulatory Commission, agência nuclear americana. O método busca prover uma base psicológica robusta para avaliar e identificar os fatores de condicionamento de desempenho (PSF), incluindo fatores organizacionais e ambientais.
- CREAM – *Cognitive Reliability and Error Analysis Method*.

Desta lista, os métodos de maior destaque são o ATHEANA e CREAM. Apenas o método CREAM será tratado neste trabalho como potencial candidato a técnica de ACH a ser utilizada no modelo proposto adiante. Para maiores detalhes sobre o método ATHEANA, o leitor poderá consultar adicionalmente Forester et al. (2007).

3.3.4.1. Cognitive Reliability and Error Analysis Method (CREAM)

O método CREAM, proposto por Hollnagel (1998), é baseado em vários princípios existentes nos métodos de primeira e segunda geração. O método permite realizar tanto análises retrospectivas (como análises de acidentes com o objetivo de investigar e compreender os mecanismos da falha ocorrida), quanto análises preditivas (que buscam prever o desempenho humano). Sob este ponto de vista, o autor o denomina de “bidirecional”. Além disso, o método pode ser aplicado tanto para análises qualitativas quanto quantitativas. O método permite ao analista:

1. Identificar partes do trabalho, como tarefas e ações, que requerem ou dependem da cognição humana, e podem afetar a confiabilidade humana;

2. Determinar as condições sob as quais a confiabilidade humana pode ser reduzida, e onde estas ações podem se tornar uma fonte de risco;
3. Desenvolver e especificar modificações para melhorar estas condições, aumentando a confiabilidade humana e reduzindo o risco.

Segundo seu autor, o CREAM pode ser utilizado como um método de análise “*stand-alone*”, para análise retrospectiva ou preditiva; como ferramenta de projeto para sistemas complexos; ou como nas análises e avaliações de segurança ou análise probabilística de risco.

O método é fundamentado em três pilares: (i) utilizar um modelo de cognição humana; (ii) elaborar um sistema de classificação; e (iii) aplicar as influências das Condições de Desempenho Comum (ver subseção 3.3.2), explicando como isso ocorre, e sua interdependência.

Sua grande inovação em relação aos métodos anteriores foi reconhecer que as ações humanas acontecem dentro de um contexto, e por isso, é fundamental descrever como o contexto exerce a influência nas ações. De fato, como será visto adiante, a quantificação da probabilidade de erro não julga o erro humano em si, mas somente o contexto em que este ocorre.

O modelo de cognição humana utilizado pelo CREAM é chamado de COCOM (*Contextual Control Model*), criado pelo próprio autor do CREAM (HOLLNAGEL, 1993a). Este método é uma evolução de outro modelo denominado de SMoC (*Simple Model of Cognition*), que reflete o consenso geral das características humanas desde as pesquisas iniciais na década de 1950. O modelo SMoC, mostrado na Figura 29, é dividido em apenas quatro fases (observação, interpretação, planejamento/escolha e execução), e tem como objetivo descrever características básicas da cognição humana. As quatro fases do SMoC são inter-relacionadas, organizadas em um modelo cíclico, como forma de representar as várias maneiras pelas quais as funções cognitivas podem se apresentar. Desta forma, este modelo pode resultar um modelo cognitivo sequencial, de acordo com o problema analisado.

Figura 29 – Modelo de SMoC
– adaptado de (HOLLNAGEL, 1998, p. 100)

O modelo COCOM defende que as atividades humanas nem sempre possuem uma natureza sequencial, e que as funções cognitivas são conectadas entre si, de acordo com o contexto. Conforme apresentado pela Figura 30, as atividades são agrupadas em duas categorias:

- O modelo de competência: que são as funções cognitivas essenciais, como observação, interpretação, planejamento e execução.
- O modelo de controle: representa como o indivíduo seleciona as atividades e gerencia a sua execução. O autor faz distinção de quatro modos de controle:
 - Controle desordenado: o controle da próxima ação é imprevisível e causal. Nesta situação, há pouco ou nenhum pensamento envolvido. Típico de situações de pânico.
 - Controle oportunista: a próxima ação é determinada pelas características do contexto, em vez de intenções ou metas pré-estabelecidas. Típico de situações para resolver um problema imediato, sem tempo de diagnóstico.
 - Controle tático: o desempenho é baseado em planejamento, e segue um procedimento ou regra. Corresponde ao comportamento baseado em regras.
 - Controle estratégico: o indivíduo considera o contexto global, utilizando um amplo horizonte de tempo, e metas de alto nível.

Figura 30 – Modelo de COCOM
– adaptado de (HOLLNAGEL, 1998, p. 155)

Definido o modelo de cognição humana do método CREAM (o modelo COCOM), para seguir com a explanação é necessário percorrer o conceito de “esquema de classificação” definido por Hollnagel (1998). O esquema de classificação existe para prover base para descrever os eventos de um acidente e identificar suas possíveis causas. O esquema de classificação deve ser capaz de descrever todas, ou a maioria das formas de manifestações de ações errôneas, e a maioria das suas causas. O nível de detalhe ótimo deve ser aquele que impede que alguma informação importante se perca, e que seja simples o suficiente para ser gerenciável. O esquema de classificação faz a distinção entre efeitos ou manifestações (fenótipo) e causas (genótipo), organizados em grupos de classificação.

O esquema de classificação está disposto em um extenso número de tabelas, divididos em grupos de classificação, indicadas a seguir:

- Modos de erro (Fenótipos):
 - Ações na hora errada;
 - Ações do tipo errado;
 - Ações no objeto errado;
 - Ações no lugar errado.
- Genótipos relativos ao homem:
 - Observação;

- Interpretação;
- Planejamento;
- Funções temporárias relativas às pessoas;
- Funções permanentes relativas às pessoas.
- Genótipos relativos à tecnologia:
 - Falha de equipamentos;
 - Procedimentos;
 - Falhas temporárias da interface;
 - Falhas permanentes da interface.
- Genótipos relativos à organização:
 - Comunicação;
 - Estruturação;
 - Treinamento;
 - Condições do ambiente;
 - Condições de trabalho;

As causas são estruturadas na tríade MTO (*Man-Technology-Organisation*), conforme visto na Figura 31, onde os genótipos homem, tecnologia e organização possuem suas causas agrupadas.

Figura 31 – Modelo de classificação do CREAM
– adaptado de (HOLLNAGEL, 1998, p. 160)

Os modos de erro se referem às características observáveis das ações, e as consequências dos erros descrevem seus efeitos no sistema. De forma simples, os modos de erros descrevem como uma ação incorreta pode se manifestar. Pode existir um número exaustivo de modos de erro, mas o CREAM utiliza apenas quatro, por razões de praticidade.

Cada grupo de classificação possui seu consequente específico e antecedente geral e específico. Os grupos não possuem uma característica hierárquica entre si, ou seja, existe um relacionamento livre entre eles que será definido na análise do evento em questão. Para tal, cada consequência descrita em um grupo precisa corresponder a um, ou mais, antecedente em outros grupos. Para cada consequência, uma lista de antecedentes prováveis (possíveis explicações) deve existir. Cada um desses antecedentes são, também, consequências em outro grupo, ou para a causa raiz.

Conforme mencionado no início desta subseção, o método CREAM é considerado bidirecional, servindo tanto para análises retrospectivas (análises de acidentes, por exemplo), quanto para análises preditivas (predição do desempenho humano). Para a análise retrospectiva qualitativa, os seguintes passos devem ser seguidos:

1. Determinar ou descrever o contexto;
2. Descrever os possíveis modos de erro;
3. Descrever as possíveis causas;
4. Analisar em detalhe para estabelecer as conexões entre os antecedentes e consequentes.

O passo 1 é feito através do preenchimento da escolha do estado de cada CPC (*Common Performance Conditions*, ou Condições de Desempenho Comum), descritos na segunda coluna da Tabela 7 (pág.81).

O passo 2 é feito escolhendo-se os possíveis, prováveis e impossíveis modos de erro, extraídos das tabelas de grupos de classificação. O método também se caracteriza por ter um critério de parada bem definido, que ocorre quando, durante a análise, não se encontram antecedentes gerais prováveis.

Para predição do desempenho humano, o principal pré-requisito é descrever o provável contexto, através dos CPCs (Tabela 7, pág.81). Esta é uma diferença básica em relação a outros métodos da ACH, uma vez que o CREAM requer a

estimativa do contexto provável pelos CPCs, e não de eventos específicos. Em caso da necessidade de se obter resultados numéricos da probabilidade de determinado evento ocorrer, por exemplo, para fins de uma PRA, o CREAM propõe duas abordagens: a básica e a estendida. O problema de quantificação no método CREAM, todavia, é consideravelmente simplificado, uma vez que o método prioriza as situações e condições de trabalho, em vez de ações individuais.

A abordagem básica para predição quantitativa de desempenho humano produz uma avaliação da confiabilidade do desempenho de uma tarefa determinada. O resultado é expresso em uma probabilidade de falha da tarefa. Resumidamente, três passos são necessários:

1. Descrever a tarefa ou segmentos da tarefa a ser analisada;
2. Avaliar os CPCs;
3. Determinar o provável modo de controle (segundo o modelo COCOM).

A avaliação dos CPCs é feita através da obtenção do resultado combinado dos 9 CPCs da Tabela 7 (pág. 81): CPCs que reduzem a confiabilidade, CPCs que não causam efeitos significativos e CPCs que melhoram a confiabilidade. Esse resultado é expresso em um vetor com três componentes: (Σ_{reduzem} , $\Sigma_{\text{não significativo}}$, Σ_{melhoram}). Descartando-se os CPCs não significativos, é possível extrair o modo de controle pelo gráfico da Figura 32:

Obtido o modo de controle provável, a probabilidade de falha da ação é obtida a partir da Tabela 17. O autor não dá detalhes de como estes intervalos de probabilidade foram calculados, apenas cita que “estes valores são comumente aceitos na literatura sobre análise da confiabilidade humana”. Como exemplo, para um resultado de CPC igual a (3, 5, 1), tem-se o modo de controle oportunista, e o intervalo de probabilidade é de 0,01 a 0,5.

Segundo Hollnagel (1998) são duas as diferenças básicas do método básico para os demais métodos quantitativos de ACH: (i) o método usa como ponto de partida o contexto, e não o inverso, ou seja, usa o contexto para alterar as probabilidades das ações; (ii) o método se refere a um modelo explícito de cognição, o que provê uma base racional para os resultados.

Figura 32 – Matriz de resultado do CPCs e modos de controle
– adaptado de (HOLLNAGEL, 1998, p. 239)

Tabela 17 – Intervalo de probabilidades dos modos de controle

Modo de Controle	Intervalo de confiabilidade (probabilidade de falha da ação)
Estratégico	$0,00005 < p < 0,01$
Tático	$0,01 < p < 0,1$
Oportunista	$0,01 < p < 0,5$
Desordenado	$0,1 < p < 1,0$

O método estendido do CREAM envolve a construção do perfil cognitivo de demanda da tarefa, e uma avaliação mais extensa das funções cognitivas. Esta avaliação faz com que sua aplicabilidade seja mais restrita, por exigir conhecimentos específicos do analista. Por este motivo, o método estendido não será tratado neste trabalho.⁹ Este método possui a vantagem de permitir que o resultado do cálculo da probabilidade de falha seja um número único em vez de um intervalo, apesar de conter tantas incertezas quanto.

⁹ Para maiores detalhes, recomenda-se consultar Hollnagel (1998). O método estendido foi revisado por Fujita e Hollnagel (2004), os quais apresentaram uma nova modelagem de cálculo do resultado dos CPCs.

3.4. Análise de sensibilidade

Os mesmos conceitos acerca da análise de sensibilidade nas análises de risco apresentados na subseção 2.4.3 valem para a análise da confiabilidade humana. Filgueiras (1996) propõe analisar a sensibilidade da confiabilidade, alterando-se os valores das variáveis de contexto, um termo que engloba os fatores de condicionamento de desempenho, sejam eles PSF ou CPC (ver seção 3.3.2, pág. 78).

Com o objetivo de avaliar as variações positivas e negativas do comportamento dos operadores, os gestores das empresas podem alterar essas variáveis de contexto, como treinamento, condições de trabalho, políticas organizacionais, remuneração, entre outros, e verificar o impacto sobre o resultado final da análise.

Filgueiras (1996) considera os seguintes passos para a análise de sensibilidade do erro humano em relação ao contexto:

1. Para cada cenário, selecionar as variáveis de contexto pertinentes, por exemplo, as listadas na Tabela 6 (pág. 80) e na Tabela 7 (pág. 81);
2. Classificar as variáveis de contexto de acordo com sua importância relativa, atribuindo um peso relativo à sua importância em relação às outras, denominado o índice de qualidade da influência (q_i): a menos significativa recebe peso 10 e as demais, múltiplos deste valor;
3. Construir uma tabela de decisão considerando os estados associados a cada variável;
4. Identificar a influência dos estados de cada variável na probabilidade de insucesso do cenário; atribui-se um valor r_i entre 0 e 1, se o estado favorece o erro humano, e acima de 1, se o estado da variável compensa o erro humano;
5. Calcular a influência relativa do contexto sobre o cenário (IC), para esta condição composta sobre o cenário, pela fórmula:

$$IC = \sum_i r_i \frac{q_i}{\sum_i q_i} \quad (15)$$

A Tabela 18 mostra um exemplo de aplicação para três variáveis de contexto. Neste exemplo de problema, deseja-se analisar três variáveis de contexto relativas ao trabalho de um operador em uma planta: experiência do operador, tempo de reação, e condições de trabalho. Para estas três variáveis de contexto, o analista arbitra seus pesos relativos q_i e diferentes estados, como por exemplo, “experiente”, “mediano” e “novato”, para a variável de contexto “experiência do operador”. A quantidade de estados é definida pelo próprio analista. Os valores r_i são atribuídos conforme critério explicado no passo 4.

Tabela 18 – Exemplo de aplicação da análise de sensibilidade

Variáveis de contexto	q_i	Estados					
		r_i		r_i		r_i	
Experiência do Operador	70	Experiente	8	Mediano	1,2	Novato	0,5
Tempo de Reação	50	Adequado	5	Inadequado	0,8		
Condições de Trabalho	10	Adequado	3	Limitado	0,3		
$\sum q_i$	130						

Após a atribuição dos valores de influência de cada estado, o resultado final desta análise é uma árvore de decisão com os valores de IC, conforme apresentada na Figura 33. Os cálculos das duas primeiras sequências estão indicados na figura. Esta árvore permite ajustar os valores de influência de cada estado em função dos demais, refletindo as dependências entre as variáveis de contexto.

3.5. Revisão bibliográfica de metodologias para incorporar fatores humanos e organizacionais em PRA

O problema de incorporar nas análises probabilísticas os fatores organizacionais não é trivial e, por isso, diferentes abordagens são encontradas em publicações da área. As principais dificuldades foram abordadas anteriormente na subseção 3.1.4.

Figura 33 – Árvore de decisão da análise de sensibilidade

Os seguintes trabalhos foram considerados mais relevantes, e foram objeto de estudo detalhado para a elaboração do modelo deste trabalho:

- Metodologia BORA (*Barrier- and Operational Risk Analysis*) de Aven, Hauge e Vinnen (2006)
- Abordagem do fator ω para inclusão dos fatores organizacionais na PRA, de Galán, Mosleh e Izquierdo (2007)
- Metodologia de avaliação de risco focada em fatores humanos e organizacionais de Ren et al. (2008).
- Sistema de classificação e análise de fatores humanos (HFACS) de Celik e Cebi (2009).
- Modelagem baseada em risco para análise de acidentes com embarcações de Celik, Lavasani e Wang (2010).
- Metodologia SAM de Murphy e Paté-Cornell (1996).

A metodologia BORA é um método que foi desenvolvido para incorporar fatores humanos e organizacionais nas análises de risco de plataformas de petróleo no Mar do Norte. O método se baseia no cálculo ou estimativa de frequência e probabilidades de eventos iniciais que significam um fator de risco para a planta. Quando estes valores não estão disponíveis na indústria, a opinião de especialistas é utilizada para quantificar o risco de um evento topo de uma árvore de falhas. Os fatores humanos e organizacionais são considerados como “fatores de influência de risco”, através de diagramas de influência. O método alcança resultados quantitativos, mas não utiliza a formulação das probabilidades condicionais nas análises probabilísticas, e sim árvores de falhas e eventos. A abordagem por árvore de falhas tem a desvantagem de não conseguir representar a complexidade dos erros humanos e fatores organizacionais. Além de tornar a análise exponencialmente complexa, na medida em que se aprofunda nos detalhes do acidente. No entanto, no passado esta abordagem era considerada um recurso válido, conforme (NUREG, 1981a).

Galán et al. (2007) fazem uma abordagem semelhante para instalações nucleares, lançando mão de redes bayesianas para quantificar a influência de fatores organizacionais em usinas nucleares. Neste trabalho, um modelo paramétrico dos fatores organizacionais é proposto, chamado de fator ω , objetivando representar a estrutura de uma organização. O fator ω é calculado da seguinte maneira:

$$\omega = \frac{\text{taxa de falha inerente que não depende da organização}}{\text{taxa de falha devido a erros organizacionais}} \quad (16)$$

Esta abordagem não se mostrou aplicável no presente trabalho por não utilizar qualquer modelo de comportamento humano, ou explicar como e onde os fatores organizacionais podem influenciar o desempenho de um operador.

A metodologia de avaliação de risco focada em fatores humanos e organizacionais, de Ren et al. (2008), apresentam uma visão ampla e moderna sobre os fatores humanos e organizacionais, incorporando os conceitos do modelo do queijo suíço de Reason (1990a). Nesta proposta, os autores empregam redes bayesianas para superar as limitações do modelo de Reason em representar as

inter-relações e probabilidades dos eventos. O modelo conceitual do acidente considera cinco níveis: nível de causa, nível do evento disparo, nível de incidente, nível de acidente, e nível de consequência. Busca-se demonstrar as correlações entre os fatores organizacionais através da elaboração de uma rede bayesiana do problema, e calcular as probabilidades através de funções de pertinência Fuzzy.

Celik e Cebi (2009) propõem o método HFACS para a quantificação dos erros humanos na investigação de acidentes a partir de relatório de acidentes. O objetivo é classificar em ordem de importância os fatores que contribuíram para o acidente, identificando os erros humanos latentes. A metodologia de análise é dividida em quatro níveis: nível das ações, pré-condições, supervisão e influências organizacionais. A metodologia permite descobrir as conexões latentes entre cada nível, e em seguida, quantificar por meio de consulta a especialistas, a relevância de cada fator. O método também é baseado no modelo de Reason para fundamentar a proposta de análise. No entanto, o método trata o acidente como um todo, e não de forma sequencial, evento por evento. Os fatores organizacionais são considerados na análise da mesma maneira como os demais fatores contribuintes, e seu peso é determinado segundo a ponderação das respostas dos especialistas.

A abordagem de Celik, Lavasani e Wang (2010) também busca compreender melhor os mecanismos que causaram um acidente marítimo, a partir da análise de relatório de acidentes. A proposta de análise de risco busca combinar as falhas organizacionais com as falhas técnicas, através de uma árvore de falha Fuzzy estendida (FFTA – *fuzzy extended fault tree analysis*). A árvore de falhas da embarcação é construída e dividida por uma porta “OU” entre falhas técnicas e organizacionais. E desta forma, calculando-se os “*cut-sets*” tem-se o caminho crítico e as dependências entre os componentes, físicos ou organizacionais. O método não aprofunda nenhum modelo de cognição humana ou de análise de fatores organizacionais, mas trata os erros humanos e organizacionais como um componente físico na árvore de falhas.

A metodologia SAM, de Murphy e Paté-Cornell (1996) tem o objetivo de expandir a análise probabilística de risco e incorporar as ações e decisões dos indivíduos que afetam o sistema físico. A metodologia SAM é abrangente e se aplica a qualquer PRA que se deseja realizar. A proposta do modelo SAM é ligar o desempenho do sistema às ações (erradas ou não) dos operadores, e estas ações a fatores gerenciais, que são geralmente moldados pela estrutura, procedimentos e

4. SISTEMAS DE ALARMES PARA EMBARCAÇÕES E ERROS HUMANOS ASSOCIADOS

Pode-se dizer que a automação tem como finalidade a substituição conveniente do elemento humano pela máquina. A conveniência da substituição é determinada por fatores diversos, tais como a hostilidade de certos ambientes à vida humana ou o ganho de produtividade de uma certa tarefa (FILGUEIRAS, 1996, p. 12).

4.1. Considerações iniciais

Em embarcações modernas, a automação das máquinas já é um assunto tratado com naturalidade pela tripulação, obrigada a interagir com vários sistemas eletrônicos instalados a bordo. A interação humana com esses sistemas é suscetível à ocorrência de erros humanos. O objetivo deste capítulo é discorrer a respeito do equipamento responsável pela monitoração de sensores e do estado dos sistemas a bordo, e por anunciar os eventos anormais à tripulação.

O sistema de alarmes, presente em embarcações de pequeno a grande porte (desde rebocadores a navios tanque), promove a segurança ao evitar erros humanos nas atividades em que a máquina atua de forma mais eficiente que o homem, como em funções repetitivas, rotineiras e monótonas. Por exemplo, na verificação de nível dos tanques, ou em funções que requerem resposta muito rápida, ou que exijam a monitoração de muitas variáveis, como as atividades de supervisão.

O capítulo ainda abordará os aspectos técnicos do sistema exigidos nas normas publicadas pelas sociedades classificadoras do setor naval, aspectos sobre suas funções relacionadas à operação e problemas, e a relação do sistema de alarmes com eventos indesejados. Também se pretende justificar a existência do sistema de alarmes nas embarcações como item obrigatório, e sua importância e função no modelo de análise de risco a ser proposto nesta tese.

4.2. Definições básicas

Abaixo estão apresentadas algumas definições fundamentais sobre alarmes e sistemas de alarmes, adaptadas de relatórios e diretrizes de IMO (1991) e ABS (2008b):

- Alarme: sinal visual e audível indicando uma condição anormal de um parâmetro monitorado.
- Sistema de alarmes: sistema que anuncia por meio sonoro, ou sonoro e visual, uma condição que requer atenção.
- Sistema de monitoramento: sistema projetado para supervisionar os estados das máquinas e sistemas por meio de instrumentação, o qual provê monitores para visualização dos parâmetros operacionais e alarmes, indicando condições anormais.
- Sistema de controle: conjunto de equipamentos conectados para transmitir comando ou ordem para efetuar uma ação desejada.
- Indicador: indicação visual que informa a condição de um sistema ou equipamento
- Alarmes de emergência: alarmes que indicam perigo imediato à vida humana ou às máquinas, e que implica uma ação imediata.
- Alarmes primários: alarmes que indicam uma condição em que uma ação imediata deve ser tomada para evitar uma condição de emergência
- Alarmes secundários: alarmes que não são nem de emergência, nem primários.
- Aceitar um alarme: silenciar manualmente um alarme sonoro, de uma posição remota.
- Reconhecer um alarme: silenciar manualmente um alarme sonoro, do local do equipamento, fazendo com que o alarme visual fique em um estado estável.
- Cancelar um alarme: manualmente parar um alarme visual, após sua causa ser eliminada.

- Agrupamento de alarmes: é a combinação de vários alarmes individuais em apenas um alarme, em uma posição remota, por exemplo, no passadiço, de forma a facilitar a visualização remota. Os alarmes podem ser agrupados por sistema (por exemplo: alarme do gerador) ou por prioridade, como alarmes de emergência, primários, etc.

O sistema que será tratado nesta tese abrange as funções de um sistema de alarme e monitoramento. Todavia, para simplificação da nomenclatura, este sistema será tratado como apenas “sistema de alarmes”.

Na literatura sobre sistemas de alarmes, os termos “sistemas de supervisão” ou “sistemas supervisórios” também podem ser encontrados. No entanto, estes termos estão mais relacionados aos sistemas que monitoram e controlam processos industriais, como em indústrias químicas; ou a empresas de transporte, como um sistema de supervisão de uma linha de metrô. As semelhanças técnicas e funcionais entre um sistema de alarmes de um navio e de uma indústria são grandes. No entanto, os sistemas na indústria são focados nos processos, para garantir a qualidade e desempenho da produção, além da redução de custos operacionais. Em embarcações, o foco principal é a segurança, através da sinalização de uma situação anormal para posterior intervenção da tripulação.

4.3. Histórico

Nas décadas passadas, a operação dos navios requeria o monitoramento constante da tripulação na praça de máquinas, exercendo atividades de verificação de água, óleo, limpeza, e manutenção. A tripulação era obrigada a se dividir em turnos, a fim de manter a operação das máquinas sem interrupções. O avanço tecnológico, inclusive do sistema de alarmes, contribuiu para automatizar muitas destas tarefas, tornando realidade a operação de uma praça de máquinas desguarnecida. A automação permitiu a redução do número de tripulantes, a implantação de políticas de manutenções preditivas, baseadas em monitoração sofisticada das máquinas, e o monitoramento remoto da praça de máquinas.

Os sistemas de alarmes nasceram e evoluíram juntamente com os sistemas de controle e monitoramento industriais. Alguns sistemas para uso naval também foram adaptados a partir de Controladores Lógicos Programáveis (CLPs), desenvolvidos no final da década de 1960, e hoje, largamente utilizados na indústria. Os monitores para visualização também seguiram as tendências da indústria, evoluindo dos painéis simples com indicadores luminosos, para monitores coloridos e LCD, com comandos através de telas sensíveis ao toque.

4.4. Componentes do sistema de alarmes

Analogamente a um CLP, o sistema de alarmes é um equipamento eletrônico microprocessado, composto por “*hardware*” e “*software*”, e com memória interna para armazenagem de instruções e para implementar funções específicas, tais como lógica, temporização, contagem e aritmética. O sistema é composto por um ou mais módulos, que exercem basicamente três funções principais, conforme apresentado na Figura 35: a aquisição dos dados dos sensores, o processamento das informações e regras de alarmes, a distribuição das informações para os monitores.

Figura 35 – Componentes típicos do sistema de alarmes

O sistema também pode também possuir módulos de saídas, para comandar atuadores ou sistemas externos. Neste caso, o sistema não possui apenas funções de monitoramento, mas é caracterizado por ser um sistema de alarmes, monitoramento e controle de embarcações. Este trabalho se limitará às análises dos sistemas de alarmes sem as funções de controle. Sob o ponto de vista das certificadoras, os sistemas que também desempenham a função de controle são enquadrados em outra classe de equipamentos, e recebem exigências de confiabilidade muito maiores.

Em relação ao tipo de entradas por eles suportado, os sistemas de alarmes são divididos em dois tipos. O primeiro tipo de sistema de alarmes compreende os sistemas que fazem a leitura de entradas puramente binárias. Entradas binárias são aquelas que possuem apenas dois estados, como ligado ou desligado, aberto ou fechado, 0 ou 1. Estes sistemas fazem a leitura de contatos, como contatos de relés normalmente abertos ou normalmente fechados.

O segundo tipo compreende os sistemas que leem entradas binárias e sinais analógicos. Os sinais analógicos mais comuns são sinais de 4 a 20 mA; tensões de 0 a 5 Volts ou 0 a 10 Volts; resistências como potenciômetros, e termorresistências. A capacidade do sistema de alarmes é medida pelo número de entradas monitoradas.

Vale observar que os sensores instalados nas máquinas não necessariamente possuem função exclusiva para o sistema de alarmes. É possível que o sistema de alarmes monitore um sensor que ao mesmo tempo é utilizado para uma função própria do sistema monitorado. Um possível exemplo é um sensor de pressão de um motor servindo para um alarme de pressão no sistema de alarmes, e como sistema de parada de segurança do próprio controlador motor. Isto pode valer tanto para sensores analógicos como digitais. Além disso, também é possível encontrar no mercado sensores com mais de uma saída de sinal, justamente para serem monitorados por mais de um sistema.

Os alarmes e indicadores sejam eles digitais ou analógicos são exibidos nos monitores espalhados na embarcação. Via de regra, o monitor principal é instalado na praça de máquinas, e repetidores são alocados no passadiço e demais localidades, como cabines, refeitório, etc. Os módulos responsáveis pelo

processamento e distribuição dos indicadores e alarmes têm a função de enviar as informações aos monitores que devem exibir este dado.

O sistema de alarmes pode possuir uma arquitetura centralizada, ou distribuída (ver Figura 36). Na arquitetura centralizada, as atividades de processamento recaem sobre a figura de um único gerente. Esta arquitetura resulta em baixa confiabilidade do sistema, uma vez que falhando o elemento central, todo o sistema perde sua função. Na arquitetura distribuída, cada componente, ou nó, possui uma função específica, e atua de forma independente. No caso de falha de um componente, apenas as funções daquele componente são perdidos, e a confiabilidade do sistema como um todo é maior.

Em um navio, a arquitetura distribuída é extremamente desejável pelo fato de otimizar o cabeamento, uma vez que as unidades de entradas podem ser dispersas pela embarcação, sendo instaladas perto das entradas (dos sensores). Na arquitetura distribuída, as centrais de aquisição ou processamento de dados são interligadas entre si com apenas um cabo de dados, e se comunicam através de protocolos padrão de comunicação, como os protocolos Modbus, CAN Bus, Profibus, entre outros, que usualmente também são utilizados em sistemas de automação industrial. A Figura 37 exibe um exemplo de aplicação de um sistema com arquitetura distribuída, onde os componentes de 1 a 5 são instalados em diferentes localidades na embarcação.

Figura 36 – Arquiteturas centralizada e distribuída dos sistemas de alarmes

Figura 37 – Exemplo de sistemas de alarmes com arquitetura distribuída

Para um alarme ou indicador binário, os principais parâmetros a serem programados são (i) se o ponto monitorado é um indicador ou um alarme; (ii) se o sensor é NA (normalmente aberto) ou NF (normalmente fechado); e (iii) os atrasos de ativação ou desativação, ou seja, após a mudança de estado (para anormal ou normal) quanto tempo o sistema deve esperar para sinalizar ou desligar um alarme ou indicação. A principal função dos atrasos é evitar falsos alarmes devido a condições transientes do sistema, ou sinais espúrios.

Para um alarme ou indicador analógico, os principais parâmetros programáveis são mais complexos. Além de ser possível programar se o ponto monitorado é um alarme ou indicador, e os atrasos de ativação e desativação, geralmente a curva do sinal do sensor deve ser também informada ao sistema. Para sensores lineares, esta programação é simplificada, por ser necessário entrar apenas com dois valores do sensor. Exemplo: para um sensor de pressão, com pressão nominal de 10 bar e com sinal de saída de 4 a 20 mA, bastaria entrar com os valores $4\text{mA} = 0\text{ bar}$ e $20\text{mA} = 10\text{ bar}$.

Também é necessário programar os limites de alarmes e pré-alarmes de máximo e de mínimo. A Figura 38 apresenta um exemplo de um sensor de pressão que faz a leitura de pressões de 0 a 10 bar, dando um sinal de saída linear de 4 a 20 mA. A faixa de operação normal, ou seja, a situação sem alarmes é indicada na figura. As faixas de pré-alarme de máximo e de mínimo servem para o sistema dar um aviso, que a pressão está se aproximando do limite da faixa de alarme. Nem

sempre é necessário programar limites de alarme de máximo e mínimo. Há situações em que apenas deseja-se alarmar uma das situações, como, alarme de nível de tanque de combustível mínimo, ou alarme de temperatura alta, não fazendo sentido ter um alarme de tanque de combustível cheio ou alarme de temperatura baixa.

Por fim, alguns fabricantes permitem programar a supressão alarmes de sensores, ou seja, quando uma das entradas suprime os alarmes de outros sensores. Um caso típico é quando os alarmes de tensões e correntes de saída de um gerador devem ser suprimidos se o sinal de “gerador ligado” não é recebido. Logicamente, se o gerador estiver desligado, não faz sentido alarmar que as tensões e correntes de saída estão fora dos valores normais de operação. A supressão de alarmes exige muito cuidado no projeto e pode ser entendida como um filtro de alarmes evitando o inconveniente problema de avalanche de alarmes.

Figura 38 – Faixas de operação do sensor e alarmes

4.5. Exigências das sociedades classificadoras

Apesar das principais sociedades classificadoras de embarcações possuírem requisitos similares sobre sistemas de alarmes, existe uma grande variabilidade no que diz respeito ao que se deve monitorar de acordo com o porte e função da embarcação. Esta seção tem por objetivo expor a base destas exigências de forma a familiarizar o leitor sobre o equipamento. Não se pretende criticar ou analisar estas exigências, e tampouco citá-las em detalhes.

O capítulo V da norma SOLAS (ver seção 2.3) trata na Regulamentação 15 sobre princípios de projeto de pontes de comando. Segundo esta diretriz, o projeto da ponte de comando deve ter como objetivo, entre outros, “minimizar o risco de erro humano e detectar este tipo de erro. No caso de ocorrer, a tripulação do passadiço e piloto devem tomar as ações apropriadas em tempo, através do sistema de alarmes e monitoramento” (IMO, 2004, p. 367).

A IMO ainda acrescenta outros objetivos para o sistema de alarmes, como permitir ao oficial devotar completa atenção à navegação segura do navio; permitir a identificação imediata de qualquer situação anormal que requer alguma ação para manter a navegação segura do navio; evitar distrações de alarmes que requerem atenção, mas não exercem influência na segurança da navegação ou que não requerem ação imediata para restaurar ou manter a navegação segura (IMO, 2007). Este último, indica que os alarmes devem ser minimizados, e somente os alarmes e indicadores requeridos pelas resoluções da IMO devem ser exibidos.

A norma ABS intitulada, “*Guide for automatic or remote control and monitoring for machinery and system (other than propulsion) on offshore installations*”, apresenta tabelas com os alarmes necessários para os seguintes sistemas (ABS, 2008a):

- Motores diesel
- Turbinas (a vapor ou gás)
- Caldeiras (a óleo, ou a óleo cru, ou metano)
- Plantas de geração de energia elétrica
- Aquecedores a óleo
- Motores a combustão
- Máquinas/sistemas que manipulam líquidos perigosos

- Incineradores
- Geradores de gás inerte
- Geradores de nitrogênio
- Caldeira de reaproveitamento de calor
- Sistema de óleo combustível.

A Tabela 19 apresenta o exemplo específico dos alarmes exigidos para plantas de geração de energia elétrica. Os limites dos alarmes e pré-alarmes não são mencionados, pois são específicos de cada equipamento.

Tabela 19 – Tabela de alarmes para plantas de geração de energia elétrica
– adaptado de (ABS, 2008a)

Sistema	Alarme	Exibição
Gerador	Falha	Em operação
Tensão	Alta/Baixa	Volts
Corrente	Alta	Amp.
Frequência	Alta/Baixa	Hz
Pressão do óleo no tubo de admissão	Baixa	Pressão
Bomba de resfriamento do gerador ou ventilador do motor	Falha	Temperatura
Temperatura de resfriamento do gerador	Alta	
Falha equipamento de aterramento	Falha Terra	
Temperatura da bobina estacionária	Alta	
Vazamento da água de resfriamento	Vazamento	
Falha interna fase-a-fase ou de aterramento	Falha	

Abaixo, encontram-se algumas citações de normas e diretrizes da IMO e das classificadoras Bureau Veritas (BV) e ABS sobre sistemas de alarmes:

- Um sistema de alarmes deve ser provido de forma a permitir prontamente a identificação de falhas nas máquinas e supervisão satisfatória dos equipamentos relacionados. O sistema pode ser arranjado em uma estação principal de controle ou, alternativamente, em estações de controle subsidiárias. No último caso, um monitor de alarmes deve ser instalado na estação de controle principal, exibindo nas estações subsidiárias a condição de falha (BV, 2005).
- A menos que justificado, o sistema de monitoramento e de controle devem ser separados (BV, 2005).
- O sistema de alarmes deve ativar um alarme sonoro e visual na ponte de comando em qualquer situação que requeira atenção de um oficial (BV, 2005).

- O sistema de alarmes deve ser do tipo “*self-monitoring*”, ou seja, este deve alarmar uma condição de falha do próprio sistema. Os alarmes devem ser visuais e sonoros, e devem piscar quando ocorrerem. Para os painéis luminosos, estes devem apresentar um meio de testar todas as luzes, de forma a ser possível identificar um indicador ou alarme com a luz queimada (ABS, 2008a).
- Os alarmes devem ser reconhecidos manualmente, mudando do estado “piscando”, para o estado “aceso permanente”. O estado aceso permanente deve permanecer ativo até que a condição de falha seja retificada (ABS, 2008a).
- O sistema de alarmes deve ser continuamente alimentado, possibilitando um chaveamento automático em caso de perda da alimentação normal (BV, 2005).
- O reconhecimento dos alarmes deve ser possível somente na estação de controle ativa (BV, 2005).
- As cores dos alarmes e indicadores devem seguir a norma ISO 2412, denominada “*Shipbuilding -- Colours of indicator lights*” (IMO, 1991).

Algumas sociedades classificadoras, como a Germanischer Lloyd e ABS, fazem distinção entre os requisitos para sistemas utilizados em três situações: (i) embarcações com praça de máquinas permanentemente desguarnecida, quando a presença da tripulação não é exigida continuamente; (ii) embarcações com praça de máquinas temporariamente desguarnecida, quando a presença da tripulação não é exigida por um período definido, por exemplo, de 8 horas; e (iii) embarcações com praça de máquinas permanentemente guarnecida, onde a presença da tripulação é exigida continuamente (MARINHA DO BRASIL, 2005).

No caso de sistemas de alarmes para embarcações com praça de máquinas temporariamente ou permanentemente desguarnecida, existem ainda requisitos a serem cumpridos em relação a sinalização e reconhecimento dos alarmes:

- O alarme do chefe de máquinas deve ser ativado quando um alarme de máquinas não for reconhecido em até 5 minutos na praça de máquinas, ou na sala de controle. (BV, 2005; IMO, 1991) (IMO, 1991)
- O alarme deve ter uma conexão com os compartimentos públicos dos engenheiros e cabines. (BV, 2005)

- O reconhecimento do alarme na ponte de comando não silencia o alarme sonoro na praça de máquinas. (BV, 2005)

Para os sistemas de alarmes baseados em computador, o “*software*” deve ser também verificado. A Germanischer Lloyd faz a certificação do “*software*” através de um questionário, que funciona como uma análise de risco qualitativa, avaliando a maneira com que o programa é desenvolvido e testado pelo fabricante, e as medidas de controle de qualidade, vulnerabilidade a falhas, e documentação (GL, 1996).

Em resumo, as exigências das sociedades classificadoras são mais focadas nas funções do sistema e na exibição dos alarmes, do que em requisitos físicos ou arquiteturas do sistema. Desta forma, os fabricantes possuem a flexibilidade de desenvolver seus sistemas a partir de qualquer plataforma como equipamentos próprios, CLPs industriais ou mesmo sistemas baseados em computador pessoal.

4.6. Modelos de comportamento relacionados aos alarmes

...there is yet no model which accurately reflects what process operators describe, namely the transition between the boredom of normal process operations and the panic of an anticipated major fault. (JENKINSON, 1997, p. 4)

Segundo Hollnagel e Wood (1983), um sistema cognitivo é um sistema que produz uma “ação inteligente”, e que seu comportamento é orientado a metas. Um sistema cognitivo é adaptável e capaz de ver os problemas sob vários pontos de vista. Também é capaz de operar utilizando conhecimento sobre si e sobre o ambiente. O homem é um sistema cognitivo. Um sistema homem-máquina também é. A Figura 39 mostra um exemplo de um sistema cognitivo, representando as interações entre o operador e demais componentes. Segundo Hollnagel (1998), a noção de sistema cognitivo implica modelar o processo (ou o sistema) e o operador em nível de igualdade, e os acoplamentos entre ambos são necessários para a análise das interações entre os dois modelos.

Figura 39 – Exemplo de um sistema cognitivo
– adaptado de (HOLLNAGEL, 1998, p. 72)

Para se projetar, ou simplesmente, entender e analisar um sistema homem-máquina focado no elemento humano, é necessário o conhecimento de alguns modelos cognitivos que possam servir como orientação. Os principais modelos de comportamento humano foram apresentados na subseção 3.1.3.1. Adicionalmente, a Figura 40 apresenta um modelo de controle humano de um navio, proposto por Kristiansen (2005).

Todos os modelos apresentados são uma aproximação ou uma tentativa de descrever o comportamento da mente humana. Nenhum modelo foi capaz de fazer essa descrição eficazmente, conforme a citação de Jenkinson (1997) do início desta seção.

Figura 40 – Controle Homem-Máquina de um navio
– adaptado de (KRISTIANSEN, 2005, p. 319)

Para aplicação no modelo de análise de risco dos sistemas de alarmes, o modelo SMOc (ver Figura 29, pág. 97) é um modelo bastante adequado, pois as quatro atividades nas quais o modelo é dividido, observação, interpretação, planejamento, e execução, podem ser claramente identificadas no processo de diagnóstico de um evento anormal através de um monitor do sistema de alarmes.

O modelo SRK de Rasmussen (ver Figura 20, pág. 63) também é adequado para descrever as tarefas de diagnóstico. Vários aspectos relativos aos processos cognitivos, baseados nos conceitos do modelo de Rasmussen, envolvendo sistemas supervisórios são apresentados no trabalho de Murphy e Mitchell (1986). As autoras enumeram 17 atributos cognitivos relativos a esses sistemas e respectivas implicações práticas no projeto da interface do sistema.

Como exemplo, em uma tarefa de monitoramento visual, os seguintes esquemas do nível de comportamento baseados em habilidades estão envolvidos: formação de uma imagem mental da tela do monitor, com expectativas dos dados que irão aparecer em campos específicos; e posteriormente, atenção e busca visual aos campos específicos, de acordo com a experiência, rotina e estratégia.

Um outro exemplo seria em um cenário de alarmes, onde três processos cognitivos estão envolvidos:

- Quando um alarme é recebido, acontece a ativação do esquema mental de “alerta” no reconhecimento do operador baseado em habilidades.
- Os procedimentos a serem executados a seguir, seguem uma resposta baseadas em regras.
- Não havendo uma solução, o modo baseado em conhecimento é então ativado, resultando de uma abordagem única para a resolução.

Por estes dois modelos sugeridos, é possível posicionar as tarefas envolvendo o sistema de alarmes na fase anterior a tomada de decisão e execução da ação. Logo, o projeto de um sistema de alarmes ou alterações de projeto após uma análise de risco podem ser feitas de forma a auxiliar os operadores em suas limitações cognitivas, reduzindo a chance de um erro humano, como por exemplo, aliviando o operador de processos mentais desnecessários.

4.7. Fatores e erros humanos relacionados ao sistema de alarmes

Conforme já exposto anteriormente, o sistema de alarmes não exerce funções de controle na embarcação, exceto os sistemas que possuem as funções de monitoramento e controle integradas. De qualquer maneira, em um navio, o operador é obrigado a interagir com os sistemas de automação, e esta interação é suscetível à ocorrência de erros humanos. Uma das mais frequentes causas de erro humano é o sobrecarga mental do operador provocada, entre outros fatores, pelo balanceamento inadequado entre a operação humana e a automação (FILGUEIRAS, 1996). O balanceamento entre a operação humana e a automação é definido como a atribuição criteriosa das funções do operador e da automação, de forma a garantir a segurança e eficiência da operação.

O balanceamento é realizado para otimizar as funções delegadas ao homem e à máquina. Segundo Filgueiras (1996), a presença do operador é justificada para a monitoração das funções da máquina, e sua capacidade de inovação frente a situações imprevistas. Já a automação é pertinente para funções que exijam rapidez na resposta e repetibilidade; funções que incorram em risco para o operador, tais como o teste e manutenção de equipamentos em locais contaminados; funções que demandem tempo longo para se completarem; funções cuja execução incorra em atividades monótonas, pois podem gerar insatisfação, distração e consequente erro humano; funções com muitos passos, requerendo alta concentração, como o caso de algumas tarefas de manutenção (nestes casos, o operador pode errar, omitindo algum passo); funções de supervisão que exijam a monitoração de muitas variáveis, pois o elemento humano tem a tendência de se fixar em apenas algumas variáveis que ele considera representativas do estado; e funções de teste repetitivo.

A existência do sistema de alarmes é justificada, pois este se encaixa em vários dos pontos acima. Desta forma, é correto afirmar que o sistema evita o erro humano nestas atividades não favoráveis ao homem, como nas funções repetitivas e rotineiras das embarcações, por exemplo, a verificação de níveis de tanques, de indicadores dos motores, e na agilidade em detectar um estado anormal.

O sistema de alarmes também contribui para evitar o erro humano:

- Ao aliviar da carga mental do operador, uma vez que permite que o operador foque sua atenção em outras atividades, como a navegação;

quando uma situação anormal ocorrer, sua atenção é chamada automaticamente;

- Na rapidez de detecção de uma situação anormal, aumentando a confiabilidade do diagnóstico e possibilidade de recuperação. Segundo a norma IEC-964 (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 1989), todas as funções, que tiverem que ser executadas dentro de um intervalo de tempo especificado após a detecção de um evento anormal, devem ser automatizadas.

Por outro lado, o erro humano também pode acontecer na interação com o sistema de alarmes. Kumamoto e Henley (1996) analisam estes erros sob o aspecto das limitações do ser humano em uma tarefa de diagnóstico. Algumas tendências básicas de erro seriam (REASON, 1988):

- Propensão para a similaridade: as pessoas tendem a escolher explicações de diagnósticos baseadas em comparações de situações parecidas;
- Propensão para a frequência: as pessoas tendem a escolher explicações de diagnósticos que ocorreram com êxito e com alta frequência no passado;
- Racionalidade limitada: a consciência do espaço é limitada. Por isso, as pessoas possuem apenas recursos mentais limitados para o diagnóstico;
- Racionalidade imperfeita: as pessoas raramente fazem diagnósticos pensando na aplicação das teorias de lógica, estatística, utilidade esperada, etc., mesmo quando estas são de seu conhecimento;
- Racionalidade relutante: as pessoas tendem a realizar um diagnóstico de forma a minimizar o esforço cognitivo ou o esforço de pensamento;
- Conhecimento incompleto ou incorreto: o conhecimento humano é só uma aproximação da realidade, há um número de modelos limitados do mundo externo.

Segundo a IMO, é claro que a automação cria novos caminhos para o erro humano, e pode até atrasar a detecção de um problema, eliminando as chances de

recuperação. Foi demonstrado que operadores realizam a monitoração menos eficaz quando um sistema de automação é instalado, e menos ainda quando este funciona adequadamente por um longo período. No entanto, de acordo com a IMO, observa-se que sistemas sofisticados operados por tripulantes bem capacitados levam a tomada de melhores decisões. Mas quando operados por operadores com baixo treinamento, criam um ambiente ainda mais perigoso. Como na indústria naval, a introdução da tecnologia é algo crescente, a chave do problema é garantir a qualificação dos operadores (IMO, 2003).

4.7.1. Projeto da interface

A interface de um sistema de alarmes não é somente o meio pelo qual o operador interage com o sistema, mas é uma ferramenta de tomada de decisão, que permite a compreensão do problema para o planejamento das ações. O projeto de interfaces homem-máquina é um problema comum que envolve fatores humanos, como visibilidade, percepção, semântica, entre outros, e deve ter como objetivo auxiliar a consciência situacional e a tomada de decisão. O projeto inadequado da interface do sistema de alarmes também pode ser um fator que contribui para o erro humano e acidentes em embarcações. Os principais problemas relacionados a interfaces são descritos a seguir (MURPHY; MITCHELL, 1986):

- Indução à falha de recuperação de memória e erro devido à exibição ambígua de informações (os monitores devem evitar a necessidade de fazer o operador se lembrar de uma informação ou instrução).
- Indução a não percepção de informações cruciais, e falha em reconhecer estados desconhecidos do sistema, devido a apresentação complexa das informações.
- Indução a falsa sensação de segurança, devido à avaliação incompleta do impacto de um evento.
- Aumento da carga mental devido ao aumento da demanda cognitiva
- Redução na capacidade de se detectar anormalidades e redução da consciência situacional, devido ao tédio associado aos períodos de monitoração.

Interessante notar que as normas de diretrizes para sistemas de alarmes da área naval já preveem recomendações para evitar estes problemas, conforme já visto na seção 4.5.

Alguns fatores humanos devem ser considerados no projeto da interface do sistema de alarmes (KOENE; VEDAM, 2000):

- Formas, cores e limites visuais e auditivos do operador, de forma a melhorar o reconhecimento de padrões, e não prejudicar a visão noturna;
- Informações hierarquizadas e técnicas de navegação no “*software*”, permitindo acesso rápido à dados importantes;
- Interface orientada às tarefas do operador tanto nas situações normais quanto anormais;
- Indicação integrada dos alarmes, eventualmente podendo visualizar resumos, e ordenação por prioridades, grupos ou nível de detalhes.

Não é objetivo deste trabalho entrar no mérito da elaboração de uma interface homem-máquina, que é um campo por si só vasto para pesquisas. Apenas serão citados alguns fatores humanos pertinentes às interfaces e principais bibliografias para consulta, as quais podem ser relevantes na aplicação do modelo de análise de risco a ser proposto.

Em IMO (1991), uma lista de símbolos é apresentada como padrão para sistemas de alarmes. A diretriz ABS (2003a) apresenta várias recomendações para monitores, painéis de alarmes, e alarmes em relação à ergonomia e fatores humanos.

Uma diretriz da ABS enumera diversas recomendações sobre o projeto de interfaces e monitores em pontes de comando. Um breve resumo dos pontos principais é listado abaixo (ABS, 2003b):

- Não ser ambígua – para poder orientar apropriadamente a resposta do operador;
- Apresentar sempre a informação de forma mais simples possível – evitando informações irrelevantes para a tarefa determinada;
- A interface deve ser personalizada para apresentar apenas as informações necessárias úteis para a realização de alguma ação;
- Os displays com múltiplas funções devem ser coloridos;

- Os indicadores analógicos devem apresentar as escalas e unidades dos valores;
- Quando utilizadas siglas e abreviações, estas devem ter seu significado claro e de uso comum.

O documento ainda cita especificamente princípios para o desempenho produtivo do operador e redução do erro humano:

- Os sistemas (dentre eles o sistema de alarmes) devem prover mecanismos de prevenção ao erro e tolerâncias, por exemplo, exigindo confirmações ou chamando atenção do operador para ações que possam comprometer diretamente a segurança da embarcação;
- Evitar conflitos de comandos entre equipamentos localizados em diferentes pontos da embarcação, como no caso dos monitores repetidores do sistema de alarmes;
- Compatibilizar a tripulação aos procedimentos operacionais, que significa, em outras palavras, utilizar pessoal qualificado para operar os sistemas a bordo.

Para fins de análise de risco, na abordagem desta tese, a interface do sistema de alarmes será analisada de forma simplificada. Basicamente, será classificada como adequada ou inadequada para operação. Os aspectos específicos citados estarão embutidos nesta classificação, e não serão tratados individualmente, para não tornar as análises demasiadamente complexas e volumosas.

4.7.2. Gerenciamento de alarmes

The alarm management effort is important because problems with alarm systems are often cited as contributing factors in industrial incidents. (DUNN; SANDS, 2005, p.1)

O gerenciamento de alarmes, do inglês, *alarm management*, é a aplicação do conceito de fatores humanos em conjunto com a engenharia de automação no

projeto de sistemas de alarmes com o objetivo de aumentar a usabilidade¹⁰ do sistema. Segundo Dunn e Sands (2005), o gerenciamento de alarmes também pode ser entendido como os processos e práticas para determinar, documentar, projetar, monitorar e manter mensagens de alarmes de processos de automação e sistemas de segurança.

O ataque aos problemas relacionados aos sistemas de alarmes partiu da própria indústria, quando, em 1990, criou-se uma força tarefa chamada de *Alarm Management Task Force* (AMTF), liderada pela empresa Honeywell. Este grupo levou a criação do consórcio ASM (*Abnormal Situation Management Consortium*) que produziu documentos sobre melhores práticas em gerenciamento de alarmes, e questões relacionadas aos operadores (KOENE; VEDAM, 2000). Este consórcio fez parte do desenvolvimento de uma importante publicação feita pelo *Engineering Equipment & Materials Users Association* (EEMUA), do Reino Unido, a respeito de gerenciamento de alarmes EEMUA (1999 apud KOENE; VEDAM, 2000).

Os principais problemas para os quais se buscaram um tratamento adequado foram (DUNN; SANDS, 2005; JENKINSON, 1997):

- Alarmes incômodos (*nuisance alarms*) ou alarmes espúrios, que são alarmes que disparam sem que nenhuma condição anormal tenha ocorrido ou quando nenhuma ação do operador é requerida. Estes alarmes dessensibilizam o operador, reduzindo o tempo de resposta a alarmes reais, ou causam uma baixa credibilidade nos alarmes de problemas reais. Um exemplo típico de ocorrência de alarmes incômodos é quando o sistema monitorado se encontra em manutenção, e o sistema de alarmes acusa algum sensor desconectado ou falha do sistema monitorado.
- Alarmes ativos que permanecem nos monitores quando nenhuma ação é requerida, ou mesmo após a intervenção do operador. Estes alarmes mascaram outros alarmes para o operador, e também causam baixa credibilidade no sistema.

¹⁰ Usabilidade é definida como a adequação das interfaces homem-máquina ao seu usuário, ou como facilidade de uso. Formalmente, segundo a ISO, usabilidade é a medida pela qual um produto pode ser usado por usuários específicos para alcançar objetivos específicos com efetividade, eficiência e satisfação em um contexto de uso específico (ISO 9241-11).

- Avalanches de alarmes e taxas excessivas de alarmes durante falhas, que sobrecarregam o operador, dificultando o diagnóstico da causa do evento. “A sobrecarga de informação é um perigo real” (IMO, 2003).
- Falta de clareza nas ações a serem tomadas para os alarmes, o que causa um atraso na tomada de decisão do operador. Todo alarme deve possuir uma resposta do operador bem definida.
- Falha no diagnóstico do problema, devido à interpretação incorreta dos alarmes.

Segundo Koene e Vedam (2000), o entendimento do consórcio ASM é que os alarmes devem ter as seguintes características: (i) serem relevantes ao contexto; (ii) serem únicos e não ambíguos; (iii) prover tempo de resposta adequado; (iv) apresentar a prioridade ao operador; (v) serem compreensíveis, através de uma mensagem clara e de fácil reconhecimento. Para alcançar estes objetivos, aperfeiçoar os projetos de sistema de alarmes e evitar os problemas citados acima, algumas técnicas foram propostas e um modelo de ciclo de vida de gerenciamento de alarmes foi desenvolvido. As principais técnicas criadas foram:

- Redução de incômodos (*nuisance reduction*) que consiste em medir as taxas de alarmes, e focar na resolução os problemas crônicos;
- Guia de projeto: envolve a documentação e criação de uma filosofia de como projetar alarmes, envolvendo recomendações sobre o que alarmar, padrões de sinalização e sobre a interação do operador com o sistema;
- Racionalização de alarmes: consiste na revisão criteriosa dos alarmes;
- Supressão de alarmes: que consiste em identificar alarmes que podem ser suprimidos sob determinadas circunstâncias.

O diagrama do ciclo de vida do gerenciamento de alarmes é útil na identificação de requisitos e como sistemática de projeto do sistema. A Figura 41, resume todas as etapas contempladas neste modelo.

Figura 41 – Ciclo de vida do gerenciamento de alarmes
– adaptado de (DUNN: SANDS, 2005, p. 4)

Os passos do modelo do ciclo de vida do gerenciamento de alarmes são (DUNN e SANDS, 2005):

- 1) Filosofia: trata-se de adotar uma filosofia para o sistema e definir seus princípios de operação;
- 2) Identificação: identificar os possíveis alarmes;
- 3) Racionalização: ajustar os alarmes individuais aos princípios e requisitos definidos pela filosofia, e documentar as informações do alarme, como ação do operador, tempo de resposta, consequências de não reagir ao alarme, etc;
- 4) Projeto: consiste na configuração dos alarmes e desenho da interface;
- 5) Implantação e treinamento: consiste em colocar o sistema em operação e realizar treinamento para os operadores;

- 6) Operação: é o estágio em que o alarme está em serviço, e sinalizando as situações anormais ao operador;
- 7) Monitoramento do desempenho: compreende a análise dos dados dos alarmes durante a operação;
- 8) Manutenção: correção dos componentes que necessitam reparo;
- 9) Avaliação: auditoria periódica do sistema e dos processos organizacionais pertinentes;
- 10) Gerenciamento das alterações: é o processo de aprovação e autorização para fazer modificações no sistema.

5. METODOLOGIA DE ANÁLISE DE RISCO PARA EMBARCAÇÕES COM SISTEMAS DE ALARMES

Este capítulo irá apresentar os passos da elaboração de uma metodologia de análise de risco para embarcações com sistemas de alarmes, focando os fatores humanos e organizacionais presentes no contexto.

Entende-se por metodologia como a explanação completa e detalhada dos métodos, etapas e instrumentos do trabalho de pesquisa. A metodologia inclui (i) a apresentação da parte teórica, conceitos e ideias; (ii) a comparação de diferentes enfoques; e (iii) a crítica e escolha de um método individual.

O desenvolvimento da metodologia a ser apresentada neste trabalho utilizará os conceitos expostos anteriormente na revisão bibliográfica, e será estruturado passo a passo, começando pelo modelo de acidentes escolhido como o mais adequado para representar o problema. Também será apresentada a formulação matemática do modelo, e os métodos sugeridos para a análise probabilística de risco.

5.1. Premissas para a elaboração da metodologia

A formulação de uma metodologia de análise de risco eficiente deve possuir três premissas fundamentais. A primeira delas é deixar claro o que se deseja analisar, e quais os riscos que se deseja avaliar. Conforme exposto no Capítulo 2, existe um cardápio farto de métodos, técnicas, cada qual com seu foco e seu objetivo. A segunda premissa é a escolha de um modelo adequado para representar o problema, no caso deste trabalho, o modelo do acidente. O modelo do problema será a representação simplificada da realidade, com suas hipóteses e limitações. Trata-se de um ponto fundamental, pois a estrutura do modelo, sua profundidade de análise e grau de detalhamento são escolhas relacionadas aos custos da análise, tempo necessário, pesquisa, levantamento de dados, entre outros. Um modelo eficiente é aquele que pode ser gerenciável, cujos dados estão disponíveis e são

confiáveis, e que consegue identificar as principais opções de redução de risco. Como última premissa, a análise de risco não pode ser um fim em si mesmo. Sua função primordial é ser útil para os decisores, e, portanto, deve fornecer as informações adequadas a estes, sem excessos e sem escassez.

Ainda, segundo Hollnagel (1998), um modelo para fins de análise de risco envolvendo ações humanas, deve necessariamente incluir a descrição do contexto, do qual todas as ações fazem parte. Esse contexto deve ser descrito como uma combinação das influências do homem, tecnologia e organização, conforme apresentado na Figura 31.

Para a análise de risco de acidentes envolvendo fatores organizacionais, Ward et al. (2007) sugerem dois possíveis caminhos: o primeiro envolve a análise dos modos de falhas do sistema, e o segundo, a análise da sequência do acidente. A escolha por um ou por outro caminho dependerá da estrutura das informações disponíveis. Na análise pelos modos de falha, faz-se uma análise indutiva e busca-se calcular a probabilidade do acidente através do caminho crítico (mínimos *cut-sets*). A análise por árvore de falhas (do inglês *Fault Tree Analysis*, ou FTA) é uma ferramenta útil para se obter o caminho crítico. Já na análise pela sequência do acidente, faz-se uma análise dedutiva e lança-se mão de ferramentas como árvore de eventos (do inglês *Event Tree Analysis*, ou ETA) ou diagrama da sequência de eventos (do inglês *Event Sequence Diagram*, ou ESD) e de probabilidades condicionais para a formulação das equações de probabilidades. Ward et al. (2007) fazem a escolha pelo segundo caminho nas análises apresentadas em seu trabalho sobre um acidente marítimo e sobre um acidente de um ônibus espacial, argumentando que o segundo caminho é mais viável, pois é mais conveniente pensar sistematicamente com um conjunto de cenários de falha mutuamente exaustivos e exclusivos.

5.2. Proposta de um modelo de acidentes com sistema de alarmes

Dos modelos de acidentes apresentados no Capítulo 2, para os propósitos deste trabalho, considera-se que o modelo da Figura 19 (pág. 53), de Mosleh e Dias (2004), seja o que mais bem abrange as fase de um acidente em um navio. Isso

porque o modelo explicita os papéis do evento iniciador, condições perigosas e das barreiras, os quais são fases que podem ser claramente identificáveis na sequência de um acidente com uma embarcação. Além disso, o modelo também é disposto de forma sequencial, forma pela qual se desejará analisar o problema, conforme proposição de Ward et al. (2007) discutida no parágrafo anterior. No entanto este modelo não deixa explícito o papel do sistema de alarmes.

Para contemplar as funções do sistema de alarmes, propõe-se o modelo da Figura 42, o qual expande o modelo de Mosleh e Dias, posicionando o sistema de alarmes na sequência do acidente. Primeiramente, deve-se compreender que o sistema de alarmes, assim como os demais equipamentos de segurança, atua como uma barreira que busca impedir que o evento iniciador se propague. Nesse modelo, as barreiras estão posicionadas antes e depois do incidente. Isso porque, dado um evento iniciador e uma condição de perigo, deve-se tentar evitar que a combinação de ambos provoque um incidente. E, dado o incidente, deve-se também evitar que este cause perdas.

Utiliza-se como premissa que um evento iniciador cause uma situação anormal detectável pelo sistema de alarmes. Ou seja, assume-se que uma função importante da embarcação é necessariamente monitorada pelo sistema, conforme a exigência das normas das sociedades certificadoras. Os sensores e máquinas não monitoradas não são relevantes para a avaliação do risco da embarcação. O evento iniciador fará com que um ou mais sensores atinjam seus valores limites, fazendo com que o sistema de alarmes anuncie o problema. A análise dos eventos iniciadores tem o objetivo de prever e avaliar situações que possivelmente podem “dar errado” (ocasionar um problema). No contexto da análise probabilística de risco, os eventos iniciadores são geralmente falhas de equipamentos.

No entanto, nota-se, pelo diagrama da Figura 42, que o sistema de alarmes está posicionado na área tracejada da barreira. Isso porque se deseja representar a ideia de que o sistema de alarmes e monitoramento não é uma barreira por si só, já que não exerce controle nenhum nas máquinas ou atuadores. A barreira será a combinação entre o sistema de alarmes e a tripulação, ou melhor, a barreira será efetivamente a atuação da tripulação reagindo ao alarme, e tomando ações que recuperem a situação anormal no sistema. Para o evento iniciador se propagar, este deve ultrapassar todas as barreiras pelos buracos do queijo suíço, conforme o modelo de Reason da Figura 25.

Figura 42 – Modelo de acidente para embarcação com sistema de alarmes

Se por algum motivo, a tripulação não conseguir recuperar o estado normal, e todas as barreiras forem ultrapassadas, o incidente ocorre. Dado o incidente, o sistema (no caso, a embarcação) pode ainda possuir mecanismos para evitar ou mitigar as perdas. Neste caso, outras barreiras estão posicionadas entre o incidente e as perdas. O sistema de alarmes pode também participar das ações de mitigação das perdas.

O que pode ocorrer é que, após o incidente, outros sensores monitorados podem ser afetados. Neste caso, os novos alarmes indicarão as consequências imediatas do incidente nas máquinas e sistemas monitorados da embarcação. Novamente, dependerá da tripulação e demais barreiras agir na recuperação do problema.

É importante frisar que as barreiras não são apenas barreiras físicas, mas também procedimentos, treinamento, manuais, normas, etc. A primeira barreira está relacionada à prevenção de incidentes. A segunda barreira está relacionada com o plano da contingência, ou seja, com a gestão do incidente, que pode estar ligada apenas ao caso da perda da função do sistema, ou também à ocorrência de danos.

Também há de se deixar claro que o evento iniciador ou condição perigosa podem ser gerados por um erro humano. Desta forma, entende-se que o ser humano não está apenas ligado à prevenção de incidentes ou mitigação das perdas, mas também diretamente às causas do acidente.

O modelo de acidentes aqui proposto na Figura 42 representa, de forma clara, os eventos e fases em uma embarcação com sistema de alarmes até a propagação do evento iniciador ao acidente. O papel do sistema de alarmes se torna bem definido no modelo, o que reforça sua importância na segurança da embarcação. Entende-se, portanto, que este seja o modelo que mais bem representa a realidade de um acidente marítimo, dado o cenário de interesse, o que poderá ficar evidenciado no estudo de caso que será apresentado adiante.

Como última observação, a Figura 42 pode ser interpretada como o modelo de acidente com consequências apenas para o navio. Ou seja, as perdas consideradas são as perdas para o próprio navio. Em um contexto amplo de análise de risco, como já discutido anteriormente, podem existir danos e perdas não apenas para o navio, mas também para o ambiente externo ao sistema navio. Ou seja, as consequências do acidente podem ser ainda mais abrangentes. Essas perdas e danos podem ocorrer na imagem da empresa, perdas de contratos, impacto

ambiental, impacto na opinião pública, entre outros. A Figura 43 mostra a continuação ou expansão do modelo de acidente, incluindo as consequências para o armador, por exemplo. Barreiras de mitigação de consequências também podem ser previstas, como seguros, multas em contratos, e planos de contingência.

Figura 43 – Expansão do modelo de acidentes

5.3. O modelo cognitivo para as ações humanas

O objetivo de se escolher um modelo de cognição humana é definir como se entende que a “máquina humana” funciona para fins da análise. Essa definição pode ser uma “faca de dois gumes”, limitando o método a apenas uma maneira de enxergar o problema de avaliar as probabilidades de erro humano. Além disso, definir um único caminho significa descartar os possíveis avanços científicos que podem surgir no futuro, como por exemplo, novos modelos de cognição humana.

No entanto, definir o modelo é fundamental para um entendimento comum de como as análises devem ser conduzidas em relação às ações dos operadores. Não há pretensão aqui de inovar ou propor um novo modelo de cognição humana, mas utilizar os que já foram propostos e desenvolvidos, e adaptá-los para a aplicação deste trabalho.

Os modelos de comportamento humano foram apresentados nas subseções 3.1.3.1 e 3.3.4.1. Na subseção 3.1.3.1 foi apresentado o modelo de Rasmussen

(*Skill-Rule-Knowledge*), e na subseção 3.3.4.1 apresentou-se o modelo SMOc. Destes dois modelos extraiu-se o modelo que será utilizado aqui. O modelo de Rasmussen é um dos mais citados na literatura pesquisada, principalmente pela proposta de dividir o desempenho humano em três níveis: de conhecimento, regras e habilidades. No entanto, conforme ilustrado na Figura 20, nem todas as etapas deste modelo são explícitas e bem definidas no processo de um operador utilizando um sistema de alarmes. Simplificando algumas etapas, o modelo obtido é semelhante ao modelo SMOc (ver Figura 29), um modelo mais simples e pioneiro, que serviu de base para os modelos que vieram em seguida. Portanto, optou-se por considerar neste trabalho as etapas do modelo SMOc, observação-interpretação-planejamento-ação, considerando os três níveis de desempenho de Rasmussen por analogia.¹¹

A Figura 44 ilustra a proposta deste trabalho para representar as etapas das atividades humanas na interação com o sistema de alarmes, após a ocorrência de um evento, ou de um alarme. Esta figura também foi elaborada com base nos conceitos representados nas Figuras 23 e 24.

Figura 44 – Modelo das ações de recuperação da tripulação

Além de servir como modelo para as ações humanas da tripulação para a metodologia de análise de risco proposta, pretende-se com a representação da

¹¹ Na subseção 3.3.4.1, também é citado o modelo COCOM, o qual é uma evolução do modelo SMOc, mas é um modelo mais direcionado para a aplicação do método CREAM. Por ser mais simples e genérico, o método SMOc foi preferido.

Figura 44 detalhar e explicar o bloco “Ações de recuperação da tripulação” da Figura 42. Logo, a Figura 44 propõe explicar, através de um modelo sequencial, como a tripulação pode interagir com o sistema de alarmes, e reagir para recuperar o sistema. Os blocos A, B, C e D correspondem às ações da tripulação, que quando desempenhadas de forma correta, permitirão que o sistema seja recuperado ao estado normal após um evento iniciador.

O primeiro bloco da Figura 44 corresponde à ocorrência de um evento, ou melhor, à ocorrência de um alarme, seja este real ou falso. Desta forma, limita-se o estudo das atividades do operador apenas à situação onde ocorre um evento iniciador que dispara um alarme. Não serão discutidas ações de consulta ou alterações de configuração do sistema de alarmes, ou qualquer outra interação do usuário com a interface do sistema, fora do contexto acima especificado.

O bloco que segue, bloco A, é o bloco da “Observação das informações” do monitor do sistema de alarmes. Este bloco é equivalente à fase de percepção do modelo de Rasmussen da Figura 20. Este bloco corresponde ao nível de habilidades e o erro do operador é de não responder ou não reagir ao alarme. Isso pode ocorrer pelo operador não ouvir ou visualizar o alarme, ou por uma violação, ou seja, intencionalmente o operador não responde ao alarme.

O bloco B é o bloco que corresponde à “Interpretação” do tripulante sobre os alarmes exibidos no sistema de alarmes. Esta interpretação envolve não somente avaliar os alarmes ativos, mas também os alarmes inativos. Em uma situação de anormalidade, os alarmes inativos também transmitem informação do que ainda está operacional, e servem de base para a tomada de decisão. Portanto, considera-se que o operador interpreta o estado do sistema de alarmes, ou seja, o conjunto dos alarmes ativos e inativos. Este bloco é equivalente aos blocos de reconhecimento e avaliação do modelo de Rasmussen. Desta forma, agrupa-se estas duas etapas em uma apenas, já que a diferença entre reconhecer e avaliar não é bem definida para esse problema. Portanto, o bloco B está nos níveis de regras e conhecimento, os quais, segundo a Tabela 5, podem produzir o erro de engano.

O bloco C corresponde a decidir e planejar a ação. Uma vez interpretado o alarme, com as informações do sistema e informações externas, o operador irá tomar a decisão do que fazer. Este bloco corresponde aos blocos de Decisão e Planejamento do modelo de Rasmussen. Ambos no nível do conhecimento. Neste nível, este bloco também pode produzir um erro de engano.

Por fim, o bloco D corresponde à execução da ação de recuperação da situação anormal que causou o alarme. A execução da ação, de acordo com o modelo de Rasmussen, corresponde ao nível de habilidade. Os erros neste nível, de acordo com a Tabela 5, são erros de memória e execução, correspondendo aos deslizes e lapsos. A Tabela 20 é uma síntese desta explanação, e faz associação entre os blocos do modelo cognitivo proposto (Figura 44) e os conceitos do modelo de Rasmussen:

Tabela 20 – Atividades humanas relacionadas ao sistema de alarmes

Atividade	Tipo de erro primário	Nível de Desempenho
A - Observação	Não responde	Nível de habilidade
B - Interpretação	Engano	Nível de regras e conhecimento
C - Decisão	Engano	Nível de conhecimento
D - Execução	Deslize ou Lapso	Nível de habilidade

No caso de um erro humano, sempre há possibilidade de recuperação da ação do operador (linha pontilhada da Figura 44). A eficácia da recuperação dependerá, entre outros fatores, do tempo decorrido, uma vez que o sistema já pode ter atingido seu tempo de deterioração.

Ainda, pela Figura 44, em todas as atividades, conforme os modelos de erro humano apresentados no Capítulo 3, o operador é influenciado pelo contexto. Os fatores organizacionais estão inseridos neste contexto. Conforme já exposto, vários autores propuseram diferentes meios de abordar a influência do contexto, como por exemplo, os fatores de condicionamento de desempenho (PSF) e os CPCs de Hollnagel (1998). Em análises mais direcionadas, podem-se isolar alguns fatores organizacionais de interesse, e executar a análise probabilística e análise de sensibilidade com apenas estes fatores, obtendo-se resultados para comparação da influência (sensibilidade) da cada fator.

Conforme exposto na subseção 3.1.4.2 (pág. 70), onde foram apresentados alguns exemplos de fatores organizacionais presentes no setor naval, pode-se propor a seguinte divisão dos fatores organizacionais segundo sua influência:

- Nas ações e decisões da tripulação;
- No sistema físico (políticas de manutenção, especificações de equipamentos, alteração da planta durante a fase operacional);

- Na mitigação das perdas e consequências do acidente (regras para situações de emergência, impacto no público, na imagem da empresa).

Neste trabalho, para fins da aplicação no modelo proposto, serão considerados apenas os fatores organizacionais que influenciam o comportamento da tripulação durante o acidente, ou seja, os fatores que influenciam na interpretação dos sinais de alarmes, e nas decisões e ações da tripulação.

Partindo da ideia de Murphy e Paté-Cornell (1996), que consideram os fatores organizacionais como um botão de ajuste, é possível fazer uma nova analogia sobre o conjunto os fatores organizacionais presentes no contexto. Esse conjunto de fatores organizacionais do contexto funcionaria como uma mesa de mixagem de áudio, conforme ilustrado na Figura 45. Os fatores organizacionais seriam os botões de ajuste de ganho de cada canal de áudio.

Figura 45 – Analogia dos fatores organizacionais a uma mesa de mixagem

A ideia aqui proposta com essa analogia, representada na Figura 45, é que a influência dos fatores organizacionais no contexto será o conjunto ou a combinação de cada fator segundo seu ganho individual. Assim, a “melodia” final (contexto) é o que irá exercer influência na tripulação. Considera-se, portanto, que cada botão de ajuste afeta o estado do indivíduo (treinamento, estresse, carga de trabalho, etc.) e a sua situação no contexto, como reação frente a incentivos, ameaças, cultura organizacional, etc.

A grande dificuldade dos gestores é ajustar o nível do “volume” de cada fator organizacional, de forma que a “melodia” seja a que influencie os operadores positivamente na direção da eficiência e segurança.

5.4. Modelagem do sistema de alarmes

Foi citado na seção anterior que o operador, após o evento iniciador, irá consultar os monitores do sistema de alarmes para tomar a decisão sobre as ações de recuperação do problema. O sistema de alarmes apresentará os alarmes ativos e inativos. Entretanto, no caso da apresentação errada de um alarme, ou de um estado do sistema que não condiz totalmente com uma situação anormal, o operador pode ser induzido ao erro. Ou, caso o sistema não detecte o evento iniciador, o operador pode não responder. Para tratar estes casos, Kumamoto e Henley (1996) definem os conceitos de falha-segura e falha-perigosa.

- Falha-segura (*failed-safe*): é quando o sistema gera um alarme espúrio de um sensor, em uma condição de operação normal.
- Falha-perigosa (*failed-dangerous*): é quando o sistema não gera um alarme de sensor, em uma condição anormal.
- Falha de falha-perigosa (*failed-dangerous failed*): é quando o sistema não gera um alarme de falha de sistema, quando em condição anormal.

Para expressar estas condições de falha do sistema de alarmes, será utilizada a seguinte terminologia:

- a. Alarme ativo: quando o sistema de alarmes captura corretamente um evento iniciador.
- b. Alarme falso ativo: quando o sistema exibe um alarme enquanto o sistema físico encontra-se em uma condição normal (situação de falha-segura).
- c. Alarme inativo: o sistema não exibe o alarme de determinado ponto monitorado enquanto o sistema físico encontra-se em uma condição normal.

- d. Alarme falso inativo: o sistema não exibe o alarme de determinado ponto monitorado enquanto o sistema físico encontra-se em uma condição anormal (situação de falha-perigosa).

As condições a. e c. são condições de operação normal do sistema. As condições b. e d. são condições nas quais o sistema de alarmes falha em exibir corretamente a informação do alarmes. Apesar dos casos de falso-alarme (falso ativo) serem relativamente frequentes e, portanto, relevantes para o contexto de análise de acidentes, o modelo de acidentes proposto na Figura 42 parte do princípio que sempre há um evento iniciador. Neste caso, as condições de um alarme falso-ativo e inativo não são de interesse para a análise.

Em relação aos alarmes ativos, sabendo-se a probabilidade de ocorrência de um evento iniciador, e a confiabilidade do sistema de alarmes, ou seja, a probabilidade do sistema de alarmes capturar o alarme do evento iniciador, dado um evento iniciador, pode-se calcular a probabilidade de um alarme ativo da seguinte maneira:

$$P(\text{alarme ativo}) = P(\text{alarme ativo}|\text{evento iniciador}) \cdot P(\text{evento iniciador}) \quad (17)$$

Analogamente, a probabilidade de ocorrer um alarme falso inativo pode ser calculada como segue:

$$P(\text{alarme falso inativo}) = P(\text{alarme falso inativo}|\text{ev. iniciador}) \cdot P(\text{ev. iniciador}) \quad (18)$$

Kumamoto e Henley (1996) apresentam alguns aspectos teóricos sobre a confiabilidade do sistema de alarmes, ou, “sistema de sensores”, como eles originalmente generalizam. A confiabilidade do sistema é alterada, por exemplo, considerando a redundância de sensores, e diferentes arranjos em série e paralelo dos sensores de um ponto monitorado. Trata-se de um tema extremamente pertinente para o analista de risco e para o projetista do sistema de alarmes. Todavia, não será abordado neste trabalho, uma vez que é um assunto mais ligado ao projeto de arranjo dos sensores e instrumentação.

O sistema de alarmes também está relacionado ao tempo de correção do problema e recuperação do sistema. Uma vez ocorrido um evento iniciador, pode-se distinguir alguns instantes de tempo importantes na recuperação do sistema. A Figura 46 ilustra estes conceitos.

Figura 46 – Linha do tempo da deterioração do sistema

Nesta figura:

- t_0 é o instante do evento iniciador – instante em que ocorre o evento iniciador, ou instante exato da ocorrência do problema no sistema físico.
- t_1 é o atraso de sinalização do alarme – trata-se do tempo decorrido entre o evento iniciador, e a sinalização do alarme pelo sistema de alarmes. Este atraso está relacionado com o tempo de resposta do sensor, com os valores limites configurados para o alarme, e com os atrasos de ativação do alarme.
- t_2 é o atraso de observação – trata-se do tempo decorrido entre o evento iniciador e a observação do alarme pela tripulação. O intervalo de tempo entre t_1 e t_2 é o tempo decorrido entre a sinalização do alarme e a observação deste pela tripulação. Este tempo será tão

menor quanto mais eficaz for a sinalização do alarme na embarcação, dependendo do número de monitores (por exemplo, em cabines e refeitórios).

- t_3 é o atraso de interpretação – trata-se do tempo decorrido entre o evento iniciador e a interpretação do estado do sistema de alarmes. Este tempo é diretamente dependente do perfil do operador, sua experiência e treinamento.
- t_4 é o atraso de decisão – trata-se do tempo decorrido entre o evento iniciador e a decisão sobre as medidas de recuperação do sistema. O tempo de decisão será determinado pela estrutura hierárquica da tripulação e da organização em terra, treinamentos e procedimentos de emergência, informações técnicas disponíveis, entre outros.
- t_5 é o atraso de recuperação do sistema – trata-se do tempo decorrido entre o evento iniciador e a solução do problema, ou seja, a recuperação total do sistema. A recuperação do sistema envolverá ações da tripulação. O tempo t_5 será função da eficiência da tripulação, e dos equipamentos e máquinas instaladas.

Para cada sistema, haverá um tempo máximo para a recuperação. Este tempo máximo é aquele para o qual o sistema atinge um grau de deterioração que não permite mais seu reparo. Se t_5 for menor que o tempo máximo de recuperação (limiar de perigo do sistema), o sistema pode ser recuperado. Se o atraso de recuperação do sistema for maior que o tempo máximo de recuperação (na Figura 46, indicado por t_5^*), o acidente ocorrerá.

5.5. A estrutura do modelo de acidente para a análise de risco

Com base no modelo de acidentes (Figura 42) e no modelo de comportamento da tripulação interagindo com o sistema de alarmes (Figura 44), vai-

se estruturar uma metodologia para aplicar os modelos desenvolvidos na análise de risco para uma embarcação com sistema de alarmes. O objetivo será obter um modelo simplificado da sequência do acidente, incluindo as fases relevantes onde existe participação da tripulação e dos fatores organizacionais.

A Figura 47 apresenta uma proposta de estrutura do modelo de análise de risco. Iniciando-se por um evento anormal no sistema físico (evento iniciador), o sistema de alarmes exibirá o estado do conjunto de pontos monitorados, e seus alarmes. Com base nestas informações, a tripulação interpreta e toma decisões sobre como agir frente ao estado do sistema. Estas ações podem, por sua vez, ter várias consequências, como evitar o acidente, mitigar suas consequências, permitir a propagação do problema até uma disfunção, impedindo que a embarcação cumpra sua missão, ou até um acidente.

Figura 47 – Estrutura do modelo para a análise de risco

É importante notar que a Figura 47 particulariza o modelo de acidente da Figura 42, representando apenas a barreira referente ao conjunto “sistema de alarmes + tripulação”, parando a sequência no bloco “incidente”. Na parte referente às ações de recuperação da tripulação, o modelo da Figura 47 inclui os conceitos do modelo da Figura 44, simplificando algumas etapas, como será discutido adiante.

Os dois primeiros blocos da Figura 47 correspondem à parte do sistema físico. Os dois blocos seguintes correspondem à parte dependente da tripulação. Como hipótese, considera-se que, dado um alarme, o operador sempre irá observar o estado do sistema de alarmes. Conforme já mencionado no Capítulo 3, o erro do operador, na fase de observação, pode ser ou uma violação, ou uma falta de resposta do operador para o alarme. Como citado, as violações não serão abordadas neste trabalho. O fato do operador não responder está associado a uma

falha de projeto no anúncio do alarme, como falta de um repetidor ou de uma sirene ou sinaleiro luminoso externo. Esta condição não será tratada aqui. Desta forma, a fase de observação do alarme é omitida, e assume-se que a tripulação sempre tomará conhecimento do estado do sistema de alarmes. Assim, tem-se como premissas que sempre haverá repetidores suficientes espalhados na embarcação, e que as formas de anúncio do alarme serão adequadas.

Após a fase de interpretação do estado do sistema de alarmes, correspondente ao nível de habilidades e conhecimento, conforme a Figura 44, tem-se a fase de decisão e execução das ações de recuperação do sistema. Estas duas fases foram agrupadas no modelo simplificado da Figura 47, e utiliza-se como hipótese que, uma vez tomada a decisão da ação, a respectiva execução ocorrerá com sucesso. Tomada a decisão correta de recuperação, o sistema é recuperado. Tomada a decisão incorreta, o incidente ocorre. Essa simplificação foi adotada uma vez que a execução da tarefa não envolve a participação do sistema de alarmes.

Na estrutura do modelo da Figura 47, considera-se a influência dos fatores organizacionais pertinentes ao desempenho da tripulação. Como já discutido, os fatores organizacionais também influenciam o sistema físico. Porém, a fim de se limitar a análise, consideram-se apenas os fatores organizacionais exercerão influência nas falhas ou acertos da tripulação, ou seja, nas fases de interpretação do problema e nas fases de decisão e execução de uma ação corretiva. Desta maneira, o modelo tem como objetivo propiciar aos gestores e armadores diretrizes focadas para investimentos em sistemas de segurança, e para elaboração de políticas que influenciam o comportamento humano, e, portanto, a segurança a bordo.

A modelagem da influência dos fatores organizacionais é baseada no modelo SAM (*System-Action-Management*) de Murphy e Paté-Cornell (1996), o qual também se utiliza das probabilidades condicionais na análise probabilística do risco.

5.6. Formulação matemática

A formulação matemática para a análise probabilística de risco será desenvolvida a partir das equações das probabilidades condicionais, que permitem aplicar as probabilidades *a posteriori* em uma sequência de eventos.

Primeiramente, de acordo com a sequência do modelo de acidente da Figura 47, são definidas as variáveis, conforme que aparecem na Figura 48:

- $E \rightarrow$ evento iniciador
- $A \rightarrow$ estado do sistema de alarmes
- $I \rightarrow$ interpretação dos alarmes
- $D \rightarrow$ decisão e ação da tripulação
- $O \rightarrow$ fatores organizacionais
- $Rec \rightarrow$ sistema recuperado

Figura 48 – Variáveis da estrutura do modelo

Segundo o Teorema da Probabilidade Total, para eventos mutuamente exclusivos e exaustivos, tem-se que a probabilidade de um evento A ocorrer, sabendo-se que o evento B_i já ocorreu é dada por:

$$P(A) = \sum_i P(A|B_i) \cdot P(B_i) \quad (19)$$

Aplicando-se este teorema para a sequência do acidente da Figura 48, utilizando como hipótese que estes eventos são mutuamente exclusivos e exaustivos (também uma simplificação do problema), pode-se calcular a probabilidade da recuperação do sistema, dada uma decisão da tripulação e respectiva execução da ação de recuperação:

$$P(Rec) = \sum_n P(D_n) \cdot P(Rec|D_n) \quad (20)$$

onde D_n é um conjunto exaustivo e mutuamente exclusivo das decisões e ações. Da mesma maneira, tem-se que:

$$P(D_n) = \sum_k P(I_k) \cdot P(D_n|I_k) \quad (21)$$

onde I_k é um conjunto exaustivo e mutuamente exclusivo das possíveis interpretações da tripulação do estado do sistema de alarmes que levam a uma decisão de ação. E por fim:

$$P(I_k) = \sum_j P(A_j) \cdot P(I_k|A_j) \quad (22)$$

onde A_j é um conjunto exaustivo e mutuamente exclusivo dos possíveis estados do sistema de alarmes. A combinação das equações (21) e (22), dado um evento iniciador E , resulta em:

$$P(D_n|E) = \sum_j \sum_k P(A_j|E) \cdot P(I_k|A_j) \cdot P(D_n|I_k) \quad (23)$$

Esta equação tem interesse de analisar especificamente apenas o evento iniciador E , e não um conjunto de eventos iniciadores. Portanto, considera-se que $P(E) = 1$.¹²

Agora, pode-se calcular a expressão da eq. (20):

$$P(Rec|E) = \sum_n \sum_j \sum_k P(A_j|E) \cdot P(I_k|A_j) \cdot P(D_n|I_k) \cdot P(Rec|D_n) \quad (24)$$

Representando-se os fatores organizacionais por O_m , conforme descrito no modelo SAM (ver seção 3.5), a influência deles na probabilidade do acidente, segundo a estrutura da Figura 48, será sobre os termos que contemplam as atividades desempenhadas pela tripulação. Assim, dados o evento iniciador e o conjunto de fatores organizacionais, a probabilidade de recuperação do sistema fica:

¹² Em NASA (2002), sugere-se o modelo de Poisson para a estimativa das probabilidades do evento iniciador: $Pr(k) = e^{-\lambda t} \frac{(\lambda t)^k}{k!}$, onde λ é a frequência de ocorrência, e k é o número de eventos no tempo t .

$$P(Rec|E, O_m) = \sum_n \sum_j \sum_k P(A_j|E) \cdot P(I_k|A_j, O_m) \cdot P(D_n|I_k, O_m) \cdot P(Rec|D_n) \quad (25)$$

A eq. (25) é a equação geral do modelo de acidente da Figura 47. A análise detalhada de cada termo será feita na seção seguinte.

Vale observar que o termo $P(D_n|I_k, O_m)$ leva em conta a decisão de apenas um decisor, seja ele o usuário do sistema de alarmes, um tripulante, ou um grupo de tripulantes.

Por fim, a Figura 49 apresenta uma síntese dos modelos de acidentes e de comportamento humano propostos anteriormente, dos quais se obteve o modelo simplificado de acidente e sua equação geral para aplicação nas análises de risco para embarcações com sistema de alarmes.

5.7. Métodos aplicáveis para o cálculo das probabilidades

O objetivo desta seção é apresentar ao analista um “kit” de ferramentas para o cálculo dos termos da eq. (25). Para tal, os métodos apresentados na introdução teórica deste trabalho, Capítulos 2 e 3, serão aqui referenciados e discutidos acerca de sua aplicação.

▪ Cálculo do termo $P(A_j|E)$

Este termo expressa a probabilidade de um estado correto A_j do sistema de alarmes, dado o evento iniciador E . Lembrando que este estado A_j significa o conjunto de alarmes ativos e inativos que são exibidos nos monitores do sistema de alarmes. Este termo deve ser calculado através das técnicas de análise de risco e confiabilidade de sistemas, conforme os métodos apresentados na Figura 7. As técnicas “What-if”, FMEA, e FTA seriam as mais indicadas.

A confiabilidade do sistema pode ser comparada aos limites impostos pelas sociedades classificadoras. Análises custo-benefício (seção 2.6) podem ser feitas com o objetivo de se definir o número de sensores ou número de sistemas monitorados, de acordo com o investimento e grau de monitoramento pretendido.

Figura 49 – Modelo de acidente completo para aplicação na análise de risco

Geralmente, os estaleiros são guiados pelas normas e diretrizes prescritivas das sociedades classificadoras para definir os sistemas a serem monitorados. O analista pode reduzir o risco de um acidente, ou aumentar a chance de recuperação de um sistema, indo além das especificações, modificando o valor numérico do termo $P(A_j|E)$.

▪ **Cálculo do termo $P(I_k|A_j, O_m)$**

Este termo expressa a probabilidade do operador realizar a interpretação I_k , dados o estado do sistema de alarmes A_j , e o estado da organização, ou fatores organizacionais presentes, O_m . Este termo pode ser calculado utilizando-se as técnicas de análise de confiabilidade humana que tratam da atividade de diagnóstico (nível baseado em regras e conhecimento). As seguintes técnicas são sugeridas:

- Matriz de confusão (subseção 3.3.3.1)
- Confiabilidade Cognitiva Humana (subseção 3.3.3.5)
- CREAM (subseção 3.3.4.1)

Na ausência de dados, este termo também pode ser estimado através de técnicas de consulta a especialistas (subseção 3.3.3.2), como o método SLIM (subseção 3.3.3.3). Os fatores organizacionais devem ser levados em conta neste termo, e para tanto, deve-se dar preferência a técnicas que permitam a avaliação da influência destes.

▪ **Cálculo do termo $P(D_n|I_k, O_m)$**

Este termo expressa a probabilidade de uma decisão seguida de sua respectiva execução D_n , dados a interpretação I_k do operador e o estado da organização, ou fatores organizacionais presentes, O_m . O problema da estimativa deste termo se encontra tanto no nível de conhecimento (tomada de decisão) quanto no nível de habilidade (execução da ação). As seguintes técnicas são sugeridas para a estimativa do cálculo:

- Matriz de confusão (subseção 3.3.3.1)
- Confiabilidade Cognitiva Humana (subseção 3.3.3.5)

- THERP (subseção 3.3.3.6)
- CREAM (subseção 3.3.4.1)

Novamente, na falta de dados, as probabilidades podem ser estimadas via consulta a especialistas.

Os fatores organizacionais devem ser especialmente avaliados nesta etapa através da opção por técnicas que permitam esta avaliação. Isto porque, como já citado, treinamentos e políticas de incentivos influem diretamente na qualidade das decisões e execução das ações. A análise de sensibilidade (seção 3.4) é indicada para mensurar os efeitos destes fatores na probabilidade do termo $P(D_n|I_k, O_m)$.

▪ Cálculo do termo $P(Rec|D_n)$

Por último, o termo $P(Rec|D_n)$ expressa a probabilidade de recuperação do sistema, dada determinada ação de recuperação D_n . Este termo está ligado à resposta do sistema físico a esta ação de correção, e naturalmente, ao tempo máximo de recuperação do sistema.

Este termo pode ser estimado principalmente através de métodos de consulta a especialistas. Os especialistas devem ser capazes de mensurar os efeitos de uma ação corretiva de um sistema deteriorado, na sua recuperação ou mitigação de um incidente.

Também, podem ser estimados através métodos de análise de risco de sistemas, como diagrama causa-consequência, árvore de consequências, entre outros.

Em novos desenvolvimentos ou em uma nova construção de uma embarcação, a probabilidade deste termo pode ser modificada através da especificação dos equipamentos a bordo com foco em segurança. Por exemplo, aplicando métodos de análise de risco para a tomada de decisão da escolha dos sistemas a serem instalados.

A Figura 50 apresenta um resumo do que foi tratado nesta seção, com os métodos sugeridos de cálculo das probabilidades abaixo de cada fase do modelo de acidente.

Figura 50 – Resumo dos métodos sugeridos para cálculo dos termos

5.8. Aplicação da metodologia

Nas seções anteriores, uma proposta de metodologia de análise de risco envolvendo sistemas de alarmes foi apresentada. Sabe-se, no entanto, que esta metodologia deve estar inserida em um contexto mais amplo de um processo de avaliação formal de risco. Logo, pode-se considerar que a metodologia aqui proposta se insere em um ou mais passos de um processo completo, como o processo apresentado na estrutura da Figura 5 (pág. 23), criada por IMO (2002a), ou na estrutura da Figura 9 (pág. 35), criada por NASA (2002).

Estas estruturas de análise de risco também são tratadas como metodologia. Assim, a metodologia aqui proposta é uma metodologia dentro de outra metodologia de análise de risco mais abrangente.

Com base nestas duas estruturas de análise de risco citadas no Capítulo 2, “*Formal Safety Analysis*” de IMO (2002a) e “*PRA Procedures Guide*” de NASA (2002), entende-se que os seguintes passos são necessários para a aplicação da metodologia aqui proposta de análise de risco de embarcações com sistemas de alarmes:

1. Definição do problema e dos objetivos
2. Familiarização com o sistema e levantamento de dados
3. Identificação do evento iniciador
4. Estruturação dos cenários
5. Identificação dos fatores humanos e organizacionais
6. Modelagem lógica e formulação matemática

7. Análise quantitativa
8. Análise das incertezas e sensibilidade
9. Interpretação dos resultados
10. Opções de controle do risco
11. Avaliação custo-benefício
12. Recomendações para a tomada de decisão e conclusões

A metodologia desenvolvida neste trabalho se insere nos passos 6 e 7, de modelagem do problema e estimativa das probabilidades. Todavia, este trabalho buscou abordar por completo esta sequência de passos, de forma a direcionar o leitor para os aspectos de cada etapa relevantes e úteis em uma abordagem considerando os fatores humanos e organizacionais e o sistema de alarmes.

Esta sequência de passos não deve ser considerada como fixa, mandatória ou suficiente em todos os casos. Mas trata-se de uma referência ao analista que deseja aplicar a metodologia aqui desenvolvida. Na literatura, encontram-se diversas outras estruturas análogas, e cabe ao analista julgar a importância de cada passo, acrescentando ou eliminando etapas, aprofundando-se em cada análise, de acordo com seus recursos e objetivos.

Para finalizar, uma vez que um acidente envolvendo uma embarcação consiste em uma sequência de eventos, recomenda-se, no passo 6 (modelagem lógica), buscar dividir esta sequência de eventos em fases, de forma a transformar análise extensa e complexa em problemas menores e mais simples. A estratégia de dividir uma extensa sequência de eventos em fases é deveras adequada para análises de sistemas complexos. Todavia, a divisão das fases pode não ser uma tarefa óbvia, e o sucesso da análise de risco será fortemente dependente do critério do analista na escolha e organização da divisão das fases.

Este procedimento de divisão de fases proporciona também identificar com mais clareza as ações humanas de interpretação e decisão, facilitando a aplicação dos métodos quantitativos de estimativa da confiabilidade humana no passo 7. Após a análise de cada fase, é possível recompor a sequência completa de eventos do acidente, pois a formulação matemática do modelo de análise é estruturada por equações de probabilidades condicionais. Assim, a consequência de um incidente de uma fase, pode ser considerada como o evento que inicia a fase seguinte. Esta estratégia será mais bem demonstrada no estudo de caso do capítulo a seguir.

6. ESTUDO DE CASO

The sole objective of the investigation of an accident under the Merchant Shipping (Accident Reporting and Investigation) Regulations 2005 shall be the prevention of future accidents through the ascertainment of its causes and circumstances. It shall not be the purpose of an investigation to determine liability nor, except so far as is necessary to achieve its objective, to apportion blame. (UKMS, 2005, p. 2)

Neste capítulo apresenta-se um estudo de caso, ilustrando a aplicação do modelo proposto no Capítulo 5 a um acidente ocorrido com uma embarcação, no qual o sistema de alarme foi um elemento importante na dinâmica dos eventos.

Os objetivos da apresentação do estudo de caso são (1) ilustrar alguns passos e hipóteses a serem seguidos pelo analista em uma possível aplicação; (2) demonstrar que o modelo proposto contempla, em sua formulação, os eventos relevantes que ocorrem em uma embarcação, tendo em conta o cenário e os objetos de estudo.

A aplicação a um caso real não significará a validação definitiva do modelo aqui desenvolvido. Conforme os argumentos apresentados anteriormente sobre métodos semelhantes, há os que defendem que os modelos de comportamento humano não possuem uma validação científica. Todavia, é de suma importância apresentar um exemplo de aplicação para documentar como o modelo pode ser aplicado.

Para este estudo de caso, escolheu-se analisar o acidente da embarcação Maersk Doha, ocorrido em 2 de outubro de 2006. O acidente se deu nas proximidades de Norfolk, Virgínia, nos Estados Unidos, e foi originado por um problema na caldeira auxiliar, e culminou em um incêndio na praça de máquinas, que durou 12 horas. Na

Figura 51, apresenta-se uma fotografia da embarcação e um resumo de suas características principais.

As informações para a análise e estudo de caso foram obtidas no relatório de investigação do acidente, produzido pelo Marine Accident Investigation Branch (MAIB), e publicado em seu site na internet (MAIB, 2007).

A seguir, na seção 6.1, um resumo das principais informações do relatório de investigação do acidente é apresentado, e são tratados com maior profundidade os aspectos relevantes para a posterior aplicação da metodologia, como as informações referentes à tripulação (elemento humano) e referentes ao sistema de

alarmes. Na seção 6.2, inicia-se a análise do problema, seguindo os passos necessários para permitir a demonstração modelagem da interação “tripulação-sistema de alarmes”, para a estimativa do risco do acidente.

EMBARCAÇÃO: MAERSK DOHA
BANDEIRA: REINO UNIDO
TIPO: CONTAINER CARRIER, 4507 NOMINAL TEU
SOCIEDADE CLASSIFICADORA : LLOYD'S REGISTER
CONSTRUÇÃO : AÇO
FABRICAÇÃO: 1996, DAEWOO SHIPBUILDING AND
MARINE ENGINEERING, CORÉIA DO SUL
COMPRIMENTO : 280.52M
ARQUEAÇÃO BRUTA : 51931 TON
MOTORIZAÇÃO: MAN B&W 8K90MCC / 35500kW

Figura 51 – Embarcação Maersk Doha
- adaptado de (MAIB, 2007)

6.1. Resumo do relatório de investigação do acidente

Para o desenvolvimento do estudo de caso e da análise de risco, apresenta-se nesta seção uma síntese das principais informações do relatório de investigação do acidente. Este tipo de relatório contém informações suficientemente detalhadas e bem organizadas, que permitem a utilização de seu conteúdo para diversos fins, como, por exemplo, elaboração de novas normas e políticas de segurança, aperfeiçoamento do projeto de embarcações e equipamentos, e mesmo análises de risco com o objetivo de se entender o desdobramento do acidente. Relatórios de investigação de acidentes são geralmente organizados em uma parte informativa, com a descrição dos fatos, uma seção de análise, e, por fim, conclusões e recomendações. Os relatórios de investigação de acidentes buscam sempre colaborar com o aumento da segurança, evitando fazer julgamentos ou apontar culpados.

6.1.1. Síntese da narrativa do acidente

A narrativa apresentada no relatório de investigação do acidente inicia-se com a seguinte declaração: “As informações desta seção são baseadas em entrevistas com testemunhas, registros de bordo, e relatórios da empresa que opera o navio” (MAIB, 2007, p. 4, tradução nossa).

No dia 1º de outubro de 2006, a embarcação Maersk Doha atracou no Portsmouth Marine Terminal, em Norfolk, desligando seus motores às 06:30hs. As operações de carga e descarga se iniciaram às 8:00hs, descarregando cerca de 600 contêineres, e carregando outros 360. Sua partida para Miami estava agendada para as 0:00hs do dia seguinte. Às 23hs o aviso para a partida é dado. O terceiro oficial de máquinas cumpria turno na praça de máquinas, sob supervisão do chefe de máquinas. O terceiro oficial de máquinas havia se juntado à tripulação recentemente.

O motor é preparado de acordo com “*pre-sail checklist*” e o comando é passado ao passadiço às 23:54hs. O primeiro movimento do motor principal acontece às 0:04hs. Ao sair do porto, estavam na praça de máquinas o segundo e terceiro oficial de máquinas e o chefe de máquinas. O primeiro oficial de máquinas estava em descanso em sua cabine.

Às 0:30hs, o sistema de alarmes dispara o alarme de “Pressão Baixa de Vapor” na caldeira auxiliar. O alarme não é considerado incomum, e normalmente seria resultado de uma falha na ignição da caldeira auxiliar. No entanto, não havia outros alarmes indicando tal situação. O primeiro oficial é chamado à praça de máquinas. Os três oficiais se dirigem, então, ao compartimento da caldeira, e verificam que a chama está acesa, porém existe vapor escapando pela entrada de ar da fornalha. A primeira decisão tomada é cortar o combustível da caldeira.

A fim de garantir que o economizador não sobreaquecesse, a bomba reserva de abastecimento de água que abastece a caldeira é ligada. O objetivo era aumentar o fluxo de água do tanque para a caldeira para compensar a água perdida através do vapor que escapava pela tubulação rompida. A caldeira auxiliar e o economizador pertenciam a um mesmo circuito de água, e o economizador dependia da caldeira para receber a água para não operar em vazio, e impedir seu sobreaquecimento. Embora também existissem duas bombas para circular água para o economizador, a bomba reserva estava quebrada, devido a um problema mecânico.

Às 01:20hs, outro alarme de “Pressão Baixa de Vapor” na caldeira auxiliar é disparado, mas não se consegue distinguir se tratava-se do alarme original ou novo

alarme. Neste momento, o chefe de máquinas decide telefonar ao passadiço para avisar o problema. O comandante pergunta se é necessário ancorar, ou se é possível continuar até o navio deixar a área portuária. O chefe de máquinas comunica que é possível continuar, porém a uma velocidade reduzida, sem dar maiores informações sobre o ocorrido. O comandante interpreta o problema como sendo de pequena severidade.

Enquanto os oficiais discutiam possibilidades de conserto da caldeira, a partir de 01:36hs, o comandante, em consenso com o chefe de máquinas, começa a aumentar gradualmente a rotação do motor, até atingir o máximo em 01:43hs. Durante este período, a temperatura dos gases de escape aumenta rapidamente, e os alarmes de alta temperatura no economizador são disparados. O terceiro oficial percebe um aumento de 350°C para 600°C em menos de 5 minutos. Seiscentos graus Celsius era o fundo de escala do indicador de temperatura.

Neste momento, a rotação do motor é reduzida novamente, e ao investigar a causa da alta temperatura, o chefe de máquinas detecta fogo no economizador. O terceiro oficial e outro tripulante começam a combater o fogo com mangueiras e extintores de incêndio, porém logo desistem devido ao forte calor e fumaça. Às 02:30hs o incêndio é reportado ao passadiço. O comandante dispara o alarme de emergência da embarcação, e anuncia no sistema de áudio sobre o incêndio na casa de máquinas.

O segundo oficial, ocupado com o acionamento dos geradores, ainda estava na praça de máquinas, e ignorou o alarme de emergência, pensando ser um alarme falso. Somente após ouvir o anúncio do comandante, o segundo oficial resolve deixar o compartimento do gerador. Ao chegar à praça de máquinas com muita fumaça, este percebe que era a última pessoa que lá permanecia, e, rapidamente, deixa a zona de perigo, encontrando o chefe de máquinas e outro tripulante na sala de controle tentando abrir uma porta de escape. O chefe de máquinas ordena ao segundo oficial para desligar a bomba de água que abastece o economizador, mas esse ignora o comando pensando ser uma ação incorreta a ser feita.

Às 02:34hs o combate ao incêndio inicia. O comandante e chefe de máquinas acordam um plano de combate ao incêndio e às 02:39hs o motor principal é desligado. Devido ao desconhecimento do funcionamento do economizador, várias tentativas são feitas no intuito de apagar o fogo. Porém, nem o acionamento do sistema de CO₂, o qual disparou apenas alguns cilindros, nem o resfriamento das

paredes do economizador surtem efeito. Somente após a chegada da Guarda Costeira Americana, por volta de 06:00hs, com uma equipe de combate à incêndio, que o fogo foi combatido corretamente através do direcionamento da água nos tubos dentro do economizador. O incêndio foi declarado extinto às 12:30hs.

6.1.2. Causas do acidente

Segundo o relatório de análise do acidente, o rompimento da tubulação de vapor na fornalha da caldeira auxiliar se deu devido ao seu sobreaquecimento por operar com baixo nível de água. A causa mais provável da operação da caldeira auxiliar com baixo nível de água foi apontada como sendo uma falha no seu sistema automático de controle.

A perda da água de alimentação na caldeira auxiliar levou queda de vazão na circulação de água no economizador, fazendo sua temperatura aumentar. Períodos com rotação baixa do motor, na entrada e na saída do porto de Norfolk causaram acúmulo de fuligem no interior do economizador, ocasionando a ignição do fogo. O acúmulo de fuligem no economizador foi também explicado pela sua falta de limpeza, uma vez que o sistema automático de limpeza por ar comprimido não era utilizado em modo automático.

A demora para informar o problema e a sua condição real ao passadiço, a decisão de manter o motor ligado evitando tomar uma decisão impopular de atrasar a saída do porto, o desconhecimento do funcionamento e construção do economizador, e consequente combate de incêndio de forma incorreta, foram os fatores que, em conjunto, fizeram com que o problema inicial (ruptura da tubulação de vapor da caldeira auxiliar) desencadeasse uma sequência de eventos que culminaram no acidente (incêndio na praça de máquinas).

Não havia nenhum impedimento para ancorar a embarcação, e buscar solucionar o problema. No entanto, a decisão de atrasar a operação era impopular, o que influenciou o chefe de máquinas a assumir o risco de manter o motor ligado. Esta atitude levou o investigador do acidente a concluir que este demonstrava pouco apreço para com o estado das máquinas.

6.1.3. Tripulação

O comandante da embarcação era russo, e trabalhava para o armador por quase 10 anos. Atuava como comandante há seis anos, e seu inglês era considerado com um padrão bom.

O chefe de máquinas era da Coreia do Sul, e trabalhava embarcado desde 1978, sendo chefe de máquinas por mais de 12 anos. O comandante e outros oficiais encontravam certa dificuldade em entender seu inglês falado, o que foi constatado durante entrevistas com a empresa que investigou o acidente e a Guarda Costeira Americana. Na avaliação de língua inglesa, o chefe de máquinas alcançou uma nota 3, numa escala de 1 a 5 (sendo 1 o nível mais avançado). Segundo o critério de seleção do armador, o cargo de chefe de máquinas exigia uma nota 2.

O primeiro e segundo oficiais de máquinas eram romeno e ucraniano, respectivamente, e ambos navegavam em seus primeiros contratos com o armador. O primeiro oficial iniciou a trabalhar na embarcação a menos de 5 meses antes do acidente, e o segundo oficial a menos de 4 meses. O terceiro oficial de máquinas também era romeno, e era novo no navio, apesar de ter trabalhado para o armador por 2 anos. A experiência dos três oficiais de máquinas era considerada limitada em comparação com a experiência do chefe de máquinas.

O relatório de investigação do acidente apontou que, como os três oficiais eram do leste europeu e possuíam um idioma comum, a comunicação foi um fator que isolava o chefe de máquinas durante as circunstâncias normais, se agravando durante a situação de emergência.

6.1.4. Sistema de alarmes

A embarcação possuía um sistema de alarmes e monitoramento cobrindo as principais máquinas, permitindo a operação com praça de máquinas desguarnecida. Os pontos de medição eram monitorados pelo sistema, permitindo a visualização destes em monitores na sala de controle do motor. Ao atingir um valor limite, um alarme sonoro é ativado, e os detalhes de cada alarme são exibidos nas telas e impressos em papel para o registro permanente. Os alarmes relevantes referentes aos sistemas da caldeira auxiliar e economizador são apresentados na Tabela 21.

– adaptado de MAIB (2007)

Sistema	Alarme
Caldeira auxiliar	Nível alto Nível baixo Anormal Bomba de Serviço em operação Pressão de vapor (0-16 bar) Temperatura de saída de vapor (0-186°C)
Condensador	Nível alto de óleo
Tanque coletor do condensador	Nível baixo
Água da Caldeira	Bomba de circulação (no. 1 e 2) em operação Falha na bomba de circulação (no. 1 e 2)
Água de abastecimento	Bomba em operação Falha na bomba
Alimentação elétrica ininterrupta	Falha
Gases de escape	Temperatura de admissão (0-600°C) Temperatura de exaustão (0-600°C) Aviso de alta temperatura 350°C
Sistema de limpeza de fuligem do economizador por ultrassom	Anormal
Soprador de fuligem do economizador	Anormal

Vale chamar atenção ao fato de que os sistemas da caldeira auxiliar e do soprador do economizador eram do tipo “*self-monitoring*”, ou seja, devem alarmar quando estão em falha ou em operação anormal. Logicamente, com um problema mais grave, como falta de alimentação, este alarme de operação anormal pode não ser anunciado. Por esse motivo, se monitoram outras causas do problema, como a “falha na alimentação elétrica ininterrupta”.

O relatório de investigação menciona que quando a Guarda Costeira Americana iniciou a investigação em 3 de outubro, a impressora foi encontrada com o papel obstruído, causando a impressão ilegível dos alarmes. O último registro legível datava de 23 de setembro. Os alarmes também poderiam ser recuperados da memória RAM (*Random Access Memory*) do aparelho, mas devido às quedas de energia ocorridas durante o acidente, seus registros foram perdidos.

6.2. Modelagem e análise do acidente

Para a demonstração da aplicação da metodologia de análise de risco proposta neste trabalho, decidiu-se percorrer as etapas principais de um processo de avaliação de risco, iniciando com a definição dos objetivos da análise, até as recomendações para a tomada de decisão. Para tal, utilizar-se-á como referência a sequência de passos apresentados na seção 5.8 (pág. 154). O modelo de acidente envolvendo o sistema de alarmes, proposto no Capítulo 5, será principalmente abordado na subseção de modelagem do problema e formulação matemática.

6.2.1. Definição do problema e dos objetivos

O problema em questão consiste em analisar o acidente com uma embarcação porta-contêiner de 280m e 4500 TEU, ocorrido em 2006, nos Estados Unidos. A embarcação se encontrava em manobra de saída do porto, quando um incêndio ocorreu, causando avarias graves na praça de máquinas.

O objetivo de se realizar esta análise de risco, neste estudo de caso, é aplicar a metodologia apresentada nesta tese para auxiliar no processo de tomada de decisão sobre possíveis medidas para aperfeiçoar a segurança das embarcações semelhantes à que será analisada. Especificamente, as medidas pretendidas para aumentar a segurança estão relacionadas com os fatores humanos e organizacionais, relativos à interação tripulação-sistema de alarmes.

6.2.2. Familiarização com o sistema e levantamento de dados

A síntese da narrativa do acidente, apresentada na seção 6.1.1, consiste em uma pequena porção do relatório de investigação, o qual provê informações suficientes e detalhadas para os objetivos pretendidos deste estudo de caso. A função desta etapa é organizar e processar as informações contidas no relatório de investigação para a utilização na análise de risco.

A Tabela 22 organiza cronologicamente os eventos citados no relatório de investigação, que serão pertinentes para a aplicação da metodologia de análise de risco a seguir.

Em relação ao funcionamento do sistema de geração de vapor, a Figura 52 apresenta um diagrama esquemático do sistema “economizador + caldeira auxiliar” da embarcação Maersk Doha. O economizador depende da caldeira auxiliar para receber água, a qual é aquecida em seu interior pelos gases de escape do motor.

O sistema foi projetado para que o economizador, através do aproveitamento do calor gerado pelos gases de escape do motor, auxiliasse a caldeira na geração de vapor e no aquecimento do óleo pesado. A caldeira auxiliar era automaticamente ligada quando o motor estivesse em baixa potência, e o economizador não conseguisse gerar calor suficiente.

Uma vez que a tubulação de vapor da caldeira estava rompida, a vazão de água no economizador diminuiu. O que permitiu que este sobreaquecesse, causando a ignição da fuligem acumulada em seu interior.

Figura 52 – Diagrama esquemático do sistema de geração de vapor
– adaptado de MAIB (2007)

Tabela 22 – Cronologia dos eventos importantes para a análise

Hora	Evento
0:04 a 0:30	<ul style="list-style-type: none"> Falha no sistema automático de controle da caldeira auxiliar. Caldeira auxiliar opera com baixo nível de água.
0:30	<ul style="list-style-type: none"> Alarme de baixa pressão de vapor da caldeira auxiliar.
1:20	<ul style="list-style-type: none"> Segundo alarme de baixa pressão de vapor da caldeira auxiliar. Chefe de máquinas notifica comandante sobre problema na caldeira. Chefe de máquinas avisa que é possível continuar navegação, à baixa velocidade. O comandante interpreta o problema como sendo de pequena severidade.
1:36	<ul style="list-style-type: none"> Para a manobra de saída do porto, a rotação do motor começa a aumentar gradualmente, até atingir o máximo.
0:30 a 1:43	<ul style="list-style-type: none"> Diminuição da circulação de água no economizador. Aumento de temperatura no economizador. Acúmulo de fuligem no economizador devido à baixa rotação do motor.
1:43	<ul style="list-style-type: none"> Aviso de alta temperatura 350°C no economizador
1:48	<ul style="list-style-type: none"> Temperatura do economizador aumenta rapidamente. Alarme de alta temperatura no economizador (fundo de escala 600°C). O comandante toma a decisão de manter o motor principal ligado, mas reduz a rotação novamente.
2:19	<ul style="list-style-type: none"> Fuligem acumulada no economizador inicia o incêndio. O chefe de máquinas detecta fogo dentro do economizador.
2:30	<ul style="list-style-type: none"> O incêndio é reportado ao passadiço. Alarme de emergência da embarcação é ativado. Segundo oficial de máquinas descarta alarme de emergência como falso alarme e continua os reparos na praça de máquinas. Chefe de máquinas ordena segundo oficial a desligar a bomba de água, mas é ignorado.
2:34	<ul style="list-style-type: none"> O combate ao incêndio se inicia de forma inadequada.
2:39	<ul style="list-style-type: none"> O motor principal é desligado.
2:52	<ul style="list-style-type: none"> O sistema de CO₂ é disparado e a embarcação é ancorada.
6:00	<ul style="list-style-type: none"> Chegada da Guarda Costeira Americana, e incêndio é combatido corretamente.
12:30	<ul style="list-style-type: none"> Incêndio é declarado extinto.

6.2.3. Identificação do evento iniciador

De acordo com o relatório de investigação do acidente, o evento iniciador do acidente foi um problema no sistema automático da caldeira auxiliar, que permitiu que esta operasse, por quase 30 minutos, com baixo nível de água, causando ruptura da tubulação de vapor, próximo à fornalha.

Trata-se de um evento iniciador ocorrido no sistema técnico, provavelmente devido a uma falha na parte elétrica ou eletrônica, ou em algum atuador do sistema de controle da caldeira auxiliar. Pode-se concluir que não houve nenhum erro humano, naquela ocasião, associado a essa falha no sistema de controle da caldeira. Além disso, por atuar de forma automática, a caldeira auxiliar também não exigia a atuação permanente de um operador. No entanto, o relatório de investigação atribui essa falha técnica a uma provável rotina ineficiente de operação e manutenção.

6.2.4. Estruturação dos cenários

Em decorrência do evento iniciador, outros eventos se seguiram (ver Tabela 22), ocasionando o incêndio na praça de máquinas. Para facilitar a aplicação do modelo do acidente, decidiu-se dividir o problema em cinco fases, conforme apresentado na Tabela 23, que indica, para cada fase, o respectivo evento iniciador, suas causas (físicas ou devido a erros humanos), e sua consequência. Trata-se de um passo fundamental no processo de análise, pois a divisão das fases dependerá muito da familiarização com o problema, e determinará a estrutura para a aplicação do modelo proposto no Capítulo 5.

A fase 1 inicia-se com o evento iniciador, e suas causas foram comentadas na subseção anterior. A consequência dessa falha no sistema automático da caldeira auxiliar foi a ruptura da tubulação de vapor e diminuição na circulação de água no economizador. A caldeira auxiliar tinha a função de gerar vapor para aquecer o óleo pesado para o motor principal e para uso doméstico na embarcação. Uma vez que a caldeira apresentava-se em falha, poder-se-ia utilizar outras fontes para aquecer o óleo pesado, ou operar o motor principal a diesel. Na fase 1, o sistema de alarmes não sinalizou a operação anormal ou falha na caldeira. Isto deve ter ocorrido ou por algum problema no sistema de alarmes, o que poderia ter sido evitado com inspeções e testes periódicos, ou porque o sistema automático da caldeira auxiliar, em falha, não atuou para enviar a informação de falha ao sistema de alarmes.

Tabela 23 – Fases do acidente

Fase	Evento iniciador	Causa do evento iniciador		Consequência do evento iniciador
		Física	Erro Humano	
1.	Falha no sistema automático da caldeira auxiliar	-	Rotinas de operação e manutenção ineficiente	Ruptura da tubulação de vapor da caldeira e diminuição da circulação de água no economizador
2.	Ruptura da tubulação de vapor da caldeira auxiliar	Operação da caldeira com baixo nível de água	Demora e imprecisão em informar problema ao passadiço e decisão de continuar navegação	Aumento da temperatura do economizador
3.	Aumento de temperatura no economizador	Diminuição da circulação de água no economizador	Desconhecimento do funcionamento do economizador Operação em modo manual do sistema de limpeza do economizador Decisão de manter motor em baixa rotação	Ignição da fuligem e incêndio no economizador
4.	Incêndio no economizador	Combinação de alta temperatura com fuligem acumulada	Desconhecimento do funcionamento do economizador Decisão de continuar navegação	Propagação do incêndio na praça de máquinas
5.	Propagação do incêndio na praça de máquinas	Falha no sistema de ativação dos cilindros de CO ₂	Falha na inspeção do sistema de CO ₂ Desconhecimento das técnicas de combate ao incêndio no economizador	Perdas de equipamentos Interrupção na missão do navio.

A fase 2 inicia-se com o evento da ruptura da tubulação de vapor da caldeira auxiliar. A consequência deste problema foi o aumento da temperatura no

economizador, a qual pode ser explicada tanto por motivos técnicos quanto por erros humanos. O motivo físico do aumento de temperatura no economizador foi que o vapor que escapava pela caldeira causou a diminuição da circulação água no economizador, permitindo que esse atingisse uma temperatura elevada. Todavia, podem-se considerar como erro humano a imprecisão e demora do relato do problema na caldeira à ponte de comando, e a decisão do chefe de máquinas de assumir o risco de danificar alguma máquina e sugerir continuar a navegação, buscando deixar a zona portuária. Durante esta fase, após a ruptura da tubulação interna da caldeira auxiliar, o sistema de alarmes sinalizou o alarme de pressão baixa de vapor. Na fase 2, o estado do sistema de alarmes, portanto, era indicar apenas uma condição anormal no sistema de geração de vapor, o qual era um alarme comum que ocorria quando a caldeira falhava em iniciar sua ignição.

A fase 3 tem como evento inicial o aumento de temperatura no economizador, resultando no incêndio dentro do economizador, causado pela combinação de alta temperatura com a fuligem acumulada. Devido ao desconhecimento do equipamento pela tripulação, o soprador de fuligem do economizador era apenas operado em modo manual, o que causou a ignição da fuligem acumulada. Nesta fase, o sistema de alarmes anunciou um sobreaquecimento do economizador quando a temperatura atingiu 350°C.

A fase 4 inicia-se com o evento “incêndio no economizador”. O erro humano, associado a esta fase, também ocorreu devido ao desconhecimento do funcionamento do economizador, pois se organizou uma equipe de combate ao incêndio, a qual fez tentativas incorretas de combater o fogo com mangueiras, jorrando água na parede externa do economizador. A demora em combater o fogo corretamente causou a propagação do incêndio para a praça de máquinas. Nesta fase, o estado do sistema de alarmes indicava alta temperatura no economizador. O indicador de temperatura exibia 600°C, que era seu fundo de escala.

Finalmente, a fase 5 tem seu início no evento “propagação do incêndio na praça de máquinas”. A causa dessa propagação é a combinação entre a falha no sistema fixo de gases CO₂ de combate a incêndio e as ações ineficazes da tripulação por desconhecimento de como combater o fogo no economizador. Quando o sistema de CO₂ foi acionado, apenas 4 dos 224 cilindros da praça de máquinas liberaram gases. Ao mesmo tempo, a equipe formada de combate ao incêndio desconhecia que a maneira correta de combater o incêndio no

economizador seria jorrar água em seu interior, e não em suas paredes. A consequência da propagação do fogo foi a avaria de outros equipamentos e interrupção da missão da embarcação. Durante a fase 5, outros alarmes devem ter sido sinalizados pelo sistema de alarmes, porém o relatório de investigação não faz menção a nenhum, com exceção dos alarmes de emergência da embarcação, que não indicam falhas de máquinas, mas são disparados manualmente para que a tripulação realize os procedimentos de emergência e se reúna em algum ponto de encontro.

Fazendo um resumo dos parágrafos anteriores, a Tabela 24 apresenta os estados do sistema de alarmes de acordo com cada fase do acidente.

A partir da Tabela 23, é possível identificar os eventos pertinentes para a elaboração de um diagrama de sequência de eventos, e correspondente árvore de eventos. A Figura 53 apresenta um diagrama de sequência de eventos, partindo do evento iniciador do acidente. Associado a cada fase correspondente da Tabela 23, está indicado o correspondente alarme sinalizado na embarcação.

Figura 53 – Diagrama da sequência de eventos do acidente

Tabela 24 – Estados do sistema de alarmes

Fase	Estado do sistema alarme
1. Evento iniciador: falha no sistema automático da caldeira auxiliar	<ul style="list-style-type: none"> ▪ Informação dos alarmes inativos: <ul style="list-style-type: none"> - não havia alarmes de nível baixo de água. - não havia alarme de falha no sistema de controle da caldeira.
2. Ruptura da tubulação de vapor da caldeira auxiliar	<ul style="list-style-type: none"> ▪ Informação dos alarmes ativos: <ul style="list-style-type: none"> - alarme de baixa pressão de vapor: alarme considerado comum quando a caldeira falhava em iniciar ignição. ▪ Informação dos alarmes inativos: <ul style="list-style-type: none"> - ausência de outros alarmes indicava que não era falha na ignição. - não havia alarmes de nível baixo de água. - não havia alarme de falha no sistema de controle da caldeira.
3. Aumento da temperatura do economizador	<ul style="list-style-type: none"> ▪ Informação dos alarmes ativos: <ul style="list-style-type: none"> - alta temperatura do economizador a 350°C. ▪ Informação dos alarmes inativos: <ul style="list-style-type: none"> - não havia alarme de falha no soprador de fuligem do economizador, mas este estava operando em modo manual.
4. Incêndio no economizador	<ul style="list-style-type: none"> ▪ Informação dos alarmes ativos: <ul style="list-style-type: none"> - alta temperatura do economizador a 600°C. Era o fundo de escala do indicador, podendo significar que a temperatura estaria muito mais alta que este valor, indicando um incêndio no interior do economizador. ▪ Informação dos alarmes inativos: <ul style="list-style-type: none"> - não havia alarme de falha no soprador de fuligem do economizador, mas este estava operando em modo manual.
5. Propagação do incêndio na praça de máquinas	<ul style="list-style-type: none"> ▪ Informação dos alarmes ativos: <ul style="list-style-type: none"> - Alarme de emergência da embarcação.

Segundo Nasa (2002), o diagrama de sequência de eventos pode ser um passo anterior à elaboração da árvore de eventos de um acidente, que é a ferramenta gráfica útil para a análise probabilística quantitativa de um acidente. A

Figura 54 apresenta a árvore de eventos do acidente a partir do diagrama de sequência de eventos.

A elaboração destas duas representações gráficas, o diagrama de sequência de eventos e a árvore de eventos, é útil no entendimento e identificação dos possíveis cenários. O objetivo deste estudo de caso é aplicar a metodologia proposta a estes cenários identificados. Não serão feitas análises e discussões aprofundadas sobre o diagrama de sequência de eventos e a árvore de eventos.

Figura 54 – Árvore de eventos do acidente

Foram obtidos seis cenários a partir da análise da sequência do acidente:

- Cenário 1: Ocorre a falha no sistema automático da caldeira auxiliar, causando o seu desligamento. Mas não há ruptura de sua tubulação de vapor interna, nem sobreaquecimento do economizador. Com o sistema de limpeza de fuligem do economizador operando normalmente, a única consequência seria a necessidade de buscar fontes alternativas para o aquecimento o óleo pesado, ou operar o motor principal com diesel.

- Cenário 2: Ocorre a falha no sistema automático da caldeira auxiliar, causando o seu desligamento. Mas não há ruptura de sua tubulação de vapor interna, nem sobreaquecimento do economizador. No entanto, o sistema de limpeza de fuligem não é operado em modo automático. As consequências seriam a necessidade de buscar fontes alternativas para o aquecimento o óleo pesado, e o acúmulo de fuligem no economizador, o qual não teria sua operação afetada.
- Cenário 3: Ocorre a falha no sistema automático da caldeira auxiliar, causando a ruptura da tubulação interna de vapor, e sobreaquecimento no economizador, devido à diminuição de circulação de água. Porém o sistema de limpeza de fuligem estaria funcionando corretamente em modo automático. A ausência de fuligem impediria o início do incêndio no interior do economizador. As consequências desse cenário seriam um aumento de temperatura no economizador, que poderia causar danos, e a necessidade de se buscar fontes alternativas para o aquecimento do óleo pesado do motor principal.
- Cenário 4: Ocorre a falha no sistema automático da caldeira auxiliar, causando a ruptura da tubulação interna de vapor, e sobreaquecimento no economizador. Também, o sistema de limpeza de fuligem não estaria funcionando. Ainda não havendo indício de incêndio no economizador, a decisão de cortar a fonte de calor principal, ou seja, desligar o motor principal, impediria a ignição da fuligem, evitando o incêndio.
- Cenário 5: Dadas as condições do cenário 4, havendo início de incêndio no economizador, este poderia ser rapidamente apagado evitando danos relevantes à estrutura do economizador, e a propagação do fogo na praça de máquinas.
- Cenário 6: propagação do fogo na praça de máquinas (acidente).

Uma vez obtidos ou definidos estes possíveis cenários, o próximo passo é aplicar a metodologia proposta a cada um deles, conforme será exposto a seguir. Vale observar que a análise ainda poderia ser estendida a outros cenários, como considerar o caso do incêndio não ser combatido e se propagar por toda a embarcação, causando avaria não só às máquinas, mas a todo o navio. Ou um cenário que considerasse não apenas a perda do navio, mas de sua carga, causando prejuízos ambientais, ou na imagem da empresa, ou mesmo ações judiciais contra o armador. Para não deixar a análise demasiadamente prolongada, considera-se o escopo descrito no relatório de investigação como suficiente para ilustrar a metodologia proposta neste estudo de caso.

6.2.5. Identificação dos fatores humanos e organizacionais

O guia de avaliação formal de segurança (FSA) da IMO (2002a), comentado na seção 2.4, sugere a inclusão do processo de identificação de perigos humanos (“*human hazards*”) na metodologia de análise de risco, definindo este como sendo o processo de sistematicamente identificar as maneiras pelas quais o erro humano pode contribuir para a ocorrência de acidentes. A definição de perigos humanos se insere nos conceitos de fatores humanos e organizacionais tratados no Capítulo 3, e por isso, o levantamento dos fatores humanos e organizacionais é mais geral que o proposto pela FSA.

Por certo, um processo bem conduzido de identificação dos fatores humanos e organizacionais exigiria uma pesquisa muito mais cuidadosa, extrapolando o texto do relatório de investigação do acidente, e, provavelmente, exigindo até vistorias ou entrevistas específicas. No entanto, é possível listar alguns fatores humanos e organizacionais identificáveis na narrativa e análise do acidente.

As Tabelas 24 a 27 elencam alguns possíveis fatores humanos e organizacionais presentes no acidente com a embarcação Maersk Doha. Os fatores organizacionais foram classificados seguindo a divisão proposta na subseção 3.1.4.2 (pág. 70), a qual propõe separá-los em fatores relacionados à tripulação, ao sistema técnico e aos níveis de perda. A coluna à direita apresenta alguns comentários sobre cada fator, remetendo a algum fato descrito no relatório de investigação do acidente.

Tabela 25 – Fatores humanos identificados no relatório de investigação

Fator Humano	Comentários
Experiência	Falta de experiência dos oficiais.
Liderança	Falta de liderança do chefe de máquinas.
Consciência situacional	Falta de consciência situacional da tripulação.
Linguagem	Dificuldade de comunicação do chefe de máquinas.
Motivação	Propensão do chefe de máquinas a assumir risco frente a tomar uma decisão impopular de parar o navio.
Conhecimento	Falta de conhecimento sobre funcionamento das máquinas.

Tabela 26 – Fatores organizacionais relacionados à tripulação

Fatores organizacionais relacionados à tripulação	Comentários
Política de seleção	Inadequados critérios de seleção permitiram a chefe de máquinas ser contratado com nível de conhecimento em inglês inferior ao recomendado.
Cultura organizacional	Complacência sobre resultados das simulações de emergência. Tolerância a riscos técnicos em detrimento à segurança. Auditorias internas e externas não detectaram fraquezas nas políticas de manutenção e nos procedimentos de segurança.
Política de treinamento	Falta de investimento em treinamentos sobre funcionamento das máquinas e sobre técnicas de combate a incêndio.
Comprometimento com normas de segurança	Chefe de máquinas sugere comandante a continuar navegação.
Comprometimento com hierarquia	2º Oficial desobedece chefe de máquinas.
Filosofia orientada à segurança	Chefe de máq. sugere comandante a continuar navegação. Decisão do comandante em continuar navegação. Complacência com impressora com papel prensado, durante mais de uma semana.
Comunicação interna	Problema de comunicação durante estágios iniciais, quando o chefe de máquinas não reportou problema completo ao comandante. Armador não reforçou suficientemente a existência de arquivos com procedimentos de emergência, e importância das circulares técnicas. Tripulação desconhecia circular que tratava sobre incêndio na fuligem do economizador. Limitada interação entre equipes de deck e engenharia. Sistema computacional de SMS (Safety Management System) não era suficientemente conhecido e utilizado.

Tabela 27 – Fatores organizacionais relacionados ao sistema técnico

Fatores organizacionais relacionados ao sistema técnico	Comentários
Políticas de inspeção	<p>Inspeção do sistema de CO₂ falharam em detectar problema no sistema de válvula piloto.</p> <p>Tripulação desconhecia procedimentos de inspeção e testes do sistema de monitoramento.</p>
Políticas de manutenção	<p>Prioridade maior para reparo de defeitos que para manutenção preventiva.</p> <p>Diversos sistemas de emergência falharam quando solicitados, indicando que manutenção não detectaram defeitos latentes:</p> <ul style="list-style-type: none"> - Bomba reserva de circulação de água do economizador - Sistema de CO₂ - Gerador de emergência a diesel - Bomba de incêndio de emergência

Tabela 28 – Fatores organizacionais relacionados aos níveis de perda

Fatores organizacionais relacionados aos níveis de perda e consequências	Comentários
Treinamento para situações de emergência ou acidentes	<p>Procedimentos de emergência não eram familiares suficiente para serem úteis.</p> <p>Tripulação desconhecia manual que tratava sobre incêndio na fuligem do economizador.</p> <p>Armador não reforçou suficientemente a existência de arquivos com procedimentos de emergência, e importância das circulares técnicas.</p> <p>Complacência sobre resultados das simulações de emergência.</p>
Treinamento para mitigação de consequências	Complacência sobre resultados das simulações de emergência.
Seleção de pessoal com perfil adequado	Comandante recusou oferta do piloto em requisitar assistência à guarda costeira americana.

Os fatores humanos e organizacionais apresentados nas tabelas anteriores descrevem o contexto das ações humanas e do ambiente na ocasião do acidente. Estas informações serão úteis durante a aplicação dos métodos de análise de confiabilidade humana, conforme será visto nas seções seguintes.

6.2.6. Modelagem do problema e formulação matemática

Neste ponto do estudo, o analista já teria as informações necessárias para a aplicação da metodologia proposta no Capítulo 5. O cenário que será analisado neste estudo de caso é o cenário 6 (Figura 54), ou seja, o acidente em si, resultando no incêndio da praça de máquinas da embarcação Maersk Doha. O cenário 6 cobre praticamente as análises que seriam feitas nos cenários de 1 a 5, portanto, para os objetivos deste estudo de caso, é o mais adequado.

Para todas as fases, adotou-se um procedimento padrão de: (i) estruturar as variáveis (evento iniciador, conjunto dos fatores humanos e organizacionais) e recuperação do sistema); (ii) definir os possíveis conjuntos mutuamente exclusivos e exaustivos dos estados do sistema de alarmes, interpretações e decisões e ações da tripulação; (iii) obter a equação geral do modelo.

Como proposto na seção 6.2.4, far-se-á a análise em fases de acordo com a Tabela 23. A fase 5 não será analisada, pois faz parte da recuperação do navio, ou seja, o combate e extinção do incêndio, não envolvendo nenhuma interação relevante com o sistema de alarmes.

▪ Fase 1: do evento iniciador até a ruptura da caldeira

Seguindo a estrutura de análise proposta na Figura 47 (pág. 146), a sequência do acidente aplicada à fase 1 é apresentada na Figura 55.

Figura 55 – Sequência de eventos – fase 1

O objetivo será estruturar a equação probabilística desta sequência, conforme a equação geral do modelo de análise proposto, eq. (25), pág. 150. Para tal, devem-se fazer as seguintes definições:

- Evento iniciador E_{fase1} : falha no sistema automático da caldeira
- Conjunto dos fatores humanos e organizacionais do contexto O_1 : conjunto dos fatores representados nas Tabelas 24 a 27.
- Recuperação do Sistema Rec_{fase1} : recuperar a falha no sistema automático da caldeira, impedindo a ruptura da tubulação e perda de água.

A Tabela 29 apresenta uma possibilidade de formação dos conjuntos mutuamente exclusivos e exaustivos A_j , I_k , e D_n . Naturalmente a formação deste conjunto irá variar de acordo com a percepção de cada analista, e com o nível de detalhe desejado para analisar o problema. O conjunto dos estados do sistema de alarmes, por exemplo, é composto apenas por alguns estados julgados relevantes na análise. Estados com probabilidade baixa de ocorrência podem ser omitidos, para diminuir a complexidade das equações. O conjunto de interpretações e decisões também pode ser tão numeroso quando se desejar. Para simplificar o problema, escolheu-se agrupar as interpretações não relevantes ou não relacionadas ao evento iniciador no elemento I_4 , e as decisões sem influência na recuperação do problema em D_5 . Assim, considera-se que qualquer outra interpretação ou decisão não listada não irá influenciar a recuperação do sistema.

Tabela 29 – Conjunto das variáveis do modelo na fase 1 do acidente

CONJUNTO DOS ESTADOS DO SISTEMA DE ALARMES A_j	CONJUNTO DAS INTERPRETAÇÕES DA TRIPULAÇÃO I_k	CONJUNTO DAS DECISÕES E AÇÕES DA TRIPULAÇÃO D_n
<ul style="list-style-type: none"> • A_1: NENHUM ALARME ATIVO • A_2: ALARME DE FALHA DO SISTEMA AUTOMÁTICO DA CALDEIRA ATIVO • A_3: FALSO ALARME ATIVO • A_4: ALARME DE FALHA DO SISTEMA AUTOMÁTICO E FALSO ALARMES ATIVO 	<ul style="list-style-type: none"> • I_1: NENHUMA INTERPRETAÇÃO • I_2: FALHA NO SISTEMA AUTOMÁTICO DA CALDEIRA • I_3: FALHA EM OUTRO SISTEMA • I_4: OUTRA INTERPRETAÇÃO NÃO RELACIONADA COM O EVENTO INICIADOR 	<ul style="list-style-type: none"> • D_1: NENHUMA DECISÃO OU AÇÃO • D_2: DESLIGAR A CALDEIRA • D_3: DESLIGAR MOTOR PRINCIPAL • D_4: REDUZIR ROTAÇÃO DO MOTOR • D_5: OUTRA DECISÃO SEM INFLUÊNCIA NA RECUPERAÇÃO DO PROBLEMA

O conjunto dos fatores humanos e organizacionais não foi incluído na Tabela 29, pois partiu-se da premissa que não é necessário fazer a distinção do conjunto dos fatores organizacionais entre as fases, pois não houve nenhum acontecimento

que determinasse a alteração do contexto entre uma fase e outra. Em outras palavras, pode-se considerar o conjunto dos fatores organizacionais O_m , como sendo formado apenas por um elemento, O_1 , que será o mesmo para as fases 1 a 4.

Logo, para esta fase do acidente, a equação geral do modelo, eq. (25) (pág. 150), pode ser escrita da seguinte maneira:

$$\begin{aligned}
 P(Rec_{fase\ 1} | E_{fase\ 1}, O_1) \\
 = \sum_{n=1}^5 \sum_{k=1}^4 \sum_{j=1}^4 P(A_j | E_{fase\ 1}) \cdot P(I_k | A_j, O_1) \cdot P(D_n | I_k, O_1) \\
 \cdot P(Rec_{fase\ 1} | D_n)
 \end{aligned} \tag{26}$$

Dependendo do interesse do analista, é possível fazer análises específicas de determinados eventos. Um exemplo interessante seria a análise para se entender a probabilidade do sistema ter sido recuperado, de acordo com a sequência real do acidente, é particularizar a equação geral com os eventos que realmente ocorreram. Para a fase 1, a equação geral do modelo pode ser particularizada conforme segue:

$$\begin{aligned}
 P(Rec_{fase\ 1} | E_{fase\ 1}, O_1) = \\
 P(A_1 | E_{fase\ 1}) \cdot P(I_1 | A_1, O_1) \cdot P(D_1 | I_1, O_1) \cdot P(Rec_{fase\ 1} | D_1)
 \end{aligned} \tag{27}$$

Embora não tenha ocorrido, poderia ser interesse do analista estudar outros cenários, bastando particularizar a equação geral da mesma maneira. Para o cenário particular definido acima, da eq. (27) podem-se extrair as seguintes conclusões:

- A probabilidade de recuperação da caldeira, dado a decisão D_1 , $P(Rec_{fase\ 1} | D_1)$, pode ser considerada zero. Ou seja, não sendo tomada nenhuma ação, ocorrerá a ruptura da fornalha.
- A probabilidade de se tomar uma decisão ou ação correta, dada a interpretação do alarme I_1 , $P(D_1 | I_1, O_1)$, também pode ser considerada zero. Ou seja, não ocorrendo interpretação dos alarmes, nenhuma ação é tomada.

- A probabilidade de ser realizada uma interpretação correta, dado o estado do sistema de alarmes A_1 , $P(I_1|A_1, O_1)$, também pode ser considerada zero. Ou seja, não havendo nenhum alarme ativo, a tripulação não será chamada a atenção para interpretar o estado do sistema de alarmes.

Portanto, o termo a ser trabalhado nesta fase, ocorrido estes acontecimentos, é o termo $P(A_j|E_{fase\ 1})$, que trata da probabilidade de um estado do sistema de alarmes, dado o evento iniciador de falha no sistema automático da caldeira. A seção 5.7 orienta como deve ser feita a análise deste termo. Este termo é relacionado com o sistema físico, logo, as análises pertinentes se darão no domínio das técnicas de confiabilidade de sistemas. A pergunta a ser respondida é como garantir o anúncio de um alarme, em caso da falha do sistema automático da caldeira. Pelo reportado no relatório de investigação, pode-se concluir que:

- Ou o sistema automático da caldeira falhou em sinalizar ao sistema de alarmes sua falha, através do alarme de situação anormal na caldeira auxiliar ou de algum alarme de nível (ver Tabela 21, página 161).
- Ou o sistema de alarmes falhou em anunciar estes alarmes, o que não pode ser descartado, pois o relatório de investigação citava que não havia um protocolo de inspeção ou testes periódicos.
- Ou para esse tipo de falha no sistema automático da caldeira, não havia um alarme específico previsto.

Para aumentar a confiabilidade deste tipo de monitoramento, as sociedades classificadoras exigem que as falhas de sistemas sejam sinalizadas através de contatos tipo normalmente fechados. Assim, uma máquina deve manter um relé fechado enquanto operando. Em caso de falha, este relé abre naturalmente, indicando o alarme.

Não será feito o aprofundamento na análise do termo $P(A_j|E_{fase\ 1})$, uma vez que este pode ser estudado através das técnicas conhecidas de análise de confiabilidade de sistemas (ver Figura 50, pág. 154). No entanto, outras análises poderiam ser úteis, considerando o estado do sistema de alarmes A_2 , o qual

indicaria o anúncio de um alarme de falha no sistema automático da caldeira. Neste caso, trata-se de um exemplo típico onde a recuperação do sistema é dependente do tempo disponível de recuperação. Pela Tabela 22 (pág. 165), sabe-se que este tempo é inferior a 26 minutos, pois foi o intervalo de tempo entre a partida do motor e o primeiro alarme de baixa pressão no sistema de vapor, quando a fornalha já estava rompida. O exemplo de análise do cenário com o estado do sistema de alarmes A_2 não será apresentado, uma vez que será apresentado um exemplo semelhante nas análises das fases do acidente a seguir.

▪ **Fase 2: da ruptura da tubulação de vapor da caldeira auxiliar até o aumento de temperatura do economizador**

A sequência dos eventos da fase 2 pode ser estruturada conforme mostrado na Figura 56. Para não causar conflito com o termo “evento iniciador” da fase 1, que deve ser entendido como o evento gatilho que originou a sequência de eventos, o termo “evento inicial” será utilizado para denominar o primeiro evento que caracteriza as fases 2 a 4.

As variáveis do problema são definidas da seguinte maneira:

- Evento inicial E_{fase2} : Ruptura da tubulação de vapor da caldeira auxiliar e diminuição da vazão de água no economizador
- Conjunto dos fatores humanos e organizacionais do contexto O_1 : conjunto dos fatores representados nas Tabelas 24 a 27.
- Recuperação do Sistema Rec_{fase2} : recuperar a perda de água do economizador, impedindo o seu sobreaquecimento.

FASE 2

Figura 56 – Sequência de eventos – fase 2

A Tabela 30 mostra possíveis elementos dos conjuntos de A_j , I_k , e D_n .

Tabela 30 – Conjunto das variáveis do modelo na fase 2 do acidente

CONJUNTO DOS ESTADOS DO SISTEMA DE ALARMES A_j	CONJUNTO DAS INTERPRETAÇÕES DA TRIPULAÇÃO I_k	CONJUNTO DAS DECISÕES E AÇÕES DA TRIPULAÇÃO D_n
<ul style="list-style-type: none"> • A_1: ALARME PRESSÃO BAIXA VAPOR • A_2: NENHUM ALARME ATIVO • A_3: FALSO ALARME ATIVO • A_4: ALARME PRESSÃO BAIXA VAPOR E UM FALSO ALARME ATIVO 	<ul style="list-style-type: none"> • I_1: FALHA NA CALDEIRA AUXILIAR • I_2: NENHUMA INTERPRETAÇÃO • I_3: FALHA EM OUTRO SISTEMA • I_4: OUTRA INTERPRETAÇÃO NÃO RELACIONADA COM O EVENTO INICIAL 	<ul style="list-style-type: none"> • D_1: CONTINUAR NAVEGAÇÃO • D_2: PARAR NAVEGAÇÃO • D_3: OUTRA DECISÃO SEM INFLUÊNCIA NA RECUPERAÇÃO DO PROBLEMA

Portanto, a equação geral para a fase 2 pode ser escrita como segue:

$$\begin{aligned}
 &P(Rec_{fase\ 2} | E_{fase\ 2}, O_1) \\
 &= \sum_{n=1}^3 \sum_{k=1}^4 \sum_{j=1}^4 P(A_j | E_{fase\ 2}) \cdot P(I_k | A_j, O_1) \cdot P(D_n | I_k, O_1) \\
 &\quad \cdot P(Rec_{fase\ 2} | D_n)
 \end{aligned} \tag{28}$$

Assim como feito na fase 1, pode-se particularizar a eq. (28), apenas com os eventos que realmente ocorreram, que foram A_1 , I_1 , e D_1 . A eq. (29) mostra o resultado deste processo.

$$P(Rec_{fase\ 2}|E_{fase\ 2}, O_1) = P(A_1|E_{fase\ 2}) \cdot P(I_1|A_1, O_1) \cdot P(D_1|I_1, O_1) \cdot P(Rec_{fase\ 2}|D_1) \quad (29)$$

Da eq. (29) é possível extrair algumas conclusões preliminares:

- O primeiro termo, $P(A_1|E_{fase\ 2})$, significa a probabilidade do anúncio de um alarme de pressão baixa no sistema de vapor. Este termo é analisado com as técnicas de análise de confiabilidade de sistemas. Para sistemas bem operados e com manutenção regular, pode-se esperar uma confiabilidade alta do anúncio de um alarme de pressão baixa. Além disso, a implementação de redundâncias de medidas (sensores) e de anúncio de alarme, garante uma confiabilidade suficiente para esta aplicação.
- O termo $P(I_k|A_1, O_1)$ trata da interpretação de um alarme de pressão baixa. Pelo relatório de investigação, nota-se que a tripulação associou este alarme imediatamente a um problema na caldeira, sendo este uma falha de ignição, ou outra falha.
- O termo que mereceria mais atenção é o termo $P(D_n|I_1, O_1)$ que expressa a probabilidade de uma decisão acertada, dada a interpretação de um alarme de falha na caldeira auxiliar. A tomada de decisão nesta situação sofreu influência de um conflito entre executar uma ação impopular (parar a navegação) e a propensão em assumir o risco de danificar uma máquina do navio (fator organizacional).
- O último termo $P(Rec_{fase\ 2}|D_n)$ não exigiria a aplicação de nenhum método específico. Poder-se-ia considerar simplesmente que:
 - $P(Rec_{fase\ 2}|D_1) = 0$ (decisão de continuar navegação)
 - $P(Rec_{fase\ 2}|D_2) = 1$ (decisão de parar a navegação)
 - $P(Rec_{fase\ 2}|D_3) = 0$ (outra decisão sem influência na recuperação do problema)

Sabe-se que continuar a navegação implica o aumento da temperatura do economizador (dado que a circulação de água estava comprometida devido à ruptura da tubulação de vapor na caldeira auxiliar). E que parar a navegação implica cortar a fonte de calor, e impedir o aumento da temperatura.

Na análise da recuperação do problema, o fator tempo também é relevante. A Tabela 22 (pág. 165) aponta que o intervalo de tempo entre a ruptura da fornalha e o alarme de alta temperatura no economizador foi de uma hora e 13 minutos. Portanto, uma análise importante a ser feita para esta fase 2 é a análise do termo $P(D_n|I_1, O_1)$, dando preferência à escolha de métodos de confiabilidade humana baseados em tempo, ou cuja descrição do contexto também considerasse o tempo disponível.

▪ **Fase 3: do aumento de temperatura até incêndio no economizador**

Para fase 3 do acidente, a sequência de eventos é desenhada na Figura 57. A Tabela 31 apresenta os elementos dos conjuntos dos estados do sistema de alarmes, das interpretações e decisões e ações. As variáveis do problema são definidas como:

- Evento inicial E_{fase3} : aumento de temperatura no economizador
- Conjunto dos fatores humanos e organizacionais do contexto O_1 : conjunto dos fatores representados nas Tabelas 24 a 27.
- Recuperação do Sistema Rec_{fase3} : recuperar sobreaquecimento do economizador, impedindo a ignição da fuligem, e consequente incêndio.

Figura 57 – Sequência de eventos – fase 3

Tabela 31 – Conjunto das variáveis do modelo na fase 3 do acidente

CONJUNTO DOS ESTADOS DO SISTEMA DE ALARMES A_j	CONJUNTO DAS INTERPRETAÇÕES DA TRIPULAÇÃO I_k	CONJUNTO DAS DECISÕES E AÇÕES DA TRIPULAÇÃO D_n
<ul style="list-style-type: none"> • A_1: ALARME DE TEMPERATURA ALTA NO ECONOMIZADOR 350°C • A_2: NENHUM ALARME ATIVO • A_3: FALSO ALARME ATIVO • A_4: ALARME DE TEMPERATURA ALTA NO ECONOMIZADOR E FALSO ALARME ATIVO 	<ul style="list-style-type: none"> • I_1: PROBLEMA DE CIRCULAÇÃO DE ÁGUA NO ECONOMIZADOR • I_2: NENHUMA INTERPRETAÇÃO • I_3: FALHA EM OUTRO SISTEMA • I_4: OUTRA INTERPRETAÇÃO NÃO RELACIONADA COM O EVENTO INICIAL 	<ul style="list-style-type: none"> • D_1: REDUZIR A ROTAÇÃO DO MOTOR • D_2: MANTER NAVEGAÇÃO EM ALTA ROTAÇÃO • D_3: PARAR A NAVEGAÇÃO • D_4: BUSCAR ALTERNATIVAS PARA RESFRIAR OU LIMPAR O ECONOMIZADOR • D_5: OUTRA DECISÃO SEM INFLUÊNCIA NA RECUPERAÇÃO DO PROBLEMA

A equação geral que descreve a fase 3 é dada por:

$$\begin{aligned}
 &P(Rec_{fase\ 3} | E_{fase\ 3}, O_1) \\
 &= \sum_{n=1}^5 \sum_{k=1}^4 \sum_{j=1}^4 P(A_j | E_{fase\ 3}) \cdot P(I_k | A_j, O_1) \cdot P(D_n | I_k, O_1) \\
 &\quad \cdot P(Rec_{fase\ 3} | D_n)
 \end{aligned} \tag{30}$$

Novamente, particularizar a equação geral com os eventos reais ocorridos, auxilia o início da análise e a extração de algumas conclusões preliminares:

$$\begin{aligned}
 &P(Rec_{fase\ 3} | E_{fase\ 3}, O_1) = \\
 &P(A_1 | E_{fase\ 3}) \cdot P(I_1 | A_1, O_1) \cdot P(D_1 | I_1, O_1) \cdot P(Rec_{fase\ 3} | D_1)
 \end{aligned} \tag{31}$$

A análise minuciosa da eq. (31) permite afirmar que:

- O mesmo que foi afirmado em relação ao primeiro termo da eq. (29), da fase 2, pode-se estender para o termo $P(A_1 | E_{fase\ 3})$. Pode-se esperar uma alta confiabilidade de medida de temperatura em sistemas bem operados e com manutenção em dia. Durante a fase 3, o sistema de alarmes capturou a condição anormal corretamente.
- O termo que trata a interpretação do alarme, $P(I_k | A_1, O_1)$, pode ser analisado de 2 maneiras:

- O alarme de alta temperatura no economizador pode ser considerado óbvio demais para merecer uma análise mais aprofundada. Desta forma, considera-se que todo tripulante, com o mínimo de qualificação, saberia interpretar o alarme como um problema de circulação de água no economizador.
- Ou, pode-se considerar a interpretação deste alarme como mais complexa, e aplicar algum método de confiabilidade humana, conforme sugerido na seção 5.7 (pág. 150). Para fins didáticos, considerar-se-á esta segunda maneira, para poder ilustrar como abordar o problema.
- O termo que trata tomada de decisão $P(D_n|I_1, O_1)$ também merece maior atenção, pois se trata da mesma situação de conflito da fase 2. Este termo também pode ser analisado levando em consideração o fator tempo. Conforme narrativa do acidente, entre o alarme de temperatura alta de 350°C e o alarme de 600°C se passaram apenas 5 minutos.
- Assim como na fase 2, o último termo também pode ser analisado de forma simplificada:
 - $P(Rec_{fase\ 3}|D_1) = 0$ (decisão de reduzir a rotação do motor)
 - $P(Rec_{fase\ 3}|D_2) = 0$ (decisão de manter motor em alta rotação)
 - $P(Rec_{fase\ 3}|D_3) = 1$ (parar a navegação)
 - $P(Rec_{fase\ 3}|D_5) = 0$ (outra decisão sem influência na recuperação do problema)

Apenas o termo $P(Rec_{fase\ 3}|D_4)$ (buscar alternativas para limpar ou resfriar o economizador) poderia ter uma probabilidade diferente de 0 e 1. A consulta a especialistas, conforme sugerido na seção 5.7 (pág. 150), seria um método apropriado para quantificar este termo. Um exemplo de aplicação do método de consulta a especialistas não será apresentado neste trabalho, uma vez que o leitor poderá consultar uma das referências citadas na seção 2.8 (pág. 46).

- **Fase 4: do incêndio no economizador até a propagação na praça de máquinas**

A quarta fase do acidente será analisada conforme a sequência de eventos da Figura 58 e conjunto dos elementos da Tabela 32. Assim como nas fases anteriores, as variáveis do problema são definidas como:

- Evento inicial E_{fase4} : incêndio no interior do economizador
- Conjunto dos fatores humanos e organizacionais do contexto O_1 : conjunto dos fatores representados nas Tabelas 24 a 27.
- Recuperação do Sistema Rec_{fase4} : controlar ou extinguir o incêndio, impedindo que este se alastre para a praça de máquinas.

Figura 58 – Sequência de eventos – fase 4

Tabela 32 – Conjunto das variáveis do modelo na fase 4 do acidente

CONJUNTO DOS ESTADOS DO SISTEMA DE ALARMES A_j	CONJUNTO DAS INTERPRETAÇÕES DA TRIPULAÇÃO I_k	CONJUNTO DAS DECISÕES E AÇÕES DA TRIPULAÇÃO D_n
<ul style="list-style-type: none"> • A_1: ALARME DE TEMPERATURA ALTA NO ECONOMIZADOR 600°C • A_2: NENHUM ALARME ATIVO • A_3: FALSO ALARME ATIVO • A_4: ALARME DE TEMPERATURA ALTA NO ECONOMIZADOR 600°C E FALSO ALARME ATIVO 	<ul style="list-style-type: none"> • I_1: INCÊNDIO NO ECONOMIZADOR • I_2: NENHUMA INTERPRETAÇÃO • I_3: FALHA EM OUTRO SISTEMA • I_4: OUTRA INTERPRETAÇÃO NÃO RELACIONADA COM O EVENTO INICIAL 	<ul style="list-style-type: none"> • D_1: PARAR EMBARCAÇÃO E COMBATER INCÊNDIO COM MANGUEIRAS E CO₂ • D_2: PARAR EMBARCAÇÃO E COMBATER INCÊNDIO DE FORMA CORRETA • D_3: CONTINUAR A NAVEGAÇÃO E COMBATER O INCÊNDIO • D_4: OUTRA DECISÃO SEM INFLUÊNCIA NA RECUPERAÇÃO DO PROBLEMA

A equação geral para a fase 4 é dada por:

$$\begin{aligned}
 P(Rec_{fase\ 4} | E_{fase\ 4}, O_1) \\
 = \sum_{n=1}^4 \sum_{k=1}^4 \sum_{j=1}^4 P(A_j | E_{fase\ 4}) \cdot P(I_k | A_j, O_1) \cdot P(D_n | I_k, O_1) \\
 \cdot P(Rec_{fase\ 4} | D_n)
 \end{aligned} \tag{32}$$

Particularizando a eq. (32) para os eventos ocorridos, tem-se a eq.(33):

$$\begin{aligned}
 P(Rec_{fase\ 4} | E_{fase\ 4}, O_1) = \\
 P(A_1 | E_{fase\ 4}) \cdot P(I_1 | A_1, O_1) \cdot P(D_1 | I_1, O_1) \cdot P(Rec_{fase\ 4} | D_1)
 \end{aligned} \tag{33}$$

Da eq.(33), podem-se extrair as seguintes conclusões:

- O termo $P(A_1 | E_{fase\ 4})$ expressa a probabilidade do sistema de alarmes sinalizar a temperatura alta no economizador. Os comentários que cabem aqui são os mesmos da fase 2 e 3. A única observação a acrescentar é que, no caso extremo de um incêndio, pode haver avarias nos sensores do sistema de alarmes. Neste caso, o sistema sinalizaria um erro de sensor, mascarando a interpretação da situação real do sistema.
- O termo $P(I_k | A_1, O_1)$ expressa a probabilidade de interpretação do alarme de temperatura alta. Uma indicação analógica de temperatura, com fundo de escala, como foi mencionado do relatório de acidentes, deixa claro que a situação se tratava de algo mais grave que um sobreaquecimento.
- O termo $P(D_n | I_1, O_1)$ expressa a probabilidade de uma decisão, dada a interpretação que havia um incêndio no economizador. Pode-se considerar que duas decisões relevantes foram tomadas. A primeira decisão foi a de parar o motor e ancorar a embarcação para combater o incêndio. Trata-se de uma decisão acertada, e, ao mesmo tempo, bastante óbvia, naquele momento do acidente. A segunda decisão, portanto, que mereceria mais atenção, foi a de combater o incêndio com mangueiras, jorrando água na parede do economizador. O cálculo

deste termo deve levar em conta primordialmente os fatores humanos e organizacionais relacionados ao treinamento para situações de emergência.

- O termo $P(Rec_{fase3}|D_n)$ expressa a probabilidade de extinção do incêndio, dada uma determinada opção de estratégia de combate ao fogo. Uma possível forma de tratar este termo é utilizar técnicas de consulta a especialistas. Eventualmente, um conjunto maior de elementos D_n poderiam ser analisados, cobrindo todas as possíveis opções e todos os equipamentos de combate ao incêndio disponíveis.

De posse das quatro equações gerais de cada fase, eqs. (26), (28), (30) e (32), é possível escrever a equação geral do acidente. Para tal, algumas definições devem ser feitas:

- Evento inicial E : falha no sistema automático da caldeira (E_{fase1})
- Conjunto dos fatores humanos e organizacionais do contexto O_1 : conjunto dos fatores representados nas Tabelas 24 a 27.
- Recuperação do Sistema Rec : controlar ou extinguir o incêndio, impedindo que este se alastre para a praça de máquinas, que é a recuperação da fase 4, Rec_{fase4} .

Enxergando as quatro fases como um problema único, a não recuperação de uma fase implica no evento inicial da fase seguinte. Logo, para a recuperação do evento iniciador (falha no sistema automático da caldeira auxiliar), uma das três fases anteriores deve ser recuperada.

$$Rec = Rec_{fase1} "OU" Rec_{fase2} "OU" Rec_{fase3} \quad (34)$$

Relembrando a operação “OU” para três eventos:

$$\begin{aligned} P(A + B + C) &= P(A) + P(B) + P(C) \\ &- P(A e B) - P(A e C) - P(B e C) + P(A e B e C) \end{aligned} \quad (35)$$

Da eq. (35), percebe-se que os eventos Rec_{fase1} , Rec_{fase2} , Rec_{fase3} são mutuamente exclusivos, pois não é possível considerar a recuperação simultânea das fases 1 e 2, por exemplo. Isso implica que $P(Rec_{fase1} \text{ e } Rec_{fase2}) = 0$, assim como as demais combinações. Isso também pode ser intuído, uma vez que os eventos ocorrem em uma sequência. A eq. (36) apresenta a forma final da equação contemplando todas as fases, e já com a condição da existência do evento iniciador E , e do contexto dos fatores humanos e organizacionais O_1 .

$$P(Rec|E, O_1) = P(Rec_{fase1}|E, O_1) + P(Rec_{fase2}|E_{fase2}, O_1) \cdot P(E_{fase2}|E) + P(Rec_{fase3}|E_{fase3}, O_1) \cdot P(E_{fase3}|E_{fase2}, E) \quad (36)$$

A Figura 59 apresenta um diagrama que representa a eq. (36). Trata-se de uma visão de recuperação do sistema. Alternativamente, o analista poderia preferir uma visão de falha do sistema, e desejar calcular a probabilidade do acidente. A Figura 60 apresenta um diagrama que considera os eventos como sendo os incidentes das fases.

Figura 59 – Visão de recuperação do sistema

Figura 60 – Visão de falha do sistema

Nesse caso, para acontecer o acidente (propagação do incêndio), devem ocorrer os três incidentes intermediários:

$$Acidente = E_{fase2} \text{ "e" } E_{fase3} \text{ "e" } E_{fase4} \quad (37)$$

Relembrando a operação “e” para três eventos não independentes:

$$P(A \text{ e } B \text{ e } C) = P(A) \cdot P(B|A) \cdot P(C|A \text{ e } B) \quad (38)$$

O resultado final é a eq. (39), já condicionando o problema à existência do evento iniciador E , e do contexto dos fatores humanos e organizacionais O_1 .

$$\begin{aligned} P(Acidente|E, O_1) \\ = P(E_{fase2}|E, O_1) \cdot P(E_{fase3}|E_{fase2}, O_1) \\ \cdot P(E_{fase4}|E_{fase2} \text{ e } E_{fase3}, O_1) \end{aligned} \quad (39)$$

Vale lembrar que $P(Rec|E, O_1) = 1 - P(Acidente|E, O_1)$. Assim, as eqs. (36) e (39) reconstituem a divisão do problema em fases, em uma análise única. Estas duas equações expressam a probabilidade de recuperar o sistema dado um evento iniciador ou a probabilidade de ocorrer um acidente, dado um evento iniciador. O cálculo do valor destas probabilidades pode ser bastante custoso, dependendo da modelagem do problema, e da quantidade de fases e elementos dos conjuntos A_j , I_k , e D_n . No entanto, como já foi comentado, o trabalho da construção destas equações, por si só, já pode elucidar muitas questões relativas às falhas e erros humanos ocorridos durante o acidente. Além disso, várias conclusões importantes já podem ser extraídas com o processo de análise executado até esta etapa.

6.2.7. Análise quantitativa

Uma vez com as equações probabilísticas do problema, obtidas na subseção anterior, a sequência da avaliação quantitativa do risco é encontrar o valor numérico da probabilidade de recuperação do sistema, conforme a eq. (36) (poderia utilizar-se

a visão de ocorrência do acidente, conforme a eq. (39)). Para tal, deve-se buscar a melhor técnica para o cálculo de cada termo. Conforme já discutido anteriormente, sugestões de métodos de cálculo foram apresentadas na seção 5.7 (pág. 150), e não será objetivo deste trabalho ilustrar a aplicação de cada método para todos os termos da equação deste estudo de caso. Também como já discutido, o número a ser obtido possui pouco significado, e possui relevância apenas para efeito de comparação ou classificação de cenários.

No entanto, para ilustrar o tipo das conclusões que podem ser extraídas da análise individual de cada termo, será demonstrada a aplicação para dois casos, que envolvem a questão do sistema de alarmes e dos fatores humanos.

O primeiro termo, cujo cálculo será ilustrado, é o termo de interpretação do alarme de sobretemperatura do economizador na fase 3 do acidente. Este termo é bastante dependente dos fatores humanos e organizacionais, e, portanto, este exemplo também pode ser aplicado no cálculo do mesmo termo das demais fases.

O segundo termo a ser calculado, expressa a probabilidade de uma decisão acertada, dada a interpretação de um alarme de pressão baixa, na fase 2 do acidente. Este termo envolve a tomada de decisão sob conflito de interesses, e o método de análise escolhido também pode ser aplicado para o mesmo termo na fase 3.

▪ Exemplo de cálculo do termo $P(I_k|A_1, O_1)$ da fase 3

Conforme narrativa do acidente, o alarme A_1 da fase 3 é o alarme de sobretemperatura no sistema de vapor, interpretado pelo 3º oficial. O perfil do terceiro oficial foi superficialmente descrito no relatório de investigação, mas é reforçada a informação que se tratava de um tripulante novato e inexperiente. Para iniciar a análise probabilística, a Tabela 33 apresenta uma breve descrição acerca do erro humano de interpretação do alarme na fase 3.

A interpretação do alarme está categorizada como sendo uma atividade cujo nível de desempenho é de regras e conhecimento (ver Tabela 20, pág. 140). Por ser fortemente dependente do contexto, escolher-se-á o método CREAM para a estimativa da probabilidade de erro da interpretação. O método CREAM,

apresentado resumidamente na subseção 3.3.4.1, é um dos métodos possíveis para este cálculo, e um dos métodos sugeridos conforme Figura 50 (pág. 154).

Tabela 33 – Análise do erro de interpretação na fase 3

Análise do erro humano
Perfil do operador: inexperiente e com conhecimentos limitados.
Forma do erro: o operador interpreta o alarme de sobretemperatura no economizador como não sendo um problema de circulação de água.
Causas prováveis: pouca experiência, treinamento inadequado do tripulante e falta de conhecimento sobre o economizador.
Consequência: a interpretação errada do alarme levará a uma provável decisão ou ação errônea sobre como corrigir o problema.
Recuperação: o erro de interpretação pode ser recuperado através da intervenção de outro tripulante ou supervisor.
Formas de evitar: a existência de um documento que descreva as possíveis causas do alarme, e ações sugeridas ajuda a evitar que o operador esqueça sobre o motivo da existência de um alarme, principalmente porque os alarmes mais graves tem uma frequência de ocorrência muito baixa. Além de investimentos em treinamento, e filosofia organizacional focada em comunicação e segurança.

Seguindo os três passos do método CREAM, descritos na pág. 101, tem-se:

1. Descrição da tarefa: interpretação de um monitor de alarme, indicando um alarme de sobretemperatura de uma máquina.

2. Avaliação dos CPCs: De acordo com os fatores humanos e organizacionais levantados nas Tabelas 24 a 27, pode-se descrever o contexto, segundo a Tabela 7 (pág. 81). O resultado da descrição do contexto, de acordo com o método CREAM, está apresentado Tabela 34.

3. Determinação do modo de controle: O vetor resultante (Σ_{reduzem} , $\Sigma_{\text{não significativo}}$, Σ_{melhoram}) é igual a (5,3,1). O que resulta em um modo de controle oportunista, conforme gráfico da Figura 61. De acordo com a Tabela 17 (pág. 102), o modulo de controle oportunista implica em uma probabilidade de falha no intervalo entre 0,01 e 0,5. Portanto, o termo da probabilidade de interpretação acertada $P(I_k|A_1, O_1)$ pode ser estimado como pertencendo ao intervalo 0,5 a 0,99.

Tabela 34 – CPCs específicos referentes à fase 3 do acidente

Nome do CPC	Nível	Efeito esperado na confiabilidade do desempenho
Adequação à organização	Ineficiente	Reduz
Condições de trabalho	Compatível	Não significativo
Adequação à MMI e suporte operacional	Tolerável	Não significativo
Procedimentos disponíveis	Inapropriado	Reduz
Número de objetivos simultâneos	De acordo com capacidade	Não significativo
Tempo disponível	Adequado	Melhora
Horário	Noturno	Reduz
Treinamento e experiência	Inadequados	Reduz
Colaboração da equipe	Deficiente	Reduz

Figura 61 – Modo de controle do método CREAM aplicado à fase 3

Caso o intervalo de probabilidade não seja suficiente, o método CREAM estendido pode ser aplicado. Este método não foi descrito no Capítulo 3 por ser mais extenso e complexo.

Cabe aqui citar que a Tabela 34 foi construída a partir dos fatores humanos e organizacionais descritos no relatório de investigação, para ilustrar os passos a serem seguidos por um analista. A classificação dos CPCs pode ser tida como subjetiva, e poderá ser diferente sob os olhos de outros analistas. Desta forma, ressalta-se a importância de um time de analistas qualificados, e da aplicação das

análises de sensibilidades para verificar o grau de variação dos critérios entre os analistas.

▪ **Exemplo de cálculo do termo $P(D_n|I_1, O_1)$ da fase 2**

A decisão em questão na fase 2 do acidente levava em consideração desligar ou não os motores principais da embarcação, após o alarme de baixa pressão de vapor, e a interpretação de que este causava um problema na circulação de água no economizador. A Tabela 35 apresenta a análise do erro humano cometido pelo chefe de máquinas, que foi o responsável na ocasião por tomar a decisão.

A tomada de decisão foi fortemente dependente do contexto, logo o método CREAM também é um método adequado para a estimativa da probabilidade. Poderia ter-se escolhido um método que se trata mais especificamente o fator tempo, como o método HCR (ver subseção 3.3.3.5, pág. 88), mas o método CREAM é mais completo no tratamento dos fatores humanos e organizacionais, e contempla a questão do tempo no CPC “Tempo disponível”. Novamente, seguindo os passos do método CREAM:

1. Descrição da tarefa: tomada de decisão sobre como proceder, frente a um problema de circulação de água no economizador.

Tabela 35 – Análise do erro de interpretação na fase 2

Análise do erro humano
Perfil do operador: experiente, com conhecimentos limitados e com forte problema de liderança e comunicação.
Forma do erro: o operador toma a decisão de não desligar os motores.
Causas prováveis: falta de conhecimento sobre o economizador, propensão ao risco e falta de comprometimento com segurança.
Consequência: manter o motor funcionando implica em um provável aumento de temperatura do economizador.
Recuperação: o erro de decisão pode ser recuperado através da intervenção de um superior, quando informado sobre o problema.
Formas de evitar: a existência de um documento que descreva as possíveis causas do alarme, e ações de recuperação do problema. Além de investimentos em treinamentos técnicos, de emergência, mitigação de consequências, de utilização de normas de segurança, e adoção de uma filosofia organizacional focada na comunicação e segurança.

2. Avaliação dos CPCs: A partir dos fatores humanos e organizacionais levantados nas Tabelas 24 a 27, pode-se descrever o contexto como apresentado na Tabela 36. Percebe-se que no caso do chefe de máquinas, os CPCs são mais favoráveis, uma vez que o chefe de máquinas possuía um treinamento e experiência adequados.

Tabela 36 – CPCs específicos referentes à fase 2 do acidente

Nome do CPC	Nível	Efeito esperado na confiabilidade do desempenho
Adequação à organização	Eficiente	Não significativo
Condições de trabalho	Compatível	Não significativo
Adequação à MMI e suporte operacional	Tolerável	Não significativo
Procedimentos disponíveis	Inapropriado	Reduz
Número de objetivos simultâneos	Menor capacidade	Não significativo
Tempo disponível	Adequado	Melhora
Horário	Noturno	Reduz
Treinamento e experiência	Adequados	Melhora
Colaboração da equipe	Deficiente	Reduz

3. Determinação do modo de controle: O vetor resultante é igual a (3,4,2), resultando em um modo de controle tático, conforme Figura 62. Este modo de controle possui um intervalo de falha entre 0,01 e 0,1 (ver Tabela 17, pág. 102). Logo, a probabilidade de uma decisão acertada se encontra no intervalo entre 0,9 e 0,99.

Figura 62 – Modo de controle do método CREAM aplicado à fase 2

Para a obtenção de um número único da probabilidade estimada de erro humano, o método CREAM estendido também poderia ser aplicado. No entanto, sabe-se que o chefe de máquinas tomou a decisão de continuar a navegação por receio de tomar uma decisão impopular. Uma imprecisão que pode ser citada sobre o método CREAM é que este, através de sua descrição do contexto, possui dificuldades de expressar essa condição de decisão sob conflito, da mesma maneira como qualquer outro método apresentado neste trabalho teria.

6.2.8. Análise das incertezas e análise de sensibilidade

A análise das incertezas e de sensibilidade são passos importantes na análise probabilística de risco, e o analista poderia dar dois tipos de tratamento para ambas neste estudo de caso.

O primeiro tratamento seria analisar as incertezas de cada termo calculado. Por exemplo, pode-se investir tempo na discussão de quais incertezas seriam relevantes em relação à estimativa do termo $P(I_k|A_1, O_1)$ da fase 3, cujo cálculo foi demonstrado na subseção anterior, através do método CREAM. Como já foi discutido, qualquer método que se proponha a modelar a atividade humana possui intrinsecamente incertezas embutidas. As controvérsias destas incertezas são infundáveis, e, neste estágio, sua discussão seria improdutiva (as dificuldades de se modelar a atividade humana foram abordadas no Capítulo 3). Um bom exercício, no entanto, para a análise das incertezas de cada termo é fazer uma análise de sensibilidade. Especificamente para o método CREAM, pode-se variar a descrição do contexto, alterando as classificações de cada CPC.

Por exemplo: caso os “Procedimentos disponíveis” fossem adequados, e o operador fosse experiente, teria-se o vetor resultante ($\Sigma_{reduzem}$, $\Sigma_{n\grave{a}o\ significantivo}$, $\Sigma_{melhoram}$) = (3,3,3), e um modo de controle tático. Neste caso, o intervalo de probabilidade de falha mudaria de 0,01 a 0,5 para 0,01 a 0,1. Portanto, o intervalo da probabilidade de acerto da interpretação mudaria de 0,5 a 0,99 para 0,9 a 0,99.

A conclusão da análise de sensibilidade seria que estes dois fatores organizacionais, treinamento e disponibilidade de procedimentos, são fatores chave para reduzir a probabilidade de erro humano na interação com o sistema de alarmes. E é exatamente este o objetivo da metodologia proposta neste trabalho, ou

seja, proporcionar uma ferramenta que permita aos gestores identificar como direcionar investimentos que melhor influenciem na segurança da embarcação, através da melhoria dos fatores humanos e organizacionais.

Outra abordagem de análise de sensibilidade, ainda focando o tratamento de cada termo da equação de probabilidades, é a abordagem proposta por Filgueiras (1996) descrita na seção 3.4 (pág. 103). A fim de se ilustrar um exemplo de análise de sensibilidade, segundo o processo descrito na seção 3.4, foi construída a Tabela 37, a qual apresenta a matriz com os pesos q_i e notas r_i de cada CPC. A Tabela 37 preenchida de acordo com o julgamento deste autor, a fim de exemplificar a aplicação da técnica pelo analista. Cabe observar novamente que estes valores podem variar segundo a percepção de cada analista.

A análise de sensibilidade, neste exemplo, foi feita escolhendo-se três CPCs, dos quais se deseja analisar a influência por serem considerados os mais relevantes. Neste caso, não se deseja avaliar a influência dos outros CPCs, por exemplo, por serem difíceis de modificar, ou por terem baixo impacto no contexto.

Para a atribuição dos pesos q_i , começa-se escolhendo o CPC de menor relevância, no caso o CPC “Colaboração da equipe”, que recebe o peso 10. Em seguida, os demais CPCs recebem pesos múltiplos de 10. Assim, os CPCs “Procedimentos disponíveis” e “Treinamento e experiência” por terem a mesma importância, recebem o peso 20. Logo, neste exemplo, considera-se que os CPCs com peso 20 são duas vezes mais importantes que o CPC “Colaboração da equipe”.

De acordo com os critérios definidos na seção 3.4, as notas r_i de cada estado foram atribuídas de 0 a 1, se o estado favorece o erro humano, e acima de 1 se o estado compensa o erro humano.

Tabela 37 – Tabela de análise de sensibilidade CPCs da fase 3

Variáveis de contexto	Estados							
	q_i	r_i		r_i		r_i		r_i
Procedimentos disponíveis	20	apropriado	5	aceitável	1	inapropriado	0,5	
Treinamento e experiência	20	muito experiente	8	adequado	2	inadequado	0,2	
Colaboração da equipe	10	muito eficiente	2	eficiente	1	ineficiente	1	deficiente 0,5
Σq_i	50							

A Tabela 38 apresenta o resultado da análise, com as 36 possíveis combinações dos estados dos CPCs. O valor do índice de influência relativa do contexto sobre o cenário (IC), calculado segundo a eq. (15) (pág. 103), é apresentado na última coluna.

Tabela 38 – Resultado da análise de sensibilidade CPCs da fase 3

	Procedimentos disponíveis	Treinamento e experiência	Colaboração da equipe	IC
1	apropriado	muito experiente	muito eficiente	2,56
2	apropriado	muito experiente	eficiente	1,28
3	apropriado	muito experiente	ineficiente	1,28
4	aceitável	muito experiente	ineficiente	1,28
5	apropriado	muito experiente	deficiente	0,64
6	apropriado	adequado	muito eficiente	0,64
7	aceitável	muito experiente	muito eficiente	0,512
8	aceitável	adequado	muito eficiente	0,512
9	apropriado	adequado	eficiente	0,32
10	apropriado	adequado	ineficiente	0,32
11	apropriado	inadequado	muito eficiente	0,256
12	aceitável	muito experiente	eficiente	0,256
13	inapropriado	muito experiente	muito eficiente	0,256
14	inapropriado	adequado	muito eficiente	0,256
15	apropriado	adequado	deficiente	0,16
16	aceitável	muito experiente	deficiente	0,128
17	inapropriado	muito experiente	eficiente	0,128
18	inapropriado	muito experiente	ineficiente	0,128
19	aceitável	adequado	eficiente	0,064
20	aceitável	adequado	ineficiente	0,064
21	inapropriado	muito experiente	deficiente	0,064
22	aceitável	inadequado	muito eficiente	0,0512
23	apropriado	inadequado	eficiente	0,032
24	apropriado	inadequado	ineficiente	0,032
25	aceitável	adequado	deficiente	0,032
26	inapropriado	adequado	eficiente	0,032
27	inapropriado	adequado	ineficiente	0,032
28	inapropriado	inadequado	muito eficiente	0,0256
29	apropriado	inadequado	deficiente	0,016
30	inapropriado	adequado	deficiente	0,016
31	aceitável	inadequado	eficiente	0,0064
32	aceitável	inadequado	ineficiente	0,0064
33	aceitável	inadequado	deficiente	0,0032
34	inapropriado	inadequado	eficiente	0,0032
35	inapropriado	inadequado	ineficiente	0,0032
36	inapropriado	inadequado	deficiente	0,0016

Esta tabela permite ao analista concluir qual cenário influi mais positivamente ou negativamente no contexto. Uma possível conclusão, por exemplo, em um contexto com procedimentos disponíveis apropriados, é melhor investir em treinamento e recrutar tripulantes experientes (cenário 3), a investir em formação de equipes colaborativas (cenário 6).

Além disso, a análise de sensibilidade também ajuda a reduzir a incerteza quanto à classificação dos CPCs. Sabe-se que o critério adotado para cada CPC também sofrerá influência do perfil e da habilidade do analista, e também pode ser desejável mensurar o impacto da variação de critérios entre os especialistas. A análise de sensibilidade, então, poderia ser feita através da qualificação dos CPCs por mais de uma pessoa, e o analista poderia considerar o critério mais votado para cada CPC.

Um segundo tratamento da análise de incertezas seria desprezar as incertezas de cada termo, e considerar uma incerteza global do processo. Neste caso, o primeiro passo seria garantir que a comunicação da incerteza da metodologia seja feita aos tomadores de decisão, ou, em outras palavras, os “clientes” da análise de risco. Deve-se reforçar a ideia de que o número obtido é um valor que deve servir apenas para fins de comparação ou classificação, e não significam uma medida real do risco de um acidente.

A análise de sensibilidade também é uma ferramenta útil, pois pode-se comparar os resultados variando um fator de interesse, e medindo sua influência no valor final da probabilidade das equações (36) ou (39).

Por fim, Paté-Cornell (1996) orienta que a avaliação das incertezas só deve ser tratada quando esta for relevante para os tomadores de decisão, uma vez que a análise de incertezas também consome recursos. Paté-Cornell (1996) sugere alguns caminhos para contornar as incertezas do problema, dependendo do nível de relevância que as incertezas significarem para a tomada de decisão:

- Decidir se a incerteza oferece ou não risco ao sistema.
- Escolher o pior caso.
- Escolher o “quase pior caso”, ou o caso mais plausível.
- Escolher a melhor estimativa ou a média de um intervalo de incerteza.
- Realizar análises mais aprofundadas.

6.2.9. Interpretação dos resultados

Apesar de ter sido demonstrada parte da análise de risco quantitativa do acidente, certamente o número maior de conclusões úteis aos decisores podem ser extraídas nas etapas anteriores, principalmente durante a elaboração da formulação matemática, onde se consegue enxergar relações não óbvias entre os termos. Ademais, a própria modelagem do problema já elucida muitos detalhes e acoplamentos das ações humanas durante a sequência do acidente.

Pode-se afirmar que se trata de um caso típico onde o caminho percorrido é mais importante que o lugar de chegada em si. Em outras palavras, o processo trabalhado até a obtenção da equação geral de probabilidades é mais importante que o valor final que se obteria em seu cálculo.

A interpretação dos resultados obtidos até este ponto permite concluir que:

- Na fase 1 do acidente, além do evento iniciador (falha no sistema automático da caldeira), ocorreu também uma falha no sistema eletrônico para sinalizar um problema ao sistema de alarmes. Ou seja, deveria existir um monitoramento mais confiável de falha no sistema automático da caldeira. Isto teria permitido que a tripulação interviesse no sistema antes da ruptura da fornalha. O alarme de situação anormal no sistema da caldeira já havia sido previsto, conforme apresentado na Tabela 21. Logo, a probabilidade de êxito nas ações humanas de recuperação do sistema, sem a sinalização do alarme de situação anormal na caldeira, foi zero.
- O erro humano, que permitiu o incidente nas fases 2 e 3, se deu no bloco de tomada de decisão. O chefe de máquinas optou por não desligar o motor, para não comprometer o cronograma de saída do porto da embarcação. Um documento relacionando a cada alarme com possíveis ações de recuperação teria ajudado na tomada de decisão correta. Para a prevenção de futuros erros, a gerência deveria investir no comprometimento para com as normas de segurança e promover uma filosofia organizacional orientada à segurança e prevenção de incidentes.
- Ainda na fase 2, a tomada de decisão errada do chefe de máquinas poderia ter sido corrigida pelo comandante da embarcação, caso este

tivesse sido informado de forma precisa sobre o problema na caldeira e no economizador. O problema de comunicação também estava relacionado com o baixo nível de conhecimento do idioma inglês do chefe de máquinas. Políticas mais rigorosas de seleção de pessoal, e estímulo à comunicação interna colaborariam para prevenir futuros problemas semelhantes.

- Na fase 4, o erro humano também se deu no bloco de tomada de decisão, porém devido à falta de conhecimento em relação ao economizador e em relação às técnicas de combate à incêndio.

6.2.10. Opções de controle do risco

Na diretriz da IMO sobre avaliação formal de risco (IMO, 2002a), o passo 3 da metodologia consiste nas “opções de controle de risco”, o qual foi inserido com a função de levar à prática as conclusões da análise de risco, focando nas áreas onde necessita-se de aprimoramentos e identificando possíveis medidas para controle do risco.

O que será de interesse abordar nesse estudo de caso são as opções de controle de risco relacionadas ao sistema de alarmes, seja em relação ao equipamento em si, ou em relação à sua interação com a tripulação. Não serão pensadas outras opções de controle de risco não relacionadas ao sistema de alarmes.

Começando pela parte relativa à interação tripulação-sistema de alarmes, as principais opções de controle de risco seriam:

- Elaboração de um manual indicando possíveis causas e ações para cada alarme presente no sistema de alarmes da embarcação, dividindo essas ações entre oficiais de máquinas e passadiço.
- Desenvolvimento de treinamentos apropriados para a tripulação relacionados às funções de segurança exercidas pelo sistema de alarmes.
- Aprimoramento da cultura de segurança, com o objetivo de engajar a tripulação e promover uma mudança de postura que favoreça a

comunicação interna e o julgamento sobre aceitar ou não determinado risco.

A primeira e segunda opção de controle do risco influenciam diretamente na interpretação dos alarmes, termo $P(I_k|A_j, O_m)$, e nas decisões da tripulação, termo $P(D_n|I_k, O_m)$. Já a terceira opção de controle visa influenciar as tomadas de decisão sob conflito, como a que ocorreu na fase 2 e 3 deste acidente.

Em relação à parte do equipamento do sistema de alarmes, termo $P(A_j|E)$, as opções de controle do risco seriam:

- Implementar repetidores dos alarmes no passadiço, de forma a melhorar a comunicação entre praça de máquinas e comandante, e consequentemente, melhorar o processo de tomada de decisão em situações de emergência
- Realizar investimentos no sistema de alarmes, de forma a aumentar as máquinas monitoradas, ou melhorar a confiabilidade da captura dos alarmes através de instalação de sensores redundantes.

O repetidor no passadiço, sugerido pela primeira opção de controle de risco, teria, possivelmente, impedido que o chefe de máquinas relatasse o incidente ao passadiço de forma imprecisa e tardia. Da mesma maneira, teria permitido ao comandante questionar a opinião do chefe de máquinas sobre continuar a navegação.

A opção de controle de risco que sugere investimentos no sistema de alarmes é uma medida pró-ativa que implementa um monitoramento de alarmes além dos requisitos mínimos exigidos pelas sociedades classificadoras. A implantação de equipamentos de segurança, como o sistema de alarmes, que não só atendem as normas, mas se preocupam em cobrir todas as máquinas relevantes é fundamental, uma vez que as regras das sociedades classificadoras são genéricas, e não cobrem as particularidades de cada embarcação. Neste caso, a análise de risco pró-ativa da embarcação como um todo apontaria os alarmes adicionais recomendáveis a serem adicionados ao sistema.

Estas opções de controle de risco sugeridas complementam o capítulo de “Ações a serem tomadas” do relatório de investigação do acidente da embarcação Maersk Doha, agregando conclusões específicas relativas ao sistema de alarmes, que não poderiam ser obtidas sem uma análise direcionada a este equipamento e aos fatores humanos e organizacionais.

6.2.11. Avaliação custo-benefício

É certo que todas as medidas citadas na subseção anterior possuem um custo de implementação. O passo seguinte ao levantamento das opções de controle de risco é avaliar o custo de cada medida, e seu impacto na redução do risco (benefício). Pode-se, por exemplo, ordenar cada opção de controle de risco de acordo com seu custo estimado de implementação, ou de acordo com o benefício esperado, como a redução da probabilidade de um incidente.

Sem realizar nenhum estudo elaborado, é possível estimar que as medidas de controle do risco podem ser ordenadas, de maneira crescente, de acordo com seu custo de implementação:

- 1) Elaborar manual com ações sugeridas para cada alarme;
- 2) Implementar repetidor no passadiço;
- 3) Investir no sistema de alarmes;
- 4) Desenvolver treinamento à tripulação;
- 5) Aprimorar cultura de segurança.

A medida 1 proporcionaria uma redução na probabilidade de uma interpretação errada de um alarme. A medida 2 melhoraria o processo de tomada de decisão e das ações de recuperação. A análise custo-benefício da medida 3 é extremamente eficaz na fase de projeto e construção de uma embarcação. De acordo com os recursos disponíveis, a análise custo-benefício será uma excelente ferramenta de tomada de decisão para a definição do que pode ser monitorado além dos requisitos mínimos exigidos.

A medida 4 teria um efeito amplo, tanto na probabilidade de ocorrência de um evento iniciador, quanto na questão de interpretação dos alarmes e ações de recuperação.

Finalmente, a medida 5 talvez seja a que possa proporcionar o maior benefício de todas, uma vez que, como discutido na subseção 3.1.4.3 (pág. 72), esta medida irá não somente influenciar a embarcação sob análise, mas toda a frota de um armador. Esta medida teria impacto na descrição do contexto, tendo impacto em praticamente todos os CPCs.

6.2.12.Recomendações para a tomada de decisão e conclusões

A grande finalidade da análise de risco é sempre ser uma fonte de informação para a tomada de decisão. Este trabalho, portanto, auxiliará os decisores a responder as perguntas do capítulo de introdução desta tese (ver seção 1.2, pág. 5) relativas à como o sistema de alarme contribui em reduzir a probabilidade de acidentes em uma embarcação e como direcionar os investimentos em segurança para melhorar a interação entre tripulação e sistema de alarmes. É de suma importância prever investimentos não apenas em equipamentos, mas também em mudanças na organização e nos funcionários de terra e de bordo. Nem sempre será óbvio medir os benefícios dos investimentos na parte organizacional, mas os resultados perdurarão por longo prazo.

Para finalizar, é importante apontar algumas conclusões deste estudo de caso adicionais às conclusões do relatório de investigação do acidente. Essas conclusões, além de serem as respostas das duas perguntas do início da tese, também são uma contribuição verdadeira da aplicação da metodologia proposta à análise do acidente. Logo, após a aplicação da metodologia de análise de risco focada no sistema de alarmes e fatores humanos e organizacionais, as seguintes conclusões podem ser acrescentadas:

1. Deveria existir um monitoramento mais confiável de falha no sistema automático da caldeira, o que teria impedido a ruptura da tubulação (influência na probabilidade de ocorrência do evento iniciador na fase 1).

2. A existência de um repetidor do painel de alarmes no passadiço teria minimizado a falha de comunicação do problema na caldeira ao passadiço, permitido que o comandante questionasse a decisão de manter o motor funcionando (influência no termo $P(D_n|I_k, O_m)$).

3. A alimentação elétrica do sistema de alarmes por um banco de bateria de emergência teria impedido que a memória dos alarmes se apagasse, após o blecaute ocorrido durante o incêndio. Isso teria permitido a investigação mais precisa das causas da falha na caldeira.

4. Apesar do sistema de alarme prever um registro físico dos alarmes, através da impressão em papel, os equipamentos devem ser capazes de manter sua memória mesmo sem estarem alimentados.

5. Sistemas de alarmes mais modernos fazem a contagem de horas de operação das máquinas. Esse tipo de informação teria auxiliado nas rotinas de manutenção da caldeira, considerada como uma das causas do evento iniciador.

6. A revisão dos procedimentos de SMS (*Safety Management System*) e QMS (*Quality Management System*) foi citada como uma das ações tomadas pelos armadores no relatório de investigação. Certamente, estas abrangem procedimentos a serem tomados em situações de emergência. No entanto, a tripulação deve saber, e se possível ter na memória, as possíveis causas e ações sugeridas para cada alarme da embarcação.

7. Investimentos em segurança deveriam priorizar os fatores humanos e organizacionais, uma vez que, apesar do evento iniciador ser uma falha no sistema físico, a qualquer momento, e em todas as 4 fases, este poderia ter sido recuperado pela tripulação, e os erros humanos foram responsáveis pela propagação da falha inicial. Conforme análise de sensibilidade realizada, com as premissas adotadas na subseção 6.2.8, os fatores organizacionais treinamento e disponibilidade de procedimentos são os que mais influenciam a probabilidade de erro humano relacionada aos sistemas de alarmes.

7. CONCLUSÕES

O objetivo principal desta tese era propor uma metodologia de análise de risco para embarcações com sistemas de alarme, considerando tanto o sistema técnico, quanto a questão dos fatores humanos e organizacionais. O modelo de análise, proposto no Capítulo 5 desta tese, foi desenvolvido a partir de uma extensa revisão bibliográfica e de relatórios de análise de acidentes. Buscou-se desenvolver um modelo tão simples quanto possível, mas tão abrangente quanto necessário, a fim de tornar o método aplicável e gerenciável, e ao mesmo tempo, possibilitar capturar os eventos e etapas relevantes durante uma sequência de acidente envolvendo o sistema de alarmes. Trata-se de um cenário de estudo específico, e não genérico, mas certamente pertinente no contexto da indústria naval.

Os objetivos específicos da tese, apresentados no Capítulo 1 como sendo (1) associação das técnicas de análise ao modelo proposto; (2) elaborar uma ferramenta que permita aos gestores identificar e direcionar investimentos que melhor influenciem na segurança; (3) auxiliar e prover subsídio para as respostas das perguntas sobre a contribuição e o projeto do sistema de alarmes; foram atingidos da seguinte forma:

No Capítulo 5, foi demonstrada a elaboração de um modelo que explica a interação da tripulação com o sistema de alarmes, e foi apresentada uma metodologia de análise de risco para, através desse modelo, ser possível mensurar a probabilidade de um acidente ou de recuperação de um evento iniciador, contemplando os fatores humanos e organizacionais. Ao final do Capítulo 5, discutem-se quais técnicas apresentadas nos Capítulos 2 e 3 são mais adequadas para cada termo da equação geral do modelo proposto.

A demonstração da aplicação da metodologia foi feita através do estudo de caso apresentado no Capítulo 6, o qual teve a função de explanar e documentar um exemplo de utilização prática, percorrendo as etapas básicas de uma análise formal de risco. A aplicação da metodologia à análise do acidente com a embarcação Maersk Doha contribuiu para acrescentar novas recomendações às conclusões do relatório de investigação. Estas conclusões são restritas à questão do sistema de

alarmes e sua utilização pela tripulação, mas certamente pertinentes, uma vez que este equipamento teve um papel importante durante a evolução do acidente.

Os resultados do estudo de caso indicam que é possível auxiliar gestores, armadores, e decisores a responder as perguntas da introdução desta tese sobre a contribuição do sistema de alarmes na redução do risco de acidentes, e sobre o projeto de um sistema de alarmes, levando em conta os fatores humanos e organizacionais presentes em um navio. As recomendações para tomada de decisão e conclusões do Capítulo 6 (subseção 6.2.12) confirmam que a análise focada no sistema de alarmes permite aperfeiçoar as exigências sobre segurança, e direcionar investimentos na embarcação, na tripulação e na organização, o que corrobora que a metodologia proposta é viável e funcional, ainda que possa ter limitações.

7.1. Contribuições da metodologia

Os trabalhos de pesquisa sobre a aplicação dos métodos de análise de risco em embarcações são, na maior parte, focados nos sistemas técnicos. Trabalhos dedicados a explorar o tema de fatores organizacionais tem a tendência de prestar pouca atenção na interação do operador com as máquinas. Este trabalho buscou propor uma abordagem onde o operador, a máquina e a organização são conjuntamente considerados.

Acredita-se que o método apresentado aqui, apesar de na forma de uma análise probabilística de risco, possa ser utilizado tanto em análises qualitativas quanto em quantitativas. O cálculo da probabilidade do acidente, ou melhor, a análise quantitativa, deve ser feita sempre quando o número a ser obtido for relevante para o projeto, ou para efeitos de comparação. Sabe-se que, no domínio da confiabilidade humana, os valores probabilidades de falha são objetos de discussão, devido ao alto grau de simplificação do comportamento humano nos métodos utilizados para cálculo.

O argumento de que o aumento do nível de automação se reflete automaticamente no aumento da segurança e confiabilidade é questionável. Por um lado, um sistema totalmente automatizado elimina a necessidade de se modelar o

operador. Por outro lado, sabe-se que dificilmente um sistema complexo possa ser totalmente automatizado. Desta forma, para a aplicação na indústria naval, modelos que contemplem a participação da tripulação interagindo com a automação são altamente desejáveis.

Contudo, a principal contribuição deste trabalho se dá no campo das avaliações de segurança baseadas em risco. Como foi já comentado, existe um grande esforço das sociedades classificadoras para introduzir normas e regras baseadas em risco. Entende-se que num contexto amplo de uma análise de risco de um navio, este trabalho poderia se inserir no capítulo que trata sobre o monitoramento das máquinas e sistemas de alarmes, auxiliando os analistas com conceitos e técnicas específicas para avaliar e aperfeiçoar a segurança das embarcações.

7.2. Observações sobre a aplicação da metodologia

A aplicação da metodologia desenvolvida neste trabalho foi discutida em profundidade no Capítulo 6, onde foi apresentado um estudo de caso e um exemplo de análise de risco. A qualidade final do resultado da aplicação da metodologia proposta, como fonte de informação para os decisores, dependerá certamente da habilidade do analista e dos recursos disponíveis. Nas mãos de um analista habilidoso com informações e recursos adequados, certamente produzirá novas perspectivas para o aumento da segurança de uma embarcação.

O principal desafio se dará na dificuldade de coleta de dados, sejam eles dados estatísticos de falhas, ou erros humanos, sejam eles para se modelar o contexto e determinar os Fatores de Condicionamento do Desempenho. Além disso, é fundamental buscar determinar o nível mínimo de complexidade do cenário em análise, a fim de atingir a quantidade necessária de informações que permita a tomada de decisão. Viu-se que um cenário modelado com muitos detalhes, pode implicar uma análise que exija mais recursos e dados que o disponível.

Outro desafio se dá no campo do cálculo da confiabilidade humana. Como demonstrado durante o estudo de caso apresentado no Capítulo 6, as técnicas para estimativa da confiabilidade humana não se baseiam em dados muito precisos, e

seus resultados são extremamente dependentes da capacidade do analista em identificar os tipos de erros possíveis e encontrar na bibliografia dados semelhantes ou métodos adequados para estimação quantitativa.

Para o analista que fará a aplicação da metodologia, é importante ter ciência e buscar contornar as limitações intrínsecas da metodologia, dentre elas:

- As incertezas do modelo de comportamento humano proposto, devido à sua simplificação em relação às atividades humanas.
- Necessidade de modelar sistemas complexos, uma vez que na maioria dos casos, desejar-se-á aplicar a metodologia para analisar o risco de sistemas complexos, os quais são modelados simplificadamente para tornar viável a análise.
- Incertezas das técnicas de análise de confiabilidade humana, conforme discutido no Capítulo 3.

7.3. Desenvolvimentos futuros

A pesquisa realizada para elaborar esta tese abre perspectivas de continuidade, que podem complementar ou estender o modelo aqui proposto. Um dos campos que se abre para desenvolvimentos futuros é o da adaptação do modelo para outros sistemas de bordo que exijam interação com o elemento humano, e, portanto, dependente de fatores organizacionais. As máquinas mais modernas, como motores e geradores, já são fornecidos com seus sistemas de diagnóstico e alarmes dedicados. A mesma metodologia poderia ser aplicada, por exemplo, para identificar possíveis medidas para se aumentar a segurança na operação da eletrônica de operação de motores.

Outro campo que poderia ter como ponto de partida este trabalho é a análise das interfaces homem-máquina em embarcações, levando em conta a questão de fatores humanos e ergonomia a bordo.

O tema tomada de decisão também poderia ser considerado uma direção para novos desenvolvimentos. Viu-se na subseção 6.2.7 (pág. 190) que as técnicas apresentadas neste trabalho, para modelagem das decisões da tripulação, pouco abordam questões sobre decisões com múltiplos objetivos, decisões sob conflitos,

decisões em situações de incerteza, entre outras. O modelo poderia ser certamente enriquecido com modelos de decisão, não somente para as decisões tomadas a bordo, mas também para as decisões tomadas pelos gestores em relação às medidas a serem adotadas de controle de risco ou investimentos em segurança.

Este trabalho também poderia servir como subsídio para a análise de risco da aplicação de sistemas inteligentes que não só sinalizam os alarmes, mas também possuem inteligência para tomar decisões e atuar nas máquinas (abrindo ou fechando uma válvula, ou desligando um motor). Devido ao alto grau de confiabilidade exigido, este tipo de automação nem é cogitado em algumas embarcações. O modelo apresentado aqui contribuiria para aperfeiçoar o desenvolvimento destes sistemas focando nos fatores humanos e organizacionais pertinentes.

Por fim, as dificuldades apontadas na seção anterior também podem gerar trabalhos futuros, como o aperfeiçoamento ou criação de novos modelos de comportamento humano, ou novas técnicas de análise confiabilidade humana.

7.4. Considerações finais

Muitas normas e regras, hoje exigidas pelas sociedades classificadoras da indústria naval e offshore, foram criadas após algum acidente ou catástrofe, sob forte pressão da sociedade. A avaliação de risco, na grande parte dos casos, é aplicada nas fases finais de projeto com o objetivo de verificar e validar os resultados obtidos. Desta forma, algumas deficiências serão descobertas apenas após algum acidente acontecer. A aplicação da avaliação de risco nos estágios iniciais do projeto pode ter grande impacto na prevenção de acidentes, se todas as fases de projeto forem realizadas com foco na segurança.

A prevenção de acidentes marítimos, como apresentado neste trabalho, requer tanto avanços e melhorias técnicas como organizacionais. O modelo proposto cumpre seu objetivo de ter uma aplicação suficientemente simples e de contemplar as variáveis importantes para a análise. Sua inovação está em contemplar como fator chave a interação homem-máquina, ou melhor, tripulação-

monitor de alarmes. Claramente, como qualquer modelo de análise de risco, existem limitações. Neste caso, as limitações residem principalmente na simplificação dos modelos de comportamento humano e influência dos fatores organizacionais. Todavia, qualquer método que descarte estes fatores oferecerá uma precisão irreal ao analista.

A metodologia não deve ser encarada como um modelo genérico para o cálculo da probabilidade de ocorrência de um acidente. Mas sim, provê sua contribuição na resposta de perguntas muito mais relevantes a projetistas e decisores, como: “Qual a contribuição do sistema de alarmes na redução do risco?”, ou “ Como melhorar o projeto de um sistema de alarmes considerando os fatores humanos e organizacionais?”.

Por fim, é deveras importante a utilização destas ferramentas de análise de forma pró-ativa, buscando evitar novos acidentes, antecipando-se a falhas futuras, não previstas no projeto da embarcação ou não contempladas nas diretrizes de segurança do navio.

REFERÊNCIAS

ABNT ISO/IEC. **Guia 73 - Gestão de riscos - Vocabulário - recomendações para uso em normas**. ABNT ISO/IEC. Rio de Janeiro, p. 11. 2005. (ABNT ISO/IEC GUIA 73:2005).

ABS. **Guidance Notes on Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries**. American Bureau of Shipping (ABS). EUA. 2000.

ABS. **Guidance notes for the application of ergonomics to marine systems**. American Bureau of Shipping. Houston. 2003a.

ABS. **Guidance on ergonomic design of navigation bridges**. American Bureau of Shipping. Houston. 2003b.

ABS. **Automatic or remote control for machinery and systems (other than propulsion) on offshore installation**. American Bureau of Shipping. EUA. 2008a.

ABS. **Guide for automatic or remote control and monitoring for machinery and system (other than propulsion) on offshore installations**. American Bureau of Shipping. Houston. 2008b.

ALERT! Just waiting to happen. The work of UK P&I Club. **ALERT! The International Maritime Human Element Bulletin**, Inglaterra, n. 1, p. 3, 2003.

ATSB. Australian Transport Safety Bureau. **Transport Safety Investigations and Reports**, 2010. Disponível em: <<http://www.atsb.gov.au/publications/safety-investigation-reports.aspx?s=1&mode=Marine>>. Acesso em: 11 Julho 2010.

AVEN, T.; HAUGE, S.; VINNEM, J. E. Methodology for Incorporating Human and Organizational Factors in Risk Analysis for Offshore Installations. **International Journal of Materials & Structural Reliability**, v. 4, n. 1, p. 1-14, Março 2006.

AYYUB, B. M. **A Practical Guide on Conducting Expert-Opinion Elicitation of Probabilities and Consequences for Corps Facilities**. U.S. Army Corps of Engineers Institute for Water Resources. Alexandria-VA. 2001.

AYYUB, B. M. **Elicitation of Expert Opinions for Uncertainty Risk Analysis**. Boca Raton: CRC Press, 2001.

AYYUB, B. M. **Risk analysis in engineering and economics**. ilustrada. ed. EUA: Chapman & Hall / CRC, 2003.

BIRD, F. E.; GERMAIN, G. L. **Practical Loss Control of Leadership**. Loganville, GA: International Loss Control Institute, 1992.

BV. **Rules for the Classification of Steel Ships**. Bureau Veritas. Neuilly-sur-Seine - France. 2005.

CARD, S. K.; MORAN, T. P.; NEWELL, A. **The psychology of human-computer interaction**. Hillsdale: Lawrence Erlbaum Associates, 1983.

CEBI, S. et al. An expert system towards solving ship auxiliary machinery troubleshooting - SHIPAMT. **Expert Systems with Applications**, v. 36, p. 7219-7227, 2009.

CELIK, M.; CEBI, S. Analytical HFACS for investigating human errors in shipping accidents. **Accident Analysis and Prevention**, v. 41, p. 66-75, 2009.

CELIK, M.; LAVASANI, S. M.; WANG, J. A risk-based modelling approach to enhance shipping accident investigation. **Safety Science**, v. 48, n. 1, p. 18-27, Janeiro 2010.

CLOAREC, J.-M. How Dependability Studies Contribute to Controlling Risks. **IEEE**, Brest, v. 1, p. I/560-I/564, 13-16 Setembro 1994. ISSN 0-7803-2056-5.

COMPERATORE, C. A.; RIVERA, P. K. **Crew Endurance Management Practices – A Guide for Maritime Operations**. United States Coast Guard. Washington. 2003.

COOPER, S. E.; RAMEY-SMITH, A. M.; WREATHALL, J. **A Technique for Human Error Analysis (ATHEANA)**. US Nuclear Regulatory Commission. Washington. 1996. (NUREG/CR-6350).

DIAS, A. et al. **A framework for application of probabilistic risk analysis techniques**. 19th Congress of Mechanical Engineering. Brasília: ABCM. 2007a.

DIAS, A. et al. **Análise de risco - uma síntese dos setores marítimo, aéreo e nuclear**. Congresso Íbero-americano de Engenharia Naval - COPINAVAL 2007. 2007: IPIN. 2007b.

DOUGHERTY, E. M. J. Human reliability analysis - where shouldst thou turn? **Reliability Engineering & System Safety**, v. 29(3), p. 283-299, 1990.

DOUGHERTY, E. M.; FRAGOLA, J. R. **Human reliability analysis - a system engineering approach with nuclear power plant applications**. Nova Iorque: John Wiley & Sons, 1988.

DUNN, D. G.; SANDS, N. P. **Alarm Systems management and Design Guide**. ISA Expo 2005. Chicago: ISA. 2005.

EEMUA. **Alarm Systems - a guide to design, management and procurement.** Engineering Equipment and Materials Users Association. Londres. 1999. (EEMUA 191).

EMBREY, D. E. et al. **SLIM-MAUD: An approach to assessing human error probabilities using structured expert judgement.** United States Nuclear Regulatory Commission. Washington. 1984. (NUREG/CR-3518).

ERICSON, C. A. **Hazard Analysis Techniques for system Safety.** Hoboken, NJ: John Wiley & Sons, 2005.

FILGUEIRAS, L. V. L. **APIS: Método para análise e projeto de interfaces homem-computador visando confiabilidade humana.** Escola Politécnica da Universidade de São Paulo. São Paulo. 1996.

FORESTER, J. et al. **ATHEANA User's Guide.** U.S. Nuclear Regulatory Commission. Washington. 2007. (NUREG-1880).

FREITAS, Â. D. F. S.; VENÂNCIO, E. D. S. S.; ARRUDA, R. **Fator Humano & SMS.** Rio Oil & Gás Expo and Conference. Rio de Janeiro: [s.n.]. 2006.

FUJITA, Y.; HOLLNAGEL, E. Failures without errors - quantification of context in HRA. **Reliability Engineering and System Safety**, v. 83, p. 145–151, 2004.

GALÁN, S. F.; MOSLEH, A.; IZQUIERDO, J. M. Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models. **Reliability Engineering & System Safety**, n. 92, p. 1131-1138, 2007.

GL. **GL - Type Approval SOFTWARE - Requirement class 3.** Germanischer Lloyd. Hamburgo. 1996. (SW-E-AK3).

GOMES, E. D. B. F.; BORELLI, F.; NAZARÉ, J. D. C. Teoria Sócio-Técnica - resgatando o construto à luz da criticidade. **REGES - Revista Eletrônica de Gestão, Picos**, v. 2, n. 2, p. 44-55, maio/agosto 2009.

GUIMARÃES, L. D. S. **Gerenciamento de risco e segurança de sistemas.** Rio de Janeiro: ABDAN, 2003.

HANNAMAN, G. W.; SPURGIN, A. J.; LUKIC, Y. D. **Human Cognitive Reliability Model for PRA Analysis.** Electric Power Research Institute. Palo Alto, California, USA. 1984. (NUS-4531).

HETHERINGTON, C.; FLIN, R.; MEARNES, K. Safety in shipping: the human element. **Journal of Safety Research** 37, 2006. 401-411.

HOLLNAGEL, E. **Human Reliability Analysis - Context and Control**. Londres: Academic Press Limited, 1993a.

HOLLNAGEL, E. **Cognitive Reliability and Error Analysis Method**. 1a Edição. ed. Nova Iorque: Elsevier, 1998.

HOLLNAGEL, E.; KAARSATD, M.; LEE, H.-C. Error mode prediction. **Ergonomics**, Loughborough, v. 42, n. 11, p. 1457-1471, 1999.

HOLLNAGEL, E.; WOODS, D. D. Cognitive Systems Engineering - New wine in new bottles. **International Journal of Man-Machine Studies**, v. 18, p. 583-600, 1983.

HOLLNAGEL, E. The phenotype of erroneous actions. **International Journal of Man-Machine Studies**, v. 39, n. 1, p. 1-32, Julho 1993b.

HSE. **Reducing Risks, Protecting People - discussion document**. UK Health and Safety Executive. Londres, p. 81. 1999.

IMO. **Code of alarms and indicators**. International Maritime Organisation. Londres. 1991. (Resolutions A.686(17)).

IMO. International Safety Management (ISM) Code 2002. **Site da IMO**, 2002. Disponível em: <http://www.imo.org/HumanElement/mainframe.asp?topic_id=287>. Acesso em: 07 junho 2010.

IMO. **Guidelines for Formal Safety Assessment for use in the IMO rule-making process**. International Maritime Organization. Londres. 2002a.

IMO. **Guidelines on fatigue**. 1a Edição. ed. Londres: International Maritime Organization, 2002b.

IMO. **Safer shipping demands a Safety Culture**. International Maritime Organization. Londres. 2002c.

IMO. **Issues to be considered when introducing new technology on board ship**. International Maritime Organization. Londres. 2003.

IMO. **International Convention of Safety of Life at Sea – SOLAS**. Consolidated Edition. ed. Londres: International Maritime Organization, 2004.

IMO. **International Convention for the Prevention of Pollution from Ships**. Consolidated Edition. ed. Londres: International Maritime Organization, 2006.

IMO. **International shipping and world trade - facts and figures**. International Maritime Organization. Londres. 2006.

IMO. **Revision of the performance standards for INS and IBS**. International Maritime organization. Londres. 2007. (NAV 53/INF.5).

IMO. About IMO. **International Maritime Organization**, 2010. Disponível em: <http://www.imo.org/About/mainframe.asp?topic_id=3>. Acesso em: 13 junho 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Nuclear Instrumentation - Design For Control Rooms Of Nuclear Power Plants**. International Electrotechnical Commission. [S.I.]. 1989. (IEC-964).

ISO. **Guide 51: Safety Aspects - Guidelines for their inclusion in standards**. ISO/IEC. Geneva, p. 10. 1999. (ISO/IEC GUIDE 51:1999(E)).

ISO. **Ship's bridge layout and associated equipment — Requirements and guidelines**. International Organization for Standardization. Geneva. 2006. (ISO/FDIS 8468).

JENKINSON, J. Alarm reduction in nuclear power plants - results of an international survey. **IEE - The Institute of Electrical Engineers**, Londres, 1997.

KAUER, R. et al. Risk Acceptance Criteria and Regulatory Aspects. **OMMI: Operation Maintenance and Material Issues**, Surrey, Dezembro 2002.

KOENE, J.; VEDAM, H. Alarm management and rationalization. **Third International Conference on Loss Prevention**, 2000.

KONTOVAS, K. A.; PSARAFTIS, H. N. Formal Safety Assessment - A Critical Review. **Marine Technology**, v. 46, n. 1, p. 45-59, Janeiro 2009.

KRISTIANSEN, S. **Maritime Transportation Safety Management and Risk Analysis**. 1a. Edição. ed. Oxford: Elsevier, 2005.

KUMAMOTO, H.; HENLEY, E. J. **Probabilistic Risk Assessment and Management for Engineers and Scientists**. 2a. Edição. ed. Nova Iorque: IEEE Press, 1996.

LEVESON, N. A New Accident Model for Engineering Safer Systems. **Safety Science**, v. 42, n. 4, p. 237-270, Abril 2004.

LUNDBERG, J.; ROLLENHAGEN, C.; HOLLNAGEL, E. What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals. **Safety Science**, v. 47, n. 10, p. 1297-1311, Dezembro 2009.

MAIB. **Annual Report 1999**. Marine Accident Investigation Branch. Londres. 2000.

MAIB. **Report on the investigation of the machinery breakdown and subsequent fire onboard - Maersk Doha**. Marine Accident Investigation Branch. Southampton. 2007. (Report No 15/2007).

MAIB. Marine Accident Investigation Branch. **Publications**, 2010. Disponível em: <<http://www.maib.gov.uk/publications/index.cfm>>. Acesso em: 11 Julho 2010.

MARINHA DO BRASIL. **Normas da autoridade marítima para embarcações empregadas na navegação de mar aberto**. Marinha do Brasil - Diretoria de Portos e Costas. Rio de Janeiro. 2005. (NORMAN 01/DPC).

MATURANA, M. C.; MARTINS, M. R. **Análise da contribuição da falha humana em acidentes de colisão**. 22º Congresso Nacional de Transporte Aquaviário, Construção Naval e Offshore. Rio de Janeiro: [s.n.]. 2008.

MCCORMICK, N. J. **Reliability and risk analysis - methods and nuclear power applications**. Nova Iorque: Academic Press, 1981.

MOREL, G.; CHAUVIN, C. A socio-technical approach of risk management applied to collisions involving Wshing vessels. **Safety Science**, n. 44, p. 599-619, 2006.

MOSLEH, A.; DIAS, A. **Towards an Integrated Methodology for Identification, Classification, and Assessment of Aviation Systems Hazards**. Center for Technology Risk-Studies – University of Maryland. Maryland. 2004.

MURPHY, D. M.; PATÉ-CORNELL, M. E. The SAM Framework: Modeling Effects of Management Factors on Human Behaviour in Risk Analysis. **Risk Analysis**, vol. 16, no. 4, Março 1996. p. 501-515.

MURPHY, E. D.; MITCHELL, C. M. Cognitive attributes: implications for display design in supervisory control systems. **International Journal Man-Machine Studies**, v. 25, p. 411-438, 1986.

NASA. **Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practioners**. National Aeronautics and Space Administration (NASA). Washington. 2002.

NUREG. **Fault Tree Handbook**. U.S. Nuclear Regulatory Commission. Washington. 1981a. (NUREG-0492).

NUREG. **Guidelines for control room design reviews**. Nuclear Regulatory Commission. Washington. 1981b. (NUREG-0700).

PATÉ-CORNELL, M. E. Uncertainties in risk analysis - Six levels of treatment. **Reliability Engineering and System Safety**, Northern Ireland, v. 54, p. 95-111, 1996.

PATÉ-CORNELL, M. E. Finding and Fixing System Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis. **Risk Analysis**, v. 22, n. 2, p. 319-334, 2002.

PATÉ-CORNELL, M. E.; DILLON, R. L. The respective roles of risk and decision analyses in decision support. **Decision Analysis**, v. 3, n. 4, p. 220-232, Dezembro 2006.

RASMUSSEN, J. Skills, rules, knowledge; signals, signs, symbols and other distinctions in human performance models. **IEEE Transactions: Systems, Man & Cybernetics**, v. 13, n. 3, p. 257-266, Maio 1983.

REASON, J. Modelling the Basic Error Tendencies of Human Operators. **Reliability Engineering and System Safety**, v. 22, p. 137-153, 1988.

REASON, J. **Human Error**. Cambridge: Cambridge University Press, 1990a.

REASON, J. The age of the organizational accident. **Nuclear Engineering International**, Julho 1990b. 18-19.

REASON, J. **Managing the Risks of Organizational Accidents**. Inglaterra: Ashgate Publishing Limited, 1997.

REASON, J.; HOLLNAGEL, E.; PARIES, J. **Revisiting the Swiss Cheese Model of Accidents**. EUROCONTROL Experimental Centre. Brétigny-sur-Orge Cedex. 2006.

REN, J. et al. A methodology to model causal relationships on offshore safety assessment focusing on human and organisational factors. **Journal of Safety Research**, v. 39, p. 87-100, 2008.

REVISTA VEJA. **Revista Veja**, n. 2253, p. 73-76, Janeiro 2012.

ROPOHL, G. Philosophy of socio-technical systems. **Society for Philosophy and Technology**, Virginia, v. 4, n. 3, 1999.

ROTHBLUM, A. M. **Human Error and Marine Safety**. National Safety Council Congress and Expo. EUA: [s.n.]. 2000.

SAE. **Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment**. Society of Automotive Engineers. Warrendale. 1996. (ARP4761).

SCHÖNBECK, M. **Human and Organizational Factors in the operational phase of safety instrumented systems: a new approach**. dissertação (Mestrado) - Eindhoven University of Technology. Eindhoven. 2007.

SHERIDAN, T. B. **Humans and Automation: System Design and Research Issues**. Santa Monica: John Willey & Sons, Inc. Publication, 2002.

SHERIDAN, T.; HENNESSY, R. **Research and modeling of supervisory control behavior**. National Academy Press. Washington. 1984.

SHIMIZO, T. **Decisão nas organizações**. 2. ed. São Paulo: Atlas, 2002.

SII, H. S.; WANG, J.; ELEYE-DATUBO, A. G. Safety Assessment of FPSO Turret-Mooring System Using Approximate Reasoning and Evidential Reasoning. **Marine Technology**, v. 42, n. 2, p. 88-102, Abril 2005.

SKJONG, R. **Risk Acceptance Criteria - current proposals and IMO Position**. Surface transport technologies for sustainable development. Valência: [s.n.]. 2002.

SQUIRE, D. **The Human Element in shipping**. Alert! – The International Maritime Human Element Bulletin. Londres. 2005.

SSRC. **Design for safety - an integrated approach to safe european Ro-Ro ferry design**. Ship Stability Research Center - University of Strathclyde. Reino Unido. 2003.

SWAIN, A. D.; GUTTMANN, H. E. **Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application**. United States Nuclear Regulatory Commission. Washington. 1983. (NUREG/CR-1278).

TRIST, E. L.; EMERY, F. E. Socio-technical Systems. **Management Sciences Models and Techniques**, Londres, v. 2, 1960.

UKMS. **The Merchant Shipping (Accident Reporting and Investigation) Regulations 2005**. The United Kingdom Merchant Shipping. Londres. 2005. (2005 No. 881).

USCG. **Risk-Based Decision Making Guidelines (Vol. 1-3)**. US Coast Guard Research and Development Center. Washington, DC. 1997.

USCG. United States Coast Guard. **USCG Office of Investigations & Analysis**, 2010. Disponível em: <<http://www.uscg.mil/hq/cg5/cg545.asp>>. Acesso em: 11 Julho 2010.

WAKEFIELD, D. J. Application of the human cognitive reliability model and confusion matrix approach in a probabilistic risk assessment. **Reliability Engineering and System Safety**, v. 22, p. 295-312, 1988.

WANG, J. Maritime Risk Assessment and its Current Status. **Quality and Reliability Engineering International**, v. 22, p. 3-19, 2006.

WANG, J. et al. Use of advances in technology for maritime risk assessment. **Risk Analysis**, v. 24, n. 4, p. 1011-1033, 2004.

WARD, E.; MILES, R. F.; WINTERFELDT, D. V. **Advances in Decision Analysis**. EUA: Cambridge University Press, 2007.

WEISZFLOG, W. **Michaelis Moderno Dicionário Da Língua Portuguesa**. 1a Edição. ed. São Paulo: Melhoramentos, 1998.

WOODS, D. D.; HOLLNAGEL, E.; LEVESON, N. **Resilience Engineering - Concepts and Precepts**. Hampshire: Ashgate Publishing Limited, 2006.

WU, C.; CONTI, M. B. **Colisão entre embarcações e encalhe em águas restritas - modelo para estimativa da probabilidade de ocorrência**. XX Copinaval. São Paulo: [s.n.]. 2007.