MARCOS COITINHO

PADRÕES BASEADOS EM METAS: UMA ABORDAGEM QUANTITATIVA
APLICADA À EMISSÃO DE GASES POR VEÍCULOS MARÍTIMOS E
AUTOMOTIVOS

SÃO PAULO

2012

MARCOS COITINHO

PADRÕES BASEADOS EM METAS: UMA ABORDAGEM QUANTITATIVA
APLICADA À EMISSÃO DE GASES POR VEÍCULOS MARÍTIMOS E
AUTOMOTIVOS

Tese apresentada à Escola Politécnica da
Universidade de São Paulo para a obtenção
do título de Doutor em Engenharia

Área de concentração:
Engenharia Marítima e Oceânica

Orientador: Professor Mardel B. de Conti

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, de março de 2012.

Assinatura do autor _____

Assinatura do orientador _____

Coitinho, Marcos

**Padrões baseados em metas: uma abordagem quantitativa aplicada à emissão de gases por veículos marítimos e automotivos / M. Coitinho. -- ed.rev. -- São Paulo, 2012.
147 p.**

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

1. Gases (Emissão) 2. Embarcações (Aspectos ambientais; Análise quantitativa) 3. Veículos automotores (Aspectos ambientais; Análise quantitativa) I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Naval e Oceânica II. t.

DEDICATÓRIA

Dedico este trabalho à minha esposa Ana Letícia e à minha filha Mariana, que, através de seu carinho, apoio e compreensão, me fizeram sentir que era possível realizar esta jornada.

AGRADECIMENTOS

Ao professor Mardel B. de Conti, pela orientação, e pelo constante estímulo transmitido durante o desenvolvimento do trabalho.

Aos meus pais Oswaldo e Rosa e aos meus irmãos Marcelo e Magali, pelo apoio e compreensão.

A todos aqueles colegas da Universidade de São Paulo entre professores, alunos e funcionários, que de forma direta ou indireta me assistiram sempre com muita boa vontade.

“Mede o que é mensurável, e torna mensurável o que não o é.”

(Galileu Galilei)

RESUMO

Este trabalho propõe um método com base no planejamento estatístico de testes de confiabilidade para proporcionar um tratamento quantitativo aos dois primeiros níveis da abordagem de padrões baseados em metas (*Goal-Based Standards*). O uso do método é demonstrado em dois exemplos práticos, através da sua aplicação na meta de confiabilidade dos componentes do sistema de pós-tratamento de gases de exaustão, em motores a diesel de veículos automotivos e marítimos.

Os fundamentos do trabalho incluem a teoria do planejamento estatístico de testes de confiabilidade, os princípios do GBS, tipos e características de metas de confiabilidade, a ferramenta de avaliação de segurança formal (FSA), e da análise do modo e efeito da falha (FMEA).

A originalidade da contribuição do trabalho está na combinação das técnicas de planejamento de testes de confiabilidade com os princípios do GBS para quantificar o nível de atendimento das metas de confiabilidade. Dessa forma, é possível ajustar o programa de testes na verificação das metas de segurança, aumentando o conhecimento sobre o desempenho do sistema. O método é de simples aplicação permitindo a sua aplicação expedita e integrada aos processos de desenvolvimento de sistemas.

Palavras-chave: Padrões Baseados em Metas (GBS), Engenharia da Confiabilidade, Planejamento Estatístico de Testes, Redução Catalítica Seletiva (SCR), Veículos Automotivos e Marítimos.

ABSTRACT

This research proposes a probabilistic method based on reliability test planning in order to provide a quantitative approach to the Tier I and II of the Goal-Based Standards (GBS). The use of the method is exhibited through its application in the reliability goal of the components of the exhaust gases post-treatment system in diesel engines for automotive and marine vehicles.

The fundamentals of this work includes the theory of statistical design of reliability tests, the GBS principles, a brief description of the types and characteristics of reliability goals, the tool of Formal Safety Assessment (FSA) recommended for maritime projects, and the risk qualitative methodology based on Failure Mode Effect Analysis (FMEA). This theoretical framework was applied to two practical examples, one in the automotive industry and the other in the shipbuilding sector.

The originality of this research lies in the combination of the reliability test planning techniques with the principles of GBS, in order to verify, from the whole project tests planning, the reliability goals of the basic components as a fundamental step in the assessment of system safety. The testing program can be adjusted to focus on verifying the safety goals, so that the level of knowledge about the product performance before it is delivered to the client. This work also offers the benefit of providing an easy method of system safety assessment, which allows a large number of companies to use it and to integrate it into their product development process.

Keywords: Goal-Based Standards (GBS), Reliability Engineering, Planning Statistical Tests, Selective Catalytic Reduction (SCR).Automotive and Ships vehicles.

LISTA DE FIGURAS

FIGURA 1-1 TIPO DE ABORDAGEM DE SEGURANÇA PARA ATENDIMENTO DAS DEMANDAS DA SOCIEDADE	18
FIGURA 1-2- PROCESSO DE TRANSFORMAÇÃO DAS DEMANDAS DA SOCIEDADE EM REQUISITOS DE SEGURANÇA ATRAVÉS DA INTEGRAÇÃO DAS ABORDAGENS GBS E DE RISCO	20
FIGURA 1-3- COMPARATIVO ENTRE AS ABORDAGENS DE RISCO.....	23
FIGURA 1-4- PRINCIPAIS DEFICIÊNCIAS FSA E FMEA.....	27
FIGURA 2-1-DIAGRAMA FN.....	34
FIGURA 2-2-ÁRVORE DE FALHA E DE EVENTOS GENÉRICA.....	37
FIGURA 2-3- CURVA DE CONFIABILIDADE DURANTE O PROJETO	38
FIGURA 2-4- ESTRUTURA GBS	42
FIGURA 2-5- PROCESSO DE GARANTIA DA CONFIABILIDADE.....	54
FIGURA 2-6- ESTRATÉGIAS DE TESTE PARA OS EXEMPLOS PRÁTICOS	63
FIGURA 3-1- MODELO DE ABORDAGEM PROBABILÍSTICA PARA O GBS.....	66
FIGURA 3-2-SISTEMÁTICA DE DESDOBRAMENTO DAS METAS DE SEGURANÇA	69
FIGURA 4-1-REDUÇÃO DE EMISSÃO DE POLUENTES [g/kWh] POR NORMAS EURO.	72
FIGURA 4-2-SELEÇÃO DO EVENTO INDESEJADO.....	73
FIGURA 4-3-CONFIGURAÇÃO BÁSICA DE UM SISTEMA SCR.....	74
FIGURA 4-4- PROCESSO DE CONVERSÃO CATALÍTICA	75
FIGURA 4-5-REATOR CATALÍTICO PARA APLICAÇÃO SCR	75
FIGURA 4-6-INCIDÊNCIA DE FALHAS DO DOSADOR NO PERÍODO DE 2006 A 2008	78
FIGURA 4-7- FALHAS POR FAIXA DE QUILOMETRAGEM	79
FIGURA 4-8-ÁRVORE DE FALHAS PARA O SISTEMA SCR	81
FIGURA 4-9-PAPEL DE PROBABILIDADE DE <i>WEIBULL</i> PARA O DOSADOR.....	87
FIGURA 4-10-EVOLUÇÃO DA TAXA DE FALHA AO LONGO DO PROJETO	89
FIGURA 4-11-REDUÇÃO DA QUOTA DE FALHA APÓS AUMENTO DO ESFORÇO DE TESTES	91
FIGURA 4-12- COMPARATIVO ENTRE A META DE QUOTA DE FALHA E OS CENÁRIOS 1 E 2.....	92
FIGURA 4-13-CRONOGRAMA DOS TESTES PARA O DOSADOR	94
FIGURA 4-14-CURVA DE RISCO PARA O DOSADOR.....	95
FIGURA 4-15-COMPARATIVO DO RESULTADO DA APLICAÇÃO DAS TÉCNICAS	96

FIGURA 4-16-CRONOGRAMA DE IMPLEMENTAÇÃO DOS LIMITES DE NO _x	100
FIGURA 4-17-CRONOGRAMA DE IMPLEMENTAÇÃO DOS LIMITES DE EMISSÃO DE SO _x	100
FIGURA 4-18-NO _x E CONSUMO DE COMBUSTÍVEL PARA VÁRIAS TECNOLOGIAS	103
FIGURA 4-19-LAYOUT TÍPICO DE UM SISTEMA SCR EM UMA APLICAÇÃO MARÍTIMA	104
FIGURA 4-20-ÁRVORE DE FALHAS PARA O SISTEMA SCR	106
FIGURA 4-21-COMPORTAMENTO DA QUOTA DE FALHA DURANTE O PERÍODO DE TESTES	113
FIGURA 4-22-COMPORTAMENTO DA QUOTA DA TAXA DE FALHA DURANTE O PROJETO	115
FIGURA 4-23-COMPARATIVO ENTRE A META DE QUOTA DE FALHA E OS CENÁRIOS 1 E 2	116

LISTA DE TABELAS

TABELA 2-1-FREQÜÊNCIA DE VÍTIMAS POR TIPO ACIDENTES ENTRE 1997 E 2008	40
TABELA 2-2-CRITÉRIOS DO FMEA PARA O CÁLCULO DO NPR	46
TABELA 4-1- POLUIÇÃO ATMOSFÉRICA NO MUNDO [$\mu\text{g} / \text{M}^3$]	70
TABELA 4-2-PRINCIPAIS MODOS DE FALHAS DO DOSADOR	80
TABELA 4-3-PARÂMETROS DOS TESTES DE PLANEJAMENTO ESTATÍSTICO	83
TABELA 4-4-FALHAS E SUSPENSÕES POR FAIXA DE QUILOMETRAGEM.....	85
TABELA 4-5- VALORES CONSOLIDADOS PARA O CÁLCULO DA CONFIABILIDADE	86
TABELA 4-6-PROGRAMA DE TESTES CONSOLIDADO DO DOSADOR PARA CALCULO DO n_{eff}	88
TABELA 4-7-PROGRAMA DE TESTES CONSOLIDADO COM AUMENTO DAS AMOSTRAS	90
TABELA 4-8-PERFIL DE OPERAÇÃO DOS MOTORES NAVAIS.....	108
TABELA 4-9-ESTIMATIVA DE VIDA DO SISTEMA SCR EM APLICAÇÕES INDUSTRIAIS	109
TABELA 4-10-DADOS DE FALHA CONSOLIDADOS	110
TABELA 4-11- QUOTA DE FALHA POR HORAS DE OPERAÇÃO.	111
TABELA 4-12-PARÂMETROS CONSOLIDADOS DE TESTES	112
TABELA 4-13-PROGRAMA DE TESTES CONSOLIDADO – MARÍTIMA.....	112
TABELA 4-14- PROGRAMA DE TESTES CONSOLIDADO COM ESFORÇO ADICIONAL– MARÍTIMA .	114

LISTA DE ABREVIATURAS E SIGLAS

ALARP	As Low As Reasonably Practicable
ECA	Emission Control Areas
EGR	Exhaust Gas Recirculation
FSA	Formal Safety Assessment
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
GBS	Goal-Based Standards
HFO	Heavy Fuel Oil
HAM	Humid Air Motor
HAZOP	Hazard and Operability Studies
IMO	International Maritime Organization
MTBF	Mean Time Between Failure
MARPOL	Convention for the Prevention of Marine Pollution From Ships
MSC	Maritime Safety Committee
NPR	Number Priority Risk
PPM	Partes por Milhão
PRA	Probabilistic Risk Analysis
RCO	Risk Control Options
SCR	Selective Catalytic Reduction
SLA	Safety Level Approach

LISTA DE SÍMBOLOS

β	Parâmetro de Forma da distribuição de Weibull
k	Número de unidades intactas da distribuição Qui-Quadrado
L_v	Relação de vida de teste e objetiva
n_{eff}	Número de amostra efetiva
P_A	Nível de confiança
q	Quota de falha
r	Fator de aceleração
R_0	Confiabilidade <i>a priori</i>
$R(t)$	Função de Confiabilidade
$R(t_s)$	Confiabilidade para o tempo requerido
$R(t_i)$	Confiabilidade do teste
t_t	Tempo de teste
t_s	Tempo requerido
T	Tempo de vida característico da distribuição de Weibull
t_0	Tempo no instante 0
t_i	Tempos de falha no instante i
$\lambda(t)$	Taxa de falha exponencial

SUMÁRIO

1	INTRODUÇÃO.....	16
1.1	Abordagem proativa de segurança	16
1.2	Objetivos	24
1.2.1	Principal.....	24
1.2.2	Específico	24
1.3	Justificativa	24
1.4	Estrutura da tese.....	27
2	FUNDAMENTOS	29
2.1	Conceituação de segurança de sistemas	29
2.1.1	Segurança como qualidade.....	29
2.2	Fundamento da gestão de risco.....	30
2.2.1	Conceito de risco.....	30
2.2.2	Risco <i>versus</i> Incerteza	31
2.2.3	Risco <i>versus</i> Perigo.....	32
2.2.4	Quantificação do risco	32
2.2.5	Aceitação do nível de risco.....	33
2.2.6	Métodos para desdobramento da meta de aceitabilidade do risco	35
2.2.7	Estratégia para acompanhar a meta de confiabilidade.....	38
2.3	Fundamentos do FSA	39
2.4	Fundamentos do GBS.....	42
2.4.1	Análise de risco com base no FMEA.....	45
2.5	Processo de engenharia de confiabilidade	48
2.5.1	Definições e Características.....	48
2.5.2	Confiabilidade como medida de risco em projetos	49
2.5.3	Metas de confiabilidade.....	50

2.5.4	Consecução das metas de confiabilidade	52
2.5.5	Planejamento estatístico de testes de confiabilidade	55
3	PROPOSTA DO MÉTODO	65
3.1	Introdução ao método proposto	65
3.2	Descrição do método proposto	65
4	EXEMPLOS PRÁTICOS	70
4.1	Aplicação Automotiva.....	70
4.1.1	Identificação do evento indesejado	70
4.1.2	Identificação das falhas potenciais	73
4.1.3	Análise dos modos das falhas dos componentes.....	80
4.1.4	Relação dos modos de falha com os eventos indesejados	81
4.1.5	Estabelecimento da meta de quota de falha por modo de falha.....	82
4.1.6	Demonstração da meta de quota de falha.....	82
4.1.7	Aplicação da Metodologia de análise de risco com base no FMEA	93
4.1.8	Análise dos resultados	96
4.2	Aplicação Marítima.....	97
4.2.1	Identificação do evento indesejado	97
4.2.2	Identificação das falhas potenciais do sistema e o modo de falha	101
4.2.3	Relação das falhas com os eventos indesejados.....	105
4.2.4	Estabelecimento da meta de quota de falha q por modo de falha.....	106
4.2.5	Demonstração da meta de quota de falha.....	112
5	CONCLUSÕES.....	117
6	REFERÊNCIAS BIBLIOGRÁFICAS	119
A	ANEXO – Fundamentos da Confiabilidade.....	128
B	ANEXO – Análise de Garantia.....	146

1 INTRODUÇÃO

1.1 Abordagem proativa de segurança

Nas últimas décadas a valorização da vida tem se tornado um tema central na pauta da sociedade moderna, e isso pode ser constatado na mudança de comportamento das pessoas, que cada vez mais vêm buscando um estilo de vida mais saudável, ambientes menos prejudiciais e tratamentos médicos mais eficazes. Esses fatores têm contribuído para o aumento significativo da expectativa de vida, que no início do século XX era em média 30 anos e hoje já supera os 80 anos em alguns países (GALOR; MOAV, 2005; WHO, 2012), mostrando que o limite para o prolongamento da vida ainda continuará sendo testado por muito tempo.

De fato existe hoje uma possibilidade concreta de se aumentar a longevidade humana através de cuidados com o corpo que visam responder às imposições da idade; porém, prolongar a vida não depende apenas disso: é preciso preservar o corpo da ação de fatores externos que podem produzir acidentes ou condições inseguras às pessoas nas diversas situações do cotidiano.

Proteger as pessoas contra os fatores externos tem-se mostrado uma tarefa complexa, pois envolve um número elevado de variáveis as quais se dividem em dois grupos: àquelas relacionadas à natureza e cujo comportamento muitas vezes não é conhecido e às que tem origem na interface das pessoas com os produtos concebidos pelo próprio homem. Nesse segundo grupo, um produto defeituoso, mal operado ou impróprio pode dar origem a acidentes.

Porém, como muitos desses produtos estão incorporados no cotidiano da vida moderna, e não há sinais de que a sociedade esteja disposta a abandoná-los, têm surgido pressões da própria sociedade para aumento da segurança para quem opera os produtos, que os utiliza e que está exposto a seus efeitos.

Por conta disso, o aumento da segurança tem sido feito em diversas áreas, mas é nos segmentos de transportes que se observam avanços efetivos isso se deve talvez pela repercussão que acidentes com veículos de transporte de massa, como navios, aviões, ônibus, produzem na mídia, gerando como consequência uma percepção de que esses veículos não são seguros e, portanto necessitam de aprimoramentos constantes.

Esse contexto faz com que o tema segurança se torne prioritário no segmento de transporte, e tem sido na área marítima que os resultados têm sido aprimorados a cada ano, é o que mostra o estudo realizado por Gavin (2006), apontando redução de 75% na taxa de perda de vidas por mil embarcações, a qual caiu de 4,3 para 1,3, no período entre 1980 e 2005. De fato, esse é um resultado que demonstra a efetividade das ações tomadas pelo setor.

Embora os resultados sejam animadores, constata-se que as mudanças mais significativas para o aumento da segurança não aconteceram como consequência de um processo de melhoria contínua, mas foram reações a graves acidentes. Citem-se, por exemplo: o naufrágio do *Princess Victoria*, em 1953, vitimando 133 vidas; o *The Herald of Free Enterprise*, com 193 mortes; o petroleiro *Exxon Valdez* que, em 1989, após a ruptura de seu casco, derramou cerca de 41 milhões de litros de óleo cru em águas remotas do Alasca (Estados Unidos), com efeitos desastrosos para a fauna e a flora da região.

Essa postura reativa para tornar os sistemas marítimos mais seguros pode estar impedindo que se avance ainda mais a redução dos acidentes e perdas de ativos das empresas (KONTOVAS *et al.*, 2007a).

Foi então que a Organização Internacional Marítima (IMO) decidiu concentrar esforços da comunidade técnica científica para encontrar maneiras de atuação proativa de segurança desde o projeto até a construção dos sistemas marítimos (HUSS, 2007).

Assim, em 2002 conforme o documento (MSC Circ. 1023, MEPC Circ. 392)¹, a IMO introduziu uma abordagem de risco, a avaliação formal de segurança (FSA), que é um processo racional e sistemático para avaliar os riscos relacionados a segurança marítima e ao meio ambiente a qual as atividades do transporte marítimo estão inseridas.

O uso da FSA inaugurou na IMO uma forma de atuação proativa como alternativa às abordagens preventiva e reativa usadas até então; a figura 1.1 mostra de forma resumida como essas abordagens transformam as demandas da sociedade em requisitos de segurança para o projeto.

Figura 1-1 Tipo de abordagem de segurança para atendimento das demandas da sociedade

Apesar da FSA ter sido aceita como uma forma efetiva de se atuar com segurança, novas propostas continuaram a surgir. Em 2002, na IMO, Bahamas e Grécia

¹ IMO: MSC :Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process . MSC circ. 1023, MEPCcirc. 392.2002.

apresentaram um conjunto de princípios (*Council document C 89/12/1*)² o qual ficou conhecido como GBS, cujo intuito era conduzir o projeto e construção de embarcações para níveis superiores de segurança. Mas foi apenas em 2006 que esses princípios tornaram-se aplicáveis ao processo de projeto e construção, pois evoluindo para uma estrutura contendo cinco níveis, passando a permitir ações de segurança, conforme documento (MSC 81/6/14)³.

Segundo Hoppe (2005), esses níveis são como diretrizes destinadas a assegurar o atendimento das metas de segurança do projeto fazendo com que as normas prescritivas deixem de ter papel central para se chegar a um projeto seguro. E isso é conseguido pela condição oferecida pelo GBS aos desenvolvedores de projeto, concedendo a eles maior liberdade na definição das especificações do projeto ligadas aos requisitos de segurança e, dessa forma, permitindo compensar a defasagem que geralmente existe nas normas prescritivas, devido a não incorporarem na mesma velocidade às mudanças ocorridas nas condições de operação dos veículos marítimos.

Embora o GBS tenha sido visto inicialmente dentro dos comitês de segurança da IMO como uma forma mais abrangente de se melhorar os aspectos de segurança dos sistemas, alguns membros dos comitês e da comunidade científica do setor marítimo, como Psaraftis, Kantovas e Zachariadis, recomendavam cautela quanto à sua imediata aplicação, por entenderem que é preciso primeiro encontrar uma forma de se validar as especificações de projeto produzidas com o uso do GBS, pelo fato de que essas especificações possam ser geradas sem respaldo das normas prescritivas.

Kontovas et al.(2007a) argumenta que os níveis do GBS são compostos por diretrizes, cujo papel é orientar as especificações do projeto, como dimensões, tipos de materiais, entre outras, e não em determiná-las, sendo essa a função dos desenvolvedores de

² IMO: Strategic plan: Consideration of the strategy and policy of the organization including the report of the working group. *Council document c 89/12/1*, 2002.

³IMO: Goal-Based New Ship Construction Standards. Safety level approach .Worked Example MSC 78/6/20, 2006.

projeto. Por conta disso, eventuais exageros, inconsistências, conflitos, poderiam ocorrer e comprometer o atendimento das metas de segurança do projeto.

Na estrutura GBS, a definição das metas de segurança é prevista no nível I e a demonstração do seu atendimento no nível II. A demonstração é feita a partir de metas de probabilidade de falha para os sistemas e componentes, que são desdobradas a partir de níveis de risco do nível I que no setor marítimo é definida pela frequência de mortes por embarcações/ano. São esses dois níveis que delimitam o escopo de atuação deste trabalho, conforme mostrado na figura 1.2. A questão central a ser respondida nessa tese é de como demonstrar o atingimento da meta de probabilidade de falha antes de projetar o produto.

Figura 1-2- Processo de transformação das demandas da sociedade em requisitos de segurança através da integração das abordagens GBS e de risco

A maneira encontrada pela IMO para responder essa questão foi aplicar o FSA em conjunto com o GBS (IMO, 2006): no entanto, essa combinação tem sido contestada. As deficiências do FSA quando aplicada à abordagem GBS para os níveis I e II são apresentadas em diversos trabalhos como Kontovas (2005), Kontovas e Psaraftis

(2006), Zachariadis et al. (2007) Kontovas et al. (2007a) e Kontovas et al.(2007b). Dentre o elenco de deficiências discutidas nesses trabalhos, duas delas são tratadas no presente trabalho:

1. Somente permite verificar se a meta de segurança é atendida após o surgimento de falhas;
2. Metas de segurança do sistema não são desdobradas por modo de falha para os componentes, dificultando a verificação do seu atendimento quanto à meta.

O primeiro ponto ressalta que a FSA não permite medir satisfatoriamente os efeitos das opções de controle de riscos (RCO's) durante o projeto, sem que haja dados suficientes para a análise, o que significa que devem ter ocorrido acidentes. Essa condição limita a possibilidade de se determinar a priori com um determinado nível de certeza se as metas de segurança serão atendidas, o que pode implicar em aprovar um projeto de um sistema sem que esteja tecnicamente maduro ou ainda que esteja ocultando uma falha crítica que não teve tempo suficiente de se manifestar.

O segundo refere-se à forma pela qual a abordagem GBS orienta o estabelecimento das metas. No GBS, o objetivo central não está apenas em saber se as características do sistema atendem a um determinado requisito de segurança, mas também em conhecer a probabilidade desse sistema falhar operando sob condições específicas durante determinado período de tempo. Para isso, é preciso atribuir a cada modo de falha potencial uma probabilidade de ocorrência e dar-lhe um tratamento estatístico adequado que permita efetuar previsões acerca do desempenho futuro do sistema.

Para lidar adequadamente com conceitos de probabilidade de falha e estimativas de desempenho, é preciso um arcabouço estatístico específico com procedimentos e formas de análise que estejam baseados na teoria da confiabilidade, cuja correta aplicação depende de profissionais especializados. A proposta do FSA não trata conceitos de probabilidade de falha com as técnicas de confiabilidade e, por essa razão, a avaliação de risco pode trazer resultados enviesados com prejuízo ao processo de tomada de decisão no projeto.

Não é só o FSA que carece dessa cobertura estatística para o conceito de probabilidade de falha. Em outras metodologias de avaliação de risco, como as baseadas na técnica da análise do modo e efeito da falha (FMEA), e que são amplamente usadas em diversos setores industriais, inclusive no marítimo, a probabilidade ocorrência da falha (O) é um valor tabelado, escolhido por decisão de especialistas, que multiplicado por outras duas variáveis, detecção (D) e severidade (S) gera um índice de risco conhecido como número de prioridade de risco (NPR) (MADDOX, 2005).

Apesar do valor tabelado de probabilidade de falha ser considerado uma razoável aproximação do valor real, a maior deficiência apontada pelos críticos quanto ao uso do FMEA está na projeção dos valores de probabilidade de falha para as fases futuras do projeto. Isso acontece, pois como aplicação do FMEA é feita nas fases iniciais do projeto, normalmente o valor do NPR está em um patamar elevado acima do aceitável. Porém, como o valor do NPR é função da multiplicação das variáveis (O), (S) e (D), uma forma de reduzir o risco é a redução dos valores uma dessas variáveis.

Quando a probabilidade de falha é um valor a ser reduzido, ações para melhoria do projeto do sistema ou componente são planejadas e, com essas medidas, assume-se que o componente terá uma probabilidade de falha reduzida, sem que haja qualquer avaliação estatística para confirmar essas projeções.

Para Puente et al. (2002); Segismundo e Miguel (2006), o FMEA é uma ferramenta que ganhou reputação dentro do processo de asseguramento da qualidade no desenvolvimento de produtos, especialmente por oferecer uma forma estruturada de análise das falhas potenciais. Porém, o uso do NPR como indicador de tomada de decisão deve ser usado com cautela; as razões são elencadas abaixo;

- ❑ Não há uma regra algébrica precisa para a determinação do índice de ocorrência (“O”) e detecção (“D”);
- ❑ O cálculo do NPR baseado no produto dos três índices pode causar distorções, pois, enquanto a probabilidade de não-detecção e sua respectiva pontuação

seguem uma função linear, a relação entre a probabilidade de ocorrência de uma falha e sua pontuação não necessariamente é linear; tratando-se de confiabilidade, segue a teoria da probabilidade;

- ❑ Diferentes pontuações de “O” e “D” podem levar a um mesmo NPR, apesar de o risco envolvido ser completamente diferente;
- ❑ O NPR não consegue mensurar a efetividade das ações de melhoria propostas.

É por conta das limitações das abordagens FSA e FMEA usadas como metodologias de gestão de riscos em projetos, surgiu aqui a motivação para o desenvolvimento de uma proposta de método quantitativo com ênfase em confiabilidade buscando-se proporcionar para as fases iniciais do projeto uma medida de risco baseada em inferências estatísticas, conferindo níveis de certeza a suas estimativas. A figura 1.3 mostra um comparativo das principais diferenças entre a metodologia proposta e os métodos FMEA e FSA.

Figura 1-3- Comparativo entre as abordagens de risco

Assim, com a apresentação do método proposto e sua aplicação em dois exemplos práticos, contribui-se para o desenvolvimento de um processo de gestão de risco que seja mais adequado para avaliação dos sistemas relacionados à segurança.

1.2 Objetivos

1.2.1 Principal

Propor um método, com base no planejamento estatístico de testes de confiabilidade, para instrumentalizar quantitativamente a abordagem “Padrões Baseados em Metas” (GBS) quanto à verificação do atendimento das metas de confiabilidade de componentes que afetam a segurança do sistema em foco. A proposta se restringe aos níveis I e II do GBS, o primeiro nível tratando do estabelecimento de metas de segurança para o sistema, e o segundo da definição de requisitos quanto à probabilidade de falha para os subsistemas.

1.2.2 Específico

Aplicar o método proposto em dois exemplos práticos para componentes do subsistema de pós-tratamento dos gases de exaustão em motores a diesel de veículos automotivos e marítimos.

1.3 Justificativa

Estimar a probabilidade de ocorrência de eventos aleatórios muitas vezes é contra intuitiva; porém, essa forma contrária ao senso comum, que tem base científica esbarra em crenças, emoções, certezas, que são despertadas por asserções ou conjecturas, podendo levar a inferências indutivas enviesadas. O resultado da tomada de decisão

com base nessas inferências tem sido uma das razões da ocorrência de falhas catastróficas em sistemas.

A deficiência apresentada pela maioria das abordagens de risco aplicada à avaliação de sistemas que afetam a segurança é que faz projeções sobre eventos aleatórios sem dar a ele um tratamento estatístico apropriado. Esse tratamento é necessário, devido a natureza incerta dos resultados do experimento aleatório, em que se pode considerar apenas sua probabilidade de ocorrência, cuja determinação requer a especificação do espaço amostral, sendo que toda conclusão tirada carregará um grau de incerteza.

A dificuldade em se afirmar se o resultado da análise de risco pode ser adotado como balizador do atendimento das metas de segurança reside no fato de que essas abordagens usam o conceito de probabilidade de falha, que tem origem na teoria da confiabilidade, sem levar em conta o tamanho da amostra e tempo de duração dos testes com apropriada cobertura estatística.

Essa deficiência de cobertura estatística do programa de testes pode produzir:

- falhas avaliadas com baixo risco no projeto, mas que aparecem mais adiante em sua operação, embora não tenha sido necessária qualquer ação de mitigação do risco;
- falhas catastróficas avaliadas com alto risco no projeto, que sofreram ações para redução do risco, mas se manifestaram na operação, implicando em custos de garantia e de eventuais indenizações.

Buscando reduzir o nível de incerteza das previsões de desempenho do sistema que afetam a segurança, o planejamento estatístico de testes de confiabilidade surge como uma alternativa aos métodos tradicionais, demonstrando estatisticamente o atendimento das metas de confiabilidade durante a realização do projeto.

Segundo Krolo *et al.* (2002), o uso das técnicas de planejamento estatístico no processo de desenvolvimento de sistemas permite saber, com um nível elevado de certeza, se os testes previstos para o componente ou sistema são suficientes para

atender às metas de confiabilidade mesmo na fase de planejamento do projeto, estágio em que ainda não há protótipos físicos .

Ademais, essa metodologia proporciona investigar, ainda na fase de planejamento do projeto, se as metas de confiabilidade, e de segurança poderão ser verificadas com o programa de testes previsto, auxiliando, assim, na construção de um programa de testes com foco na garantia da confiabilidade.

Essa situação suscita as seguintes questões: Será que as metodologias de risco são adequadas às análises de segurança de sistemas? Será que as abordagens quantitativas e qualitativas do risco são usadas de forma correta para auxiliar o gestor na tomada de decisão?

Para Raz *et al.* (2002), o gerenciamento dos riscos durante o desenvolvimento de um projeto não alcançou um nível de maturidade satisfatório e, por conta disso, ainda são necessários esforços no desenvolvimento de modelos e treinamento de pessoas. Outro aspecto destacado é que as metodologias de gerenciamento de riscos não podem ser padronizadas para todos os tipos de projetos, mas devem ser adaptadas à sua natureza de escopo e incerteza metodológica.

Embora metodologias FMEA e FSA usadas para gestão de risco necessitem de um maior aprimoramento, isso não tem impedido seu uso para tomadas de decisões em projetos. O que se observa é que as análises geradas por essas metodologias são adotadas para aprovação de projetos de sistemas, mesmo sem medidas de incerteza que mostrem eventuais supervalorizações ou subutilizações nas suposições e premissas assumidas. O quadro da figura 1.4 apresenta as principais deficiências dessas abordagens para projetar valores de probabilidade de falha ao longo do projeto.

FSA-Marítima	FMEA-Automotiva
<ul style="list-style-type: none"> ➤ Valor do risco decresce com base em ações para redução da probabilidade de falha, sem validação estatística. ➤ Permite comprovar o atendimento da meta de segurança, somente após ocorrência de falhas. ➤ Desdobra meta de probabilidade de falha até o nível de componente, <u>não chega até os modos de falha.</u> 	<ul style="list-style-type: none"> ➤ O indicador quantitativo NPR usa <u>valores tabelados de ocorrência de falha</u> sem indicar o tipo de distribuição de falha ➤ Permite comprovar o atendimento da meta de segurança <u>após ocorrência de falhas ou no final do projeto após conclusão dos testes</u>

Figura 1-4- Principais deficiências FSA e FMEA

Assim, o propósito deste trabalho está em propor uma metodologia que supere as deficiências dos métodos tradicionais como FMEA e FSA. Como os debates estão só começando, o campo está aberto para propostas de tratar o tema e que possam contribuir com projetos mais eficazes do ponto de vista da segurança.

1.4 Estrutura da tese

Este trabalho está organizado em seis capítulos:

Capítulo 1 - Introdução

Capítulo 2 - Fundamentação Teórica e Revisão de Literatura

Capítulo 3 - Proposta do Método

Capítulo 4 - Exemplos práticos

Capítulo 5 - Considerações Finais

Capítulo 6 - Referências Bibliográficas

Anexos

Capítulo 1: São apresentados o contexto da abordagem proativa de segurança, os objetivos, a justificativa e a estrutura da tese.

Capítulo 2: Exibem-se : conceituação de segurança de sistemas; fundamentos de risco; fundamentos sobre a FSA, fundamentos sobre a GBS, conceitos sobre engenharia de confiabilidade

Capítulo 3: Propõe-se um método de análise de risco com base no planejamento estatístico de testes, para aplicação em conjunto com princípios do GBS. Listam-se as principais etapas do método, as atividades e as ferramentas de análise aplicáveis.

Capítulo 4: São desenvolvidos dois exemplos práticos, um na indústria automotiva e outro na marítima. Os objetos de estudo são componentes mecânicos pertencentes a sistemas de pós-tratamento dos gases de combustão, cuja função é a redução dos poluentes aos níveis exigidos pelas normas de emissões que entrarão em vigor nos próximos anos, em ambos os segmentos.

No primeiro exemplo, são aplicadas duas técnicas de análise de risco para o mesmo componente – dosador catalítico –, sendo uma baseada na FMEA e a outra no método proposto neste trabalho. A comparam-se os resultados para se verificar qual das técnicas fornece a informação mais confiável para a tomada de decisão de entregar o sistema no prazo, com um maior nível de maturidade técnica, ou seja, na expectativa de atender aos requisitos de desempenho do sistema que podem afetar a segurança.

No segundo exemplo, o modelo proposto é aplicado para o componente reator catalítico, a fim de avaliar a técnica proposta para o segmento marítima, no qual, diferentemente do automotivo, há poucas unidades amostrais de testes. Ao final, são analisados e discutidos os resultados da aplicação do método.

Capítulo 5: São apresentadas as conclusões, sugestões críticas, contribuições e recomendações em função da experiência com a aplicação do método proposto.

2 FUNDAMENTOS

2.1 Conceituação de segurança de sistemas

Segurança é definida no dicionário Webster (1977), como a “condição de estar seguro em uma situação que cause danos ou perdas”. Para a área de engenharia, segurança é o julgamento da aceitabilidade do risco para um sistema (AYYUB et al., 2002). Segundo Guimarães (2003), o conceito de segurança de sistemas está relacionado aos fundamentos da ciência das falhas, sendo segurança de sistemas definida como a capacidade de um sistema cumprir uma missão com sucesso para o tempo ao qual foi concebido, sem que ocorram eventos com consequências indesejáveis.

Para Shtub et al. (1994), os esforços para aumentar a segurança são medidas que se destinam à redução dos riscos ou perigos relacionados a falhas catastróficas do sistema e que se são implementados através do uso de métodos e ferramentas de análise de segurança desde a concepção até a finalização do projeto .

2.1.1 Segurança como qualidade

O conceito de qualidade tem sido modificado ao longo das últimas décadas, período no qual surgiram algumas definições clássicas. Nessas definições, qualidade é:

- capacidade de satisfazer desejos (DEMING, 1982);
- desempenho do sistema, que resulta em satisfação do cliente, livre de falhas (JURAN, 1992);
- conformidade com os requisitos (CROSBY, 1979);
- minimização das perdas causadas pelo sistema para sociedade a longo prazo (TAGUCHI, 1986).

Em uma definição mais formal, qualidade é o grau em que um conjunto de características inerentes satisfaz a requisitos (ABNT, 20002).

Em segurança de sistemas, qualidade é o grau pelo qual o projeto de um sistema reflete as necessidades do mercado ou dos clientes, e o grau pelo qual o sistema ou o serviço atendem às especificações do projeto. Nesse contexto, qualidade refere-se à integração dos componentes do sistema e à compatibilidade deste com o ambiente no qual irá interagir (SHTUB et al.,1994). Para Guimarães (2003), qualidade de um sistema não se define apenas pela conformidade às especificações, mas também pela permanência de suas especificações ao longo do tempo de utilização do sistema. A capacidade do sistema de preservar suas características de desempenho ao longo da vida é conhecida como confiabilidade, tornando-a assim, uma extensão da qualidade e (GUIMARÃES, 2003).

Nesse contexto, segurança de sistemas é consequência da eficácia da gestão da qualidade do projeto, a qual deve asseverar o atendimento de todos os requisitos relevantes ao desempenho do produto do projeto, e também identificar situações que impeçam a demonstração, verificação ou até atendimento desses requisitos, prevendo formas de se avaliar os riscos para auxiliar o gerente do projeto no processo de tomada de decisão (GUIMARÃES, 2003).

2.2 Fundamento da gestão de risco

2.2.1 Conceito de risco

Risco é um termo com significado muito amplo e com aplicações diversas, como em negócios, vida social, econômica, investimentos, militar, política, industrial, entre outras. Apesar disso, ainda falta um entendimento único sobre sua definição (KAPLAN; GARRICK, 1981). Para Fischhoff et al. (1984), a definição de risco é inerentemente controversa, pois sua escolha depende de como esta se ajusta às posições políticas.

No entendimento apresentado por Thompson (1987), risco é um parâmetro abstrato para representar o impacto de um evento adverso ou ação sobre as quais não há certeza. Contudo, existe um entendimento geral de que a noção de risco envolve incertezas sobre a ocorrência dos eventos, que são associados ao tipo de perda ou falha (KAPLAN; GARRICK, 1981).

Por outro lado, Sage (1995) argumenta que o risco não está limitado somente a eventos adversos, mas pode incluir resultados positivos, desde que sua ocorrência seja incerta.

Entretanto, a aceção de risco mais usual é aquela que tem conotação mais de possibilidade de perda e falha do que de ganho. Isso não significa necessariamente que qualquer evento indesejado de uma decisão constitua risco, mas que ele somente se torna risco quando está associado à incerteza de ocorrência sendo.

A concepção de risco adotada para esse estudo é a mesma utilizada na engenharia, que é a probabilidade de ocorrência de um evento que ocasiona perda ou falha para o sistema que pode gerar impacto na segurança (AYYUB et al., 2002).

2.2.2 Risco *versus* Incerteza

Embora as palavras incerteza e risco estejam intrinsecamente relacionadas e sejam usadas de forma intercambiável, elas expressam conceitos distintos.

Ayyub et al. (2002) define incerteza como um conhecimento que pode ser incompleto, impreciso, vago, ambíguo, ou seja, uma característica inerente ao conhecimento. Por sua vez, Knight (1921) *apud* Agumya, Hunter (1999) definem risco como uma medida de incerteza. Normalmente se diz que se está em um estado de incerteza, mas dificilmente em um estado de risco. A noção de risco envolve incerteza e algum tipo de perda ou danos nessa abordagem Kaplan e Garrick (1981) escrevem risco como o resultado da soma de incerteza com danos.

2.2.3 Risco versus Perigo

Frequentemente, risco e perigo são empregados como sinônimos. No entanto, ambos possuem definições distintas. No dicionário Webster (1977), perigo é definido como uma fonte de ameaças. Kaplan e Garrick (1981) definem perigo como uma fonte de consequências adversas; para Pidgeon et al. (1992), perigo é uma ameaça para pessoas e coisas. Risco é a possibilidade de perda ou prejuízo e o grau de probabilidade de ocorrência dessa perda.

Perigo existe somente como uma fonte. Risco inclui a probabilidade de conversão da fonte em entrega da perda ou alguma forma de prejuízo. No âmbito de projetos, pode-se afirmar, então, que a incerteza na informação pode constituir um perigo, especialmente se ela for ignorada. Dessa perspectiva, pode-se argumentar que a exposição para o risco resulta da presença de perigo.

Nesse contexto, o risco poderia ser reduzido se houvesse algum tipo de proteção contra o perigo. Kaplan e Garrick (1981) expressam essa idéia por meio da relação $\text{risco} = \text{perigo} / \text{proteção}$. Essa relação traz a idéia de que o risco pode ser tão menor quanto maior for a proteção; no entanto, pelo menos em princípio, trazê-lo a zero seria impossível, mas, próximo de zero, uma possibilidade. A idéia de proteção remete a ter consciência sobre os riscos, ou seja, quando se tem consciência de risco, naturalmente busca-se sua diminuição (KAPLAN; GARRICK, 1981). Neste trabalho, a palavra perigo é aplicada no sentido empregado pela engenharia, referindo-se a causas de consequências adversas.

2.2.4 Quantificação do risco

Em ambientes de projetos em que se usa a abordagem de riscos para tomada de decisão, é muito comum as decisões serem balizadas em valores de risco que são calculados a partir de avaliações quantitativas. Essas avaliações são realizadas a partir da multiplicação de valores atribuídos aos fatores, consequência c_x e probabilidade de

ocorrência p_x para um determinado evento x ; e a partir, daí constroem-se cenários de risco $(p_x.c_x)$. O valor de risco global é a combinação de todos esses cenários, como mostra a expressão:

$$Risk \equiv [(p_1.c_1), (p_2.c_2), \dots, (p_x.c_x)]$$

Segundo Ayyub et al. (2002), quando se avaliam incertezas associadas a um evento, o risco pode ser medido através de um par de fatores, a saber, a probabilidade de ocorrência de um evento e a sua consequência, em que o primeiro se refere a um cenário de falha e outro ao efeito ocasionado pelo evento. Esse par de fatores pode ser representado pela equação (2.1):

$$Risk \left(\frac{Consequência}{Tempo} \right) = probabilidade \left(\frac{Evento}{Tempo} \right) \times impacto \left(\frac{Consequência}{Evento} \right) \quad eq.(2.1)$$

Nessa representação, risco é calculado como o sistema da probabilidade de um evento ocorrer e o impacto de sua ocorrência.

2.2.5 Aceitação do nível de risco

A aceitabilidade do risco é o ponto a partir do qual o risco é considerado aceitável, tornando esse um assunto complexo, sendo, na maioria das vezes, controverso devido às diferentes percepções de segurança que existem na sociedade, representada por exemplo pela tripulação e pelo fabricante passageiro, tripulação e fabricante. No entanto, determinar a faixa de risco aceitável é uma tarefa crucial para o patamar de desempenho de segurança que se busca para o segmento de transporte no qual sua definição deve sempre envolver os pontos de vista dos diferentes interessados (AGUMYA; HUNTER, 1999).

De acordo com Ayyub et al. (1999), uma forma de definir o nível de segurança aceitável é pelo uso de critérios. Para Mannan (2005), os critérios utilizados no segmento marítima seguem a proposta do diagrama de Farmer, que relaciona a frequência de fatalidades por navios/ano (FN). Conforme destaca Kumamoto (2007), essa curva é usual para a análise de segurança dentro do segmento marítimo, embora tenha sido inicialmente criada para o segmento nuclear.

O diagrama FN possui três regiões de risco: intolerável (não aceitável), tão baixo quanto razoavelmente praticável (ALARP) e aceitável. Um modelo genérico de diagrama é mostrado na figura 2.1.

Figura 2-1-Diagrama FN (adaptado de IMO (2007))

Essa curva é utilizada para estimar o risco das atividades marítimas para a sociedade. Risco para a sociedade é o risco médio em termos de fatalidades, em que um grande grupo de pessoas, incluindo tripulação, funcionários das instalações *offshore*, passageiros e sociedade como um todo, está exposto a um cenário de acidentes (KONTOVAS, 2007a).

2.2.6 Métodos para desdobramento da meta de aceitabilidade do risco

Existe um amplo ferramental encontrado na literatura para desdobrar a meta de aceitabilidade do risco. Abaixo estão elencados dois deles, da árvore de falhas e de eventos.

□ Árvore de falhas

Esse é um método dedutivo que usa a simbologia e os conectores da lógica booleana para relacionar a probabilidade de falha de componentes independentes com a capacidade do sistema de funcionar para uma determinada confiabilidade. Esse método inicia com a identificação do evento indesejado do sistema, conhecido como evento topo; em seguida, levantam-se os eventos intermediários e, em uma última etapa, os eventos base. Todos esses eventos são inter-relacionados através do uso de conectores e de portões lógicos, que conferem à árvore uma lógica de causa e efeito.

Nesse método, as probabilidades de falha são atribuídas para os eventos base – tal nome lhes é atribuído por eles estarem na base da árvore; a partir daí, por meio de procedimentos analíticos da teoria de confiabilidade de sistemas (sistema em série, paralelo ou misto), segue-se o caminho em direção ao topo da árvore para se chegar às probabilidades de falha dos eventos intermediários e do topo (AYYUB et al., 1999, 2002).

Em algumas situações, é preciso construir diferentes árvores para cobrir pelo menos os modos de falha mais prováveis de ocorrerem no sistema. Modos de falhas múltiplos surgem devido à utilização do sistema em diferentes condições de operação e aplicação, exigindo-se do sistema a realização de funções com diferentes requisitos. Contudo, para se chegar à confiabilidade global de cada sistema, os diferentes modos de falha devem ser considerados. Uma forma de incorporar em uma mesma análise as informações dos diversos modos de falha é através da multiplicação dos pesos de cada modo pela sua contribuição para a probabilidade total das falhas do sistema. As

probabilidades, ou taxas de cada modo de falha para um novo projeto, podem ser obtidas com base em dados de garantia de sistemas similares, históricos de projetos, simulações computacionais e opinião dos especialistas (AYYUB *et al.*, 1999).

□ Árvore de eventos

Esse método foi empregado pela primeira vez no início da década de 1970 para a avaliação de risco associada às centrais nucleares nos Estados Unidos (GUIMARÃES, 2003). A árvore de eventos é um método indutivo que tem por meta identificar as sequências de eventos, falhas ou sucesso, que podem levar a um acidente (AYYUB *et al.*, 2002).

A construção do diagrama começa com um evento inicializador indesejado que, ao ser acionado, pode desencadear várias consequências com diferentes severidades e magnitudes. Os ramos da árvore surgem a partir da seguinte questão: Como poderia ocorrer esse evento?

Aos eventos que derivam dessa questão são atribuídas duas possibilidades: ter sucesso ou falha. As probabilidades de sucesso e de falha podem ser obtidas pela árvore de falhas ou por outros métodos.

As probabilidades de vários eventos sequenciados formam um modelo de probabilidade condicional que, através de uma multiplicação apropriada, fornece a probabilidade de essa sequência ocorrer (KUMAMOTO, 2007). Um diagrama genérico (figura 2.2) mostra a combinação de árvore de falhas com árvore de eventos para a análise quantitativa de riscos, considerando-se três sistemas (NIEHAUS; LEDERMAN, 1986).

Figura 2-2-Árvore de falha e de eventos genérica (adaptado de Niehaus; Lederman(1986))

A partir da obtenção dos eventos base, chega-se aos componentes relacionados a esses eventos. Com a aplicação de um ferramental apropriado, são levantadas as possíveis falhas os modos de falhas mais prováveis e a probabilidade de ocorrência para cada modo de falha. Para um novo sistema projeto de sistema, metas de probabilidade de falha são atribuídas a esses modos de falhas e, verificado seu atendimento ao longo do projeto.

2.2.7 Estratégia para acompanhar a meta de confiabilidade

O nível de segurança de um sistema pode ser calculado a partir da probabilidade de ocorrência dos eventos indesejados, que, por sua vez, são obtidos pela probabilidade de falha do sistema (GUIMARÃES, 2003).

A probabilidade de falha torna-se, nesse caso, uma variável de controle relevante e, por essa razão, deve ser acompanhada ao longo do ciclo de desenvolvimento do novo sistema. Uma das formas de fazer esse acompanhamento é através da construção de uma curva planejada, com base na confiabilidade atual (dados de campo, testes, histórico de projetos) ou inerente (referindo-se às características do novo sistema), conforme proposta na figura 2.3 (IRESON et al., 1995). Nessa curva, a linha tracejada parte da taxa de falha inerente e a linha cheia do valor máximo admissível para o início do projeto – esse valor se aplica quando se tem apenas informações da confiabilidade atual, ou devido à ocorrência de problemas relacionados à produção (*burn-in*).

Figura 2-3- Curva de confiabilidade durante o projeto (adaptado de Ireson et al. (1995))

O tempo de recuperação mostrado no gráfico da figura 2.3 indica que, quando se parte do valor máximo admissível, é preciso ter um plano para a redução da taxa de falha durante o projeto, que permita decrescer mais rapidamente para o valor meta quando

comparado com a curva tracejada; ou seja, um maior esforço de testes e projetos deve ser alocado.

No Anexo A, são detalhados outros conceitos e técnicas da teoria da confiabilidade usada para análises de dados de falha, que darão origem às estimativas de confiabilidade, probabilidade de falha, taxa de falha e outras métricas. Os capítulos a seguir utilizam os conceitos e as técnicas de confiabilidade para apresentar metodologias de análise de risco no desenvolvimento de sistemas.

2.3 Fundamentos do FSA

O FSA é definido como um processo racional e sistemático para acessar o risco relativo à segurança marítima e à proteção ambiental e para avaliar os custos e benefícios das alternativas da IMO para reduzir esses riscos. Esse processo é composto de cinco etapas, conforme descrito abaixo (IACS – MSC 75, 2002).

0 - Etapa Preparatória

Inicia com a definição do problema que será avaliado, como tamanho e tipo da embarcação, categorias de acidentes, condições operacionais, sistemas e especificações, e sua relação com a regulação vigente. Outro aspecto abordado nessa etapa é a definição do tipo de risco que a embarcação pode oferecer às pessoas, ao meio ambiente e aos ativos da empresa, como a própria embarcação e instalações. E, por último, trata do critério de aceitação de riscos, dados e as estatísticas de falhas e acidentes.

A definição das metas globais de segurança, que ocorre nessa etapa, é orientada por situações em que se exige proteção para usuários, operadores, população e para o próprio equipamento, e deve refletir o nível de segurança que se deseja alcançar no novo sistema (LEE; McCORMICK, 2011).

Essas faixas de risco também são estabelecidas com base em históricos de acidentes. A IMO patrocinou uma série de estudos para que fossem levantadas as frequências de vítimas por tipo de navio. Um desses estudos foi apresentado no 88th MSC, de 20 de Setembro de 2010 (IMO, 2010), e atribuiu um número de vítimas para cada tipo de acidente marítimo (tabela 2.1). Esses valores passaram a ser utilizados para nortear os limites de número de vítimas por navio / ano para o desenvolvimento e a construção de novos navios.

Tabela 2-1-Freqüência de vítimas por tipo acidentes entre 1997 e 2008 (IMO, 2011)

Categoria de acidente	Vítimas por navio ano
Colisão	$5,5 \times 10^{-3}$
Contato	$2,3 \times 10^{-3}$
Naufração	$1,5 \times 10^{-3}$
Fogo/Explosão	$2,7 \times 10^{-3}$
Danos no casco	$2,0 \times 10^{-3}$
Encalhe	$7,5 \times 10^{-3}$
Falha nos equipamentos	$1,2 \times 10^{-3}$

Etapa 1 – Identificação do Risco

O propósito desta etapa é listar os riscos e os cenários associados priorizados pelo nível de risco específico do problema em análise. Com o uso de algumas técnicas, é possível identificar perigos que possam contribuir para a ocorrência de acidentes e, em seguida, priorizá-los usando uma combinação de dados disponíveis e julgamento de especialistas.

Etapa 2 – Análise do Risco

O propósito desta etapa é detalhar a investigação das causas e consequências dos cenários mais importantes identificados na etapa 1. Isso permite atentar às áreas de risco críticas a fim de identificar e avaliar os fatores que influenciam o nível de risco.

Etapa 3 – Opções de Controle de Risco (RCO's)

Esta etapa identifica as áreas que precisam ser controladas para estabelecer medidas que reduza o risco, o que pode ser obtido pela diminuição da probabilidade de ocorrência e pela mitigação das consequências. Através da reavaliação da etapa 2, medidas de risco podem ser agrupadas em opções de controle de riscos (RCO's).

Etapa 4 – Custo Benefício

O propósito desta etapa é identificar e comparar custos e benefícios associados à implementação dos RCO's identificados e definidos na etapa 3. Custos devem ser expressos em termos do ciclo de vida do sistema, que pode incluir os períodos de instalação, operação, treinamento, inspeção, certificação, desativação etc.

Etapa 5 – Recomendação para a tomada de decisão

Nesta etapa são definidas as recomendações que devem ser apresentadas aos responsáveis por tomar decisão. As recomendações devem ser feitas através da comparação do *ranking* de todos os perigos e suas causas, da comparação do *ranking* dos RCO's como uma função dos custos e benefícios associados, e da identificação de todos os RCO's que mantêm os riscos em nível baixo como aplicação desejável.

O FSA é uma ferramenta que, quando bem estruturada, pode ser valiosa e muito promissora no processo de tomada de decisão da IMO; porém, ela não deve ser encarada como uma solução mágica para os problemas de segurança na indústria marítima ou uma ferramenta que fornecerá recomendações mais corretas ou confiáveis (KONTOVAS, 2007b).

Portanto, o que se busca atualmente é identificar onde residem as deficiências no FSA e se estas podem criar grandes imprecisões nos resultados, quando aplicadas à estrutura GBS, e, em caso positivo, qual a melhor forma de corrigi-las.

2.4 Fundamentos do GBS

O GBS é um elenco de cinco níveis. Segundo Hoppe (2005), tais níveis possuem uma relação de causa e efeito em que, no topo, estão as metas, e, nos níveis subsequentes, os requisitos funcionais necessários para se alcançar essas metas; isso ocorre sucessivamente até o último nível da estrutura, que corresponde às normas e procedimentos (figura 2.4).

Figura 2-4- Estrutura GBS (adaptado de Skjong (2005))

O propósito do GBS é estabelecer diretrizes para a elaboração de normas e regulamentações para o projeto e para a construção de embarcações (HUSS, 2007). Nele sugere-se que a IMO atue com a função de definir padrões de segurança para novas embarcações e também de assegurar que todas as partes da embarcação possam ser acessadas sem dificuldade, com o intuito de permitir fácil inspeção e manutenção (ISSC, 2009; IMO, 2011). Nessa proposta, ficou acordado que os três primeiros níveis deveriam ser desenvolvidos pela IMO, enquanto o quarto e o quinto o

seriam por outros organismos de classe da indústria e da operação marítima, como ISO, IASC, entre outros (IMO, 2004):

Nível I - Objetivos

Embarcações devem ser projetadas e construídas para serem seguras quando operadas de forma apropriada sob condições ambientais específicas, e em condições intactas ou com danos apontados ao longo de sua vida. O uso do termo segurança subteme aqui, a especificação de determinado critério para aceitação do risco.

Deve-se especificar as faixas de risco aceitáveis, através do critério para aceitação do risco descrito no diagrama de Farmer, em que são estabelecidas as regiões de baixo risco aceitável, de ALARP e de risco inaceitável.

Os objetivos são aplicados para seis diferentes aspectos:

1. Segurança para a embarcação;
2. Segurança para a carga;
3. Segurança para os passageiros;
4. Proteção para o meio ambiente;
5. Segurança para a tripulação;
6. Segurança para a terceira parte (funcionários dos portos, população em geral).

Nível II - Requisitos funcionais

Para atingir os objetivos de segurança estabelecidos no nível I, a embarcação tem de prover apropriadamente diversas funções, como:

- Manobrabilidade;
- Geração de energia;
- Proteção contra fogo;
- Desempenho no mar;
- Estanqueidade;

- Estabilidade e flutuabilidade;
- Estrutura da embarcação;
- Segurança na navegação;
- Sistema de propulsão;
- Habitabilidade;
- Equipamentos de salva-vidas;

Para alcançar os objetivos relativos aos índices de segurança do Nível I, são definidas metas de probabilidade de falha para componentes e sistemas. O estabelecimento desses valores tem de considerar a proporcionalidade entre a falha da função e sua consequência em relação à segurança.

Nível III – Verificação dos critérios de atendimento

Fornecer os instrumentos necessários para demonstrar que os requisitos detalhados no nível IV concordam com as metas e requisitos funcionais dos níveis I e II, respectivamente.

Nível IV – Procedimentos técnicos e diretrizes, incluindo padrões nacionais e internacionais.

Nível V - Padrões da indústria, diretrizes, recomendações, práticas de segurança e sistemas de qualidade para treinamento, construção, operação, manutenção de embarcações.

Segundo Zachariadis et al.(2007), o GBS foi criado com o objetivo de introduzir um sistema de normas, isto é, medidas contra as quais a segurança de um navio poderia ser avaliada durante sua concepção e construção, e, mais tarde, no seu funcionamento.

Para Hoppe (2005), o principal papel do GBS não está em especificar para atender a alguma exigência, mas em estabelecer metas que permitam formas alternativas de

atender a essas exigências. Na abordagem GBS, aquele que desenvolve normas para o projeto e a construção de embarcações precisa declarar o desempenho de segurança requerido para sistemas e componentes, e não somente prescrever o atendimento ao conjunto de especificações.

2.4.1 Análise de risco com base no FMEA

O FMEA foi desenvolvido nos anos 50 pela indústria de defesa americana para que se pudesse identificar as possíveis falhas e efeitos que um sistema pode apresentar durante sua operação (CARBONE; TRIPPET, 2004; SIMÕES, 2004). Seu uso tornou-se mandatório na área de desenvolvimento de produtos a partir da introdução da ISO 9001-2000 na década de 1990 e posteriormente a ISO TS16949 nos anos 2000, as quais incorporaram seu uso para a garantia da qualidade do projeto (BERTSCHE, 2008).

A aplicação desse método exige a participação de um grupo multifuncional composto por especialistas de diversas áreas da organização, que contribuem com dados, informações e opiniões para a realização das análises e estabelecimento de ações de melhoria.

As análises previstas no método seguem etapas bem definidas que possam conduzir ao estabelecimento de ações que tornem o sistema menos suscetível a falhas catastróficas. Segundo Bertsche (2008), o FMEA é composto de cinco etapas, conforme segue abaixo:

1. Estruturação;
2. Análise funcional;
3. Análise de falha;
4. Avaliação de risco;
5. Otimização.

Na etapa (1) ocorre à descrição do sistema no nível de subsistemas e componentes, assim como, as características críticas desses componentes que em caso de não

adequadamente projetados podem ser fonte de falha. Na etapa (2) é atribuído a cada subsistema e componente a respectiva função e para suas características críticas o desempenho requerido. O propósito da etapa (3) é identificar as possíveis falhas para cada função do sistema, assim como, os respectivos modos de falha. Na etapa (4) ocorre a avaliação de risco, o qual através da multiplicação de valores de fatores (O) Ocorrência, (S) Severidade e (D) Detecção, para cada modo de falha, chega-se a um índice que representa o risco do sistema, esse índice é chamado de número de prioridade de risco (NPR). Na última etapa (5) avaliam-se as melhorias que podem ser incorporadas no sistema para trazê-lo ao nível de segurança exigido pela organização (SEGISMUNDO; MIGUEL, 2008).

A idéia de usar o FMEA como base para uma abordagem de risco no processo de desenvolvimento de produtos surgiu pela possibilidade de ampliar o uso do indicador NPR para aplicações gerenciais (Maddox, 2005). Por essa razão um detalhamento da etapa (4) é proposto como segue. O NPR é um índice obtido pela multiplicação dos fatores (O), (S) e (D) para cada modo de falha. Os valores de cada fator são obtidos pela tabela 2.2.

Tabela 2-2-Critérios do FMEA para o cálculo do NPR (adaptado de Bertsche (2008))

Critério Ranking	Severidade (S)	Ocorrência (O) em ppm	Detecção (D)
10	Muito alta	500.000	90%
9	Muito alta	100.000	90%
8	Alta	50.000	98%
7	Alta	10.000	98%
6	Moderada	5.000	99,70%
5	Moderada	1.000	99,70%
4	Moderada	500	99,70%
3	Baixa	100	99,90%
2	Baixa	50	99,90%
1	Muito Baixa	1	99,99%

A escala da tabela varia de 1 á 10,

- Probabilidade de ocorrência da falha (O): 1 menor...10 maior
- Severidade da falha (Consequência) (S): 1 menor...10 maior
- Detecção da falha (D): 1 maior ...10 menor

A metodologia de risco baseada no FMEA adota o mecanismo de cálculo do NPR, porém, adicionando subfatores a cada fator de O,S e D com ponderações específicas. Essas ponderações são obtidas por meio de *ckecklists* padrões que atribuem pesos específicos para cada questão,

- Há histórico de falhas de garantia?
- Qual é o nível de complexidade do componente?
- O componente é totalmente novo?
- Há histórico de falhas de desenvolvimento?

E, assim por diante, até levantar as informações que permitam calcular o NPR (SEGISMUNDO; MIGUEL, 2008).

O valor de NPR calculado por esse método é classificado como alto, médio e baixo de acordo com as premissas da organização, portanto podem variar de empresa para empresa. Faixas de risco usadas são mostradas a seguir:

- ☐ Aceitável é entre 1e 65 (faixa verde),
- ☐ Média é entre 65 e 343 (faixa amarela),
- ☐ Alta é entre 344 e 1000 (faixa vermelha).

Segundo Bertsche (2008), o valor de referência difere de acordo com o segmento industrial. No manual de FMEA da indústria automobilista é sugerido que um risco aceitável para liberar o sistema para produção deve ficar abaixo de 125⁴; nesse estudo estabeleceu-se 65 que é o valor utilizado pela maior parte das empresas do setor.

⁴O valor de NPR mínimo de 125 é um valor referência utilizado na indústria automotiva e é recomendado pelas normas de qualidade aplicadas a esse setor, entre elas a VDA (BERTSCHE, 2008).

2.5 Processo de engenharia de confiabilidade

2.5.1 Definições e Características

A palavra confiabilidade tem sido cada vez mais empregada pelas pessoas em situações cotidianas, quando se pretende destacar os aspectos de funcionalidade e durabilidade de um sistema. É comum ouvir que um sistema tem alta confiabilidade quando se quer dizer que ele funcionará adequadamente por um determinado tempo, e que tem baixa confiabilidade se as falhas aparecerem mais precocemente.

Embora se utilize o termo confiabilidade para qualificar um sistema, seu uso deve ser feito com prudência. O principal motivo é que a confiabilidade tem origem na teoria da probabilidade e seu valor é expresso por meio de estimativas que somente podem ser obtidas a partir de apropriada modelagem e experimentos estatísticos (BERTSCHE, 2008).

Nesse contexto, a definição técnica de confiabilidade é uma extensão da definição de probabilidade: confiabilidade é a probabilidade de um sistema não falhar sob dadas condições funcionais e ambientais durante um período determinado de tempo; ou seja, um sistema altamente confiável é aquele que atende à sua função em todas as vezes e sob todas as condições operacionais requeridas (JURAN, 1988, 1992).

De acordo com a definição do *Military Handbook 338* (1998), “confiabilidade é a probabilidade de um sistema não falhar sob determinadas condições de uso para as quais, em um intervalo de tempo definido, ele foi projetado”.

Para a ABNT (1981), “Confiabilidade é a capacidade de um item desempenhar uma função objetiva, sob condições especificadas, durante um intervalo de tempo”.

Segundo Bertsche (2008), uma vez que a definição de confiabilidade está relacionada à sobrevivência de um item ao longo do tempo, é possível, a partir da teoria da

probabilidade, obter seu valor a cada instante de tempo. A expressão matemática utilizada para isso é: $\text{confiabilidade} = 1 - \text{probabilidade de falha}$, em que confiabilidade é o complemento da ocorrência do evento gerador da falha.

□ Taxa de falha e quota de falha

A taxa de falha λ descreve o risco de uma peça falhar, se ela já sobreviveu até determinado tempo de operação t . A taxa de falha é determinada pela divisão do número de falhas em um período de tempo pela soma das unidades ainda intactas.

A quota de falha q especifica a mudança relativa no intervalo de tempo observado e serve como uma estimação da taxa de falha λ (BERTSCHE, 2008). Uma forma de se obter o q é pelo cálculo da probabilidade de falha podendo ser expressa em partes por milhão (*ppm*).

2.5.2 Confiabilidade como medida de risco em projetos

Ayyub et al. (2002) estabelecem um elo entre riscos, segurança e confiabilidade através das seguintes definições:

- Confiabilidade é um dos elementos do risco;
- Segurança é o julgamento da aceitabilidade do risco para a segurança do sistema.

Embora a confiabilidade seja independente de quem cause, do resultado da perda e de quem esteja exposto a ele, o risco, pelo contrário, depende de avaliação do resultado de perda e ganho para as pessoas ou equipamento envolvidos. Essa diferença entre confiabilidade e riscos é usualmente irrelevante para a avaliação de risco probabilístico, pois, em ambas as situações, o que se busca é reduzir o potencial de perdas para outras pessoas.

Nesse sentido, tanto um sistema de baixo risco quanto um componente ou sistema com alta confiabilidade são assumidos como sistemas de elevada segurança (LEE; McCORMICK, 2011).

Em geral, no âmbito do desenvolvimento de sistemas, dá-se mais atenção à redução de probabilidade da falha ou aumento da confiabilidade, porque ela oferece maior número de variáveis de sistemas que podem ser controladas pelos especialistas em gestão de riscos e, portanto favorecer que os requisitos de segurança do sistema sejam atendidos (AYYUB et al.,2002).

2.5.3 Metas de confiabilidade

O estabelecimento de metas de confiabilidade pode ser estabelecido de diversas formas como mostra (IRESON et al.,1995; BERSTCHE, 2008; KUMAMOTO, 2007):

1. Metas Arbitrárias

Esse tipo de meta não é desejável, mas ainda é muito utilizado, pois reflete o conhecimento dos especialistas e gestores sobre as condições pelas quais as insatisfações dos clientes se tornam um grande problema para o negócio da empresa (IRESON *et al.*,2005).

Outra característica dessas metas é que podem ser tanto qualitativas quanto quantitativas, como por exemplo: dobrar a confiabilidade do sistema para os próximos anos, taxa de falha acima de determinado valor não pode ser entregue ao cliente, custos de garantia e tempo de reparo do sistema devem ser menores do que determinado valor.

2. Metas baseadas nos requisitos de garantia do sistema

A política de garantia da adotada na organização e os indicadores de controle dos custos de garantia formam uma base razoável para a definição das metas de confiabilidade para o novo sistema. Nessa abordagem, a organização estabelece qual deve ser o nível de taxa de falha do novo componente, permitindo-lhe atingir a meta de custos de garantia. Através de um modelo matemático, são relacionadas diversas variáveis, como custo de produção, período de garantia, preço do sistema, custo de reparo do componente, entre outras, e, por meio de um procedimento de cálculo, obtém-se a taxa de falha do componente.

3. Metas de confiabilidade baseadas no desempenho de sistemas passados

No ambiente atual de desenvolvimento de sistemas, as atividades de substituição de um sistema atual por um novo, com maior complexidade e nível tecnológico, criam oportunidades para aumentar a confiabilidade dos sistemas e componentes envolvidos. A revisão dos dados de garantia, resultados de testes e tendências tecnológicas, fornece o guia básico para as propostas de metas de confiabilidade.

4. Metas baseadas na avaliação tecnológica

Em muitas situações, o conceito de uma nova peça ou componente baseia-se na compreensão sobre as tecnologias disponíveis. Nesse caso, se os dados e os parâmetros de modelos de confiabilidade empíricos são conhecidos, pode-se, então, realizar estimativas de confiabilidade com razoável precisão e credibilidade. O estabelecimento de metas de confiabilidade nessas condições pode ser feito através do uso de metodologias de avaliação tecnológica (BRAUN, 1998).

5. Metas de confiabilidade baseadas em faixas de risco de segurança

Nessa abordagem, o nível de risco é o ponto de partida para se chegar às metas de confiabilidade. A passagem entre esses dois pontos é feita por meio de técnicas da

teoria de probabilidade e de confiabilidade (AYYUB et al.,1999). Segundo Lee e McCormick (2011), metas para o gerenciamento de riscos podem ser especificadas em termos de medidas de confiabilidade.

Por ser o risco definido como a combinação da probabilidade de falha e suas consequências, assume-se que somente o grau de atendimento de confiabilidade ou probabilidade de falha seja uma definição de aceitação de nível de risco. A partir dessa definição, o grau de atendimento de confiabilidade pode ser usado para o desenvolvimento de especificações de projeto (AYYUB et al., 2002).

2.5.4 Consecução das metas de confiabilidade

Como uma meta de confiabilidade pode ser alcançada? Para Juran (2002), é mais fácil especificar uma meta de confiabilidade por meio de um nível máximo de falhas, ou um tempo médio entre falhas (MTBF), do que atingi-la. A dificuldade de atingir a meta ocorre nas fases iniciais do desenvolvimento do sistema, etapa em que se projeta o sistema para as condições de aplicação e operação que será submetido.

Juran (1992) ressalta que, quanto mais o projetista conhecer em profundidade o ambiente em que o sistema será utilizado, maiores serão as possibilidades de elaborar projetos com confiabilidade superior.

Nesse sentido, os gerentes de projeto têm tomado providências para prover maior garantia do alcance das metas de confiabilidade. Em algumas organizações, as políticas de qualidade exigem que os novos modelos de sistemas possam ser colocados no mercado somente se a sua confiabilidade for, no mínimo, igual àquela dos modelos que estão substituindo e também a dos modelos dos sistemas dos concorrentes.

Por outro lado, é muito comum observar que a confiabilidade real fica abaixo da confiabilidade planejada, ou seja, a confiabilidade alcançada no campo costuma ser

menor do que aquela planejada pelos testes em laboratório. Segundo Juran (1988), essa diferença entre teoria e prática decorre por conta de os modelos matemáticos e testes de laboratório não refletirem com precisão as reais condições de operação e aplicação.

Embora essas diferenças não possam ser eliminadas por completo, alguns passos podem ser dados para reduzir seus efeitos nocivos na confiabilidade. Um desses passos é envolver a participação de clientes, fornecedores, fabricantes e usuários, que serão impactados pelo projeto do sistema. Um passo mais abrangente é a identificação das tarefas específicas que devem ser executadas para alcançar a confiabilidade e atribuir as responsabilidades claras dos participantes em cada etapa do desenvolvimento do produto e construção (JURAN, 1992).

Essa questão é tratada por Ireson et al. (1995), sugerindo que o caminho mais eficaz de buscar uma alta confiabilidade é a realização de atividades relacionadas à garantia da confiabilidade durante o ciclo de desenvolvimento de sistemas. Para isso, devem ser estabelecidas medidas de caráter organizacional, como o estabelecimento de processos de qualidade preventiva com os respectivos responsáveis e patrocinadores dentro da organização, o que requer, em muitos casos, a criação de uma área para gerenciar as atividades de confiabilidade durante todas as fases de desenvolvimento de sistema.

Conforme indica O' Connor (2002, 2003), as atividades de garantia da confiabilidade se agrupam em cinco grandes blocos:

1. Especificação da confiabilidade;
2. Especificação dos requisitos do projeto para atender às metas da qualidade;
3. Planejamento dos testes;
4. Monitoramento da confiabilidade e fornecimento de *feedback*;
5. Projeto definitivo.

Para Dimitri (1991), engenharia de confiabilidade é um processo que fornece um conjunto de ferramentas que permite especificar, projetar, testar e demonstrar a probabilidade e a capacidade pelas quais peças, componentes, equipamentos e sistemas realizarão suas funções objetivas em determinado período de tempo, em condições de aplicação e com limites de confiança desejados, com ou sem falha.

Segundo Bertsche (2008) o processo de engenharia de confiabilidade estabelece um conjunto de atividades que compreende medição, análise, inspeção e verificação, que devem ser executadas desde as fases iniciais do projeto.

Para Ireson *et al.* (1995), embora tais atividades impliquem elevação dos custos de qualidade preventiva, ainda sim são mais baratas, quando comparadas aos custos de correção durante a produção e quando o sistema já está em operação. As atividades necessárias para assegurar a meta de confiabilidade do componente ou sistema devem estar integradas com as etapas do ciclo de desenvolvimento do sistema, formando um processo de engenharia de confiabilidade, como mostra a figura 2.5 (HAFFNER, 2005; BERTSCHE, 2008).

Figura 2-5- Processo de garantia da confiabilidade (adaptado de Jäger (2007))

Nesse processo, o propósito da etapa de planejamento é assegurar que as metas de confiabilidade reflitam o patamar de desempenho de segurança e funcionalidade que a organização busca para seus sistemas, e, por essa razão, deve seguir princípios que balizem o estabelecimento de metas. De acordo com Ireson *et al.* (1995), são quatro os princípios indicados para essa etapa:

- Metas cujos resultados forneçam o máximo de satisfação possível são as preferíveis;
- Preferências são dadas para resultados que são mais fáceis de serem atingidos;
- Preferências de desempenho são transitórias e mutuamente interdependentes;
- Existem muitas preferências sem importância.

2.5.5 Planejamento estatístico de testes de confiabilidade

Testes são usualmente muito caros e consomem muito tempo envolvendo atividades dificultosas durante o desenvolvimento de produtos e sistemas. O desenvolvimento de testes pode ser realizado para assegurar que projetos atendam os requisitos de desempenho quanto a segurança, durabilidade, confiabilidade, aspectos de regulamentação entre outros (NELSON, 1990).

Testes não são apenas um tema de engenharia, devido a importância e à magnitude dos aspectos econômicos e do negócio. Existe frequentemente pressão para reduzir testes devido ao alto custo envolvido, sem que seja feita apropriadamente a avaliação dos impactos dos efeitos no desempenho, a confiabilidade e nos custos. Testes devem ser baseados na filosofia de que poderia fornecer uma fundação para planejar todos os métodos e decisões relacionados aos testes de produtos e sistemas de engenharia (O'CONNOR, 2003).

Testes para estudo de confiabilidade são classificados de duas formas. A primeira o teste é realizado até a falha do sistema e o segundo até um determinado período de tempo sem a ocorrência de falha, e este é chamado de *sucess run*. Os testes *sucess*

run para demonstrar a especificação de confiabilidade de sistemas são conhecidos como planejamento estatístico de testes de confiabilidade (KROLO et al., 2002).

Uma das primeiras decisões para se tomar quando se desenvolve um programa de planejamento estatístico de testes de confiabilidade é determinar o tempo de duração e o tamanho da amostra de testes.

A expressão matemática que permite estimar tanto ferramenta estatística para determinar o tempo e o tamanho da amostra é a combinação da distribuição binomial combinada com a distribuição de *Weibull* (Anexo A).

A expressão matemática que combina a distribuição binomial com a distribuição de *Weibull* é dada pela equação (KLEYNER, 1996),

$$(1 - P_A) = \sum_{x=0}^k \binom{n}{x} \cdot R(t_i)^{n-x} \cdot (1 - R(t_i))^x \quad \text{eq.(2.1)}$$

onde,

P_A = Nível de confiança

x = Número de falha

n = Tamanho da amostra

$R(t_i)$ = Confiabilidade dos testes para determinado tempo t_i . Na condição de $x=0$ a expressão acima torna-se,

$$(1 - P_A) = R(t_i)^n \quad \text{eq.(2.2)}$$

Para obter a confiabilidade de testes R_i a eq.(2.2) fica,

$$R(t_i) = (1 - P_A)^{\frac{1}{n}} \quad \text{eq.(2.3)}$$

A equação (2.3) é também conhecida como *sucess run*.

A partir da equação (2.3) chega-se ao tamanho da amostra necessário para demonstrar determinada confiabilidade para um tempo t_i ,

$$n = \frac{\ln(1 - P_A)}{\ln(R_i)} \quad \text{eq.(2.4)}$$

Em geral esse conjunto de equações é aplicado para demonstrar a confiabilidade em testes sem falhas, porém verificam-se algumas limitações quanto sua adequação aos projetos que apresentam limitações orçamentárias para o programa de testes.

Limitações

- Amostras devem ser idênticas e testadas nas mesmas condições de aplicação. Exigência de difícil implementação e de elevados custos.
- Como se deseja obter a confiabilidade (meta) para um determinado tempo de vida requerido, o tempo de teste t_i deve ser igual a esse tempo de vida requerido t_s . Na prática $t_i \neq t_s$, pois testar produtos durante longos períodos de tempo geralmente ultrapassa o próprio período do projeto, e, portanto, torna-se pouco útil para melhoria do projeto.

Abordagem ampliada da técnica *sucess run*

Uma abordagem ampliada da técnica *sucess run* tem sido apresentada em artigos por um grupo de pesquisadores da Universidade de Stuttgart- Alemanha, conduzidos por Bernd Bertsche, que incorporam outras variáveis relevantes nas equações tradicionais *sucess run* afim de que essas possam produzir estimativas mais precisas considerando as restrições presentes nos programas de testes.

Na abordagem ampliada são utilizados tempos de testes e condições de aplicação diferentes e a confiabilidade demonstrada pode ser validada para um tempo objetivo

diferente do tempo de teste. Assim as limitações apresentadas na técnica *sucess run* tradicional podem ser superadas permitindo que se obtenham demonstrações de confiabilidade mais precisas.

Na sequência são apresentadas as variáveis que fazem parte da versão ampliada da técnica *sucess run*, conforme apresentado nos trabalhos de Krolo et al (2001;2002;2003), Bertsche (2008).

□ Razão de tempo de vida

Quando o tempo de duração dos testes t_t é diferente do tempo requerido t_s , utiliza-se o conceito de razão dos tempos de vida, em que a razão de t_t com t_s produz uma razão de tempos de vida L_v :

$$L_v = \frac{t_t}{t_s} \quad \text{eq.(2.5)}$$

L_v é obtida pela transformação algébrica das distribuições de confiabilidade de *Weibull* para o tempo de teste t_t e para o tempo objetivo t_s .

Distribuição de confiabilidade de *Weibull* para t_t ,

$$R(t_t) = e^{-\left(\frac{t_t}{T}\right)^\beta}$$

Distribuição de confiabilidade de *Weibull* para t_s ,

$$R(t_s) = e^{-\left(\frac{t_s}{T}\right)^\beta}$$

O logaritmo da razão das duas equações produz,

$$\frac{\ln R(t_t)}{\ln R(t_s)} = \frac{-\left(\frac{t_t}{T}\right)^\beta}{-\left(\frac{t_s}{T}\right)^\beta} = \left(\frac{t_t}{t_s}\right)^\beta = L_v^\beta \quad \text{eq.(2.6)}$$

o que permite relacionar $R(t_t)$, $R(t_s)$ com L_v ,

$$\ln R(t_t) = L_v^\beta \ln R(t_s)$$

E assim obter $R(t_t)$ em função da confiabilidade requerida $R(t_s)$ e razão dos tempos L_v ,

$$R(t_t) = R(t_s)^{L_v^\beta} \quad \text{eq(2.7)}$$

Se nenhuma falha estiver presente ($k=0$), a função da relação dos logaritmos pode ser representada por uma função de nível de confiança (MEEKER, 1998). Assim a obtenção da confiabilidade requerida em função do nível de confiança é feita através da substituição da equação (2.3) na equação (2.7).

$$R(t_s) = (1 - P_A)^{\frac{1}{L_v^\beta \cdot n}} \quad \text{eq(2.8)}$$

□ Fator de Teste

Os recursos de tempo e custos para a realização dos testes de confiabilidade são, na maioria das vezes, limitados; por isso, buscam-se constantemente alternativas para a redução do tempo dos ensaios.

Uma alternativa normalmente aplicada é a dos testes acelerados, constituídos para produzir um maior dano ao componente em um período de tempo mais curto, se comparado a uma condição normal de operação. Nesses casos, quando se pretende estimar o tempo de vida de um componente sob condições mais severas de testes, utiliza-se um fator de correlação entre essas duas condições, normal e acelerada.

Segundo Nelson (1990), esse fator é a razão entre o tempo de vida característico, determinado em campo T_f , e T_t , determinado no teste. O fator de aceleração é,

$$r = \frac{T_f}{T_t} \quad \text{eq.(2.9)}$$

Essa relação é válida apenas se o parâmetro de forma da distribuição da falha forem os mesmos dos observados no teste e no campo (NELSON, 1990; MEEKER, 1998).

Assumindo $T_f = T_s$, e isolando T_s , a equação (2.9) torna-se,

$$T_s = r.T_f \quad \text{eq.(2.10)}$$

Substituindo a equação (2.10) na equação (2.6), têm-se,

$$R(t_t) = R(t_s)^{n.(L_v.r)^\beta} \quad \text{eq(2.11)}$$

A confiabilidade requerida é obtida pela substituição a equação (2.3) na equação (2.11) chega-se a confiabilidade requerida $R(t_s)$ considerando o fator de correlação.

$$R(t_s) = (1 - P_A)^{\frac{1}{n.(L_v.r)^\beta}} \quad \text{eq.(2.12)}$$

□ Número efetivo de elementos da amostra

Essa técnica permite juntar as informações de diferentes tipos de testes, para a obtenção da confiabilidade de um componente. O número efetivo da amostra n_{eff} para o programa de testes completo é a somatória dos diferentes tipos de testes, seus respectivos tamanho de amostra n , fator de aceleração r e tempo de duração dos testes t_i . O valor de tempo t_s para atingimento da confiabilidade requerida é o único fator que não varia por tipo de teste, conforme mostra a equação 2.13, (HITZIGER, 2007):

$$n_{eff} = \sum_{i=1}^m \left(\frac{t_{t_i}}{t_s} \cdot r_i \right)^\beta \cdot n_i = \sum_{i=1}^m n_{eff} \quad \text{eq.(2.13)}$$

Através da amostra efetiva de todos os testes previstos no programa, pode-se determinar a confiabilidade para o tempo de vida planejado do componente ou sistema pela equação:

$$R(t_s) = (1 - P_A)^{\frac{1}{n_{eff}}} = (1 - P_A)^{\frac{1}{\sum_{i=1}^m \left(\frac{t_{t_i}}{t_s} \cdot r_i \right)^\beta \cdot n_i}} \quad \text{eq.(2.14)}$$

Essa equação é aplicada para uma condição de testes sem falhas (HITZIGER, 2007).

Transformando a equação (2.14), pode-se obter o tamanho de amostra efetiva para se chegar à confiabilidade requerida:

$$n_{eff} = \frac{\ln(1 - P_A)}{\ln R(t_s)} \quad \text{eq.(2.15)}$$

❑ Redução dos esforços de testes

Pela teoria clássica da probabilidade, o tamanho da amostra e o tempo necessário para demonstrar a confiabilidade de um sistema geralmente são muito elevados e, portanto, muito onerosos financeiramente. Porém, dentro do planejamento estatístico de testes, existe o recurso de reduzir esse custo através do uso de informações do desempenho passado de sistemas similares também os conhecimentos dos especialistas sobre os aspectos críticos do projeto.

Conforme apontam Krolo *et al.* (2002), o método que incorpora essas informações é o Beyer/Lauster. A principal vantagem desse método é a não exigência de uma distribuição *a priori*, mas apenas o valor de confiabilidade conhecido como R_0 . Segundo Beyer e Luster (1990, *apud* KROLO et al., 2002), a equação que permite a redução do tamanho da amostra para uma distribuição de *Weibull*, em uma condição de testes *sucess run*, é:

$$P_A = 1 - R^{n \cdot (L_v \cdot r)^\beta + \left(\frac{1}{\ln(1/R_0)} \right)} \quad \text{eq.(2.16)}$$

Resolvendo-a para o tamanho de amostra exigido para os testes, tem-se a equação:

$$n = \frac{1}{(L_v \cdot r)^\beta} \left[\frac{\ln(1 - P_A)}{\ln(R_0)} - \frac{1}{\ln(1/R_0)} \right] \quad \text{eq.(2.17)}$$

Isso significa que o tamanho de amostra exigido pode ser reduzido, considerando-se a informação *a priori*.

Estratégia de testes

A demonstração da confiabilidade requerida para um determinado sistema ou componente é feita a partir do programa de testes, porém é muito comum restrições de em termos de recursos e tempo, o que afeta diretamente o programa de testes para avaliação de confiabilidade.

O planejamento estatístico de testes permite adequar o programa de testes a partir de mudança dos parâmetros da equação (2.14);

t_{t_i} Tempo de duração dos testes

n_i Tamanho da amostra

r_i Fator de correlação

$$R(t_s) = (1 - P_A) \frac{1}{\sum_{i=1}^m \left(\frac{t_{t_i}}{t_s} r_i \right)^\beta \cdot n_i}$$

Duas estratégias podem ser estabelecidas para planejar os testes conforme figura 2.6:

Estratégia A	reduzir número de amostras	n
	→ umentar duração do teste	t_t
	→ teste mais severo: aumentar	r
Estratégia B	reduzir duração do teste	t_t
	→ teste mais severo: aumentar	r
	→ umentar nº de amostras	n

Figura 2-6- Estratégias de teste para os exemplos práticos

O intuito da estratégia A é reduzir o número de amostras, o que pode ser conseguido através do aumento da duração dos testes e do fator de aceleração que no caso é testar unidades em banco de provas ou condições mais severo daquela que o sistema

será operado. Essa proposta de estratégia é muito adotada em setores com forte restrição de protótipos de testes como o marítimo e aeronáutico.

Em situações em que há forte pressão de prazo de entrega do projeto, recomenda-se a redução da duração dos testes conforme indicada na estratégia B. Geralmente essa estratégia eleva os custos do projeto devido a necessidade de aumento das amostras de testes inclusive em banco de provas, mas mesmo assim tem sido muito utilizada em segmentos como o automotivo.

3 PROPOSTA DO MÉTODO

3.1 Introdução ao método proposto

O método proposto nesse trabalho é uma abordagem quantitativa com base no planejamento estatístico de testes de confiabilidade, e sua denominação liga-se a possibilidade de demonstrar quantitativamente a meta de confiabilidade dos componentes que impactam os objetivos globais de segurança com base no programa de testes para esse componente.

Esse método é composto de diversas etapas de análise, a partir das quais a meta global de segurança obtida pelo GBS é convertida em metas de confiabilidade dos componentes, em seguida o método recebe um tratamento estatístico a fim de demonstrar se essa meta pode ser atendida a partir do planejamento de testes previstos para o componente no projeto.

O objetivo da aplicação do método é verificar se os testes planejados podem demonstrar a confiabilidade requerida do componente. O valor de confiabilidade calculado pelo método pode ser usado para balizar o processo de tomada de decisão para aprovação do projeto, pois ele mostrará com certo grau de certeza se os recursos de testes planejados são suficientes, além de permitir que se verifique a qualidade do programa de testes nas fases iniciais do projeto, a fim de realizar os ajustes necessários para avaliações de confiabilidade.

3.2 Descrição do método proposto

O método proposto aplica-se aos níveis I e II da estrutura GBS. O conjunto de atividades do método está agrupado no bloco 2 da figura 3.1 onde é mostrado o modelo

completo de garantia das metas de segurança para um sistema projetado e construído com base na estrutura GBS.

O método proposto no presente trabalho consiste em seis macro etapas, onde são realizadas atividades que levam a demonstração das metas de confiabilidade para os componentes. Essas etapas são descritas abaixo:

Figura 3-1- Modelo de Abordagem Probabilística para o GBS

O método consiste em seis macro etapas, onde são realizadas atividades de análise da falha e de verificação do atendimento das metas de confiabilidade para os componentes, os quais em situação de falha podem prejudicar o atendimento das metas globais de segurança. Essas etapas são descritas abaixo:

1. Identificar os eventos indesejados que podem afetar a meta de segurança global. Nessa etapa, busca-se levantar o evento indesejado, o qual pode desencadear

acidentes. A identificação desse evento geralmente decorre de uma análise de traz para frente, ou seja, partindo-se do acidente para o evento que deu origem à ocorrência desse acidente.

2. Identificar falhas potenciais geradoras dos eventos indesejados. Essa etapa, divide-se em duas; Análise Crítica do Projeto e Identificação da falhas.
 - a. Na análise crítica do projeto o grupo de especialistas analisa cada parte do sistema, seu aspecto construtivo e funcional, levantando os pontos mais susceptíveis a falhas.
 - b. Após a compreensão detalhada do projeto do sistema, realiza-se um *brainstorming* procurando elencar as possíveis falhas que o sistema pode apresentar, assim como os subsistemas e componentes responsáveis por essas falhas, e avaliar se existe correlação com o evento indesejado.
3. Análise dos modos das falhas dos componentes. Nessa etapa, objetiva-se compreender o mecanismo da falha que se manifesta nos componentes e posteriormente, para se chegar aos modos de falha, isto é, à forma de manifestação da falha. Em componentes mecânicos esses modos são: quebra trínca, solto, desgastado, furado, outros. O FMEA estruturado é uma ferramenta recomendada para o trabalho de investigação do mecanismo da falha e pode ser usado nessa etapa.
4. Relacionar falhas e eventos indesejados. A ocorrência de um evento indesejado normalmente é consequência de sucessivas combinações de eventos de vários níveis: topo (indesejado), intermediário ou base. Uma forma de se construir o sequenciamento entre os eventos é por meio dessa técnica da árvore de falhas, o qual dispõe de conectores e simbologias que auxiliam na dedução lógica das falhas e eventos.
5. Estabelecer metas de probabilidade de falha para cada modo de falha dos componentes que geram os eventos base. Essa etapa fornece as bases para

uma análise quantitativa de risco, pois é nela que são atribuídos valores de probabilidade de falha para cada modo de falha dos componentes relacionados aos eventos base, os quais permitirão a elaboração de estimativas probabilísticas de ocorrência do evento topo. Os valores de probabilidade de falha objetivo podem ser definidos com base em análise de históricos de garantia.

6. Elaborar o plano de comprovação da confiabilidade, através do planejamento estatístico de testes. Essa etapa compreende:
 - a. Construir programa de testes, contendo o tipo de testes, tamanho da amostra, tempo de duração, fator de correlação;
 - b. Calcular o parâmetro de forma (beta) da função de confiabilidade;
 - c. Calcular o tamanho da amostra efetiva;
 - d. Calcular a confiabilidade e a quota de falha para o modo de falha do componente;
 - e. Construir o gráfico da evolução da estimativa da quota da taxa de falha ao longo do desenvolvimento do projeto;
 - f. Avaliar o nível de atendimento da meta de quota de taxa de falha em relação ao programa de testes atual;
 - g. Otimizar programa de testes buscando atender as metas de quota de taxa de falha.

As metas globais de segurança e os eventos inicializadores são etapas previstas nos GBS. O método proposto é aplicado somente na região delimitada pela linha tracejada, da figura 3.2, iniciando com o evento topo indesejada. Assim, assumindo que, nas análises com GBS, se verifique que o risco de perdas provocado por falha de um sistema esteja inicialmente na região vermelha no diagrama de Farmer, e que se deseja trazer esse risco para região verde (objetivo) no novo projeto, as atividades propostas no bloco 2 são aplicadas para estabelecer e assegurar o atendimento das metas de confiabilidade para os componentes que estão na base da árvore e que são responsáveis pelos eventos base.

A ligação entre o bloco 1 e o 2 é feita através do evento topo indesejado, conforme apresentado na figura (3.3). Essa figura também mostra a árvore de falha do sistema de pós-tratamento desdobrada até os quatro eventos base previstos, e que se aplicam a ambos os sistemas; automotivo e marítimo. Para a realização dos exemplos práticos é selecionado apenas um evento para cada exemplo. O critério de escolha dos eventos é apresentado em cada aplicação.

Figura 3-2-Sistemática de desdobramento das metas de segurança

4 EXEMPLOS PRÁTICOS

4.1 Aplicação Automotiva

4.1.1 Identificação do evento indesejado

A poluição atmosférica urbana se tornou um dos principais problemas ambientais da atualidade que afeta praticamente todas as grandes cidades do mundo como mostra a tabela 4.1.

Tabela 4-1- Poluição atmosférica no mundo [$\mu\text{g} / \text{m}^3$] (WORLD BANK,2007)

País	Cidade	População (milhares) (2005)	Dióxido de Nitrogênio 1995-2001	Dióxido de Enxofre 1995-2001	Material particulado 2004
Brasil	São Paulo	18,333	83	43	40
Chile	Santiago	5,683	81	29	61
Estados Unidos	Nova York	18,718	79	26	21
Inglaterra	Londres	8,505	77	25	21
China	Shangai	14,503	73	53	73
Japão	Tóquio	35,197	68	18	40
França	Paris	9,82	57	14	11
Índia	Delhi	15,048	41	24	150
Singapura	Singapura	4,326	30	10	44
Alemanha	Belim	3,389	26	18	22

Comparando os valores recomendados pela Agência Ambiental Europeia (EEA), a qual estabelece limites de $50\mu\text{g}/\text{m}^3$ de Material Particulado (MP), $40\mu\text{g}/\text{m}^3$ de NO_2 (Dióxido de Nitrogênio) e $125\mu\text{g}/\text{m}^3$ de SO_2 (Dióxido de Enxofre) (EEA, 1999), com os apresentados na tabela 4.1, nota-se que praticamente todos os grandes centros urbanos estão com valores próximos ou acima dos limites recomendados.

Para AUTODATA (2011), os meios de transporte são os principais responsáveis pela degradação do ar nessas áreas. Atualmente, isso vem sendo agravado pela forte

expansão das frotas nas grandes cidades. Segundo o Denatran (2012) só no Estado de São Paulo a frota de veículos cresceu mais de 100% entre 2000 e 2010, saltando de 10 para 20 milhões. Outro fator relevante é a lenta substituição dos veículos antigos por modelos menos poluentes, e pelo uso de combustíveis de baixa qualidade. Esse conjunto de fatores corrobora para a degradação do ar e consequentemente trazendo sérios prejuízos à saúde humana.

Segundo um estudo do Banco Mundial (WORLD BANK, 2007), a longa exposição das pessoas a altas concentrações de poluentes como fuligem, material particulado, dióxido de enxofre entre outros, traz consequências danosas à saúde, incluindo doenças respiratórias, como asma e câncer de pulmão, e doenças cardiovasculares. Segundo a organização mundial de saúde HWO (2011) morrem por ano mais de 1,3 milhão de pessoas por doenças relacionadas a poluição atmosférica.

No Brasil, a preocupação com a deterioração da qualidade do ar nas grandes metrópoles levou o Conselho Nacional do Meio Ambiente (CONAMA) estabelecer em 1986o PROCONVE, **P**rograma de **C**ontrol**e** da Poluição do Ar por **V**eículos Automotores, através da resolução nº18/86. O PROCONVE tem como objetivo reduzir continuamente as emissões de (NO_x) e material particulado (MP) através do estabelecimento de níveis de emissões cada vez mais restritivos que devem ser atendidos pelos fabricantes nos novos veículos (ROVERE et al., 2006).

Os níveis de emissões do PROCONVE possuem a nomenclatura (P1, P2, P3...), que equivalem à norma Euro adotada na Comunidade Européia. Atualmente os veículos comerciais a diesel comercializados no Brasil devem atender ao PROCONVE P5, equivalente ao Euro III. Um novo padrão o P7 entrará em vigor a partir de Janeiro de 2012 conforme determina a resolução CONAMA Nº 403, de 11 de novembro de 2008 (KREMER, 2009). Na figura 4.1 é mostrado o histórico de implantação das normas Euro na comunidade européia e suas respectivas graduações de redução.

Figura 4-1-Redução de emissão de poluentes [g/kWh] por normas Euro (adaptado de Mahr, 2002).

Para atender a esses novos limites melhorias foram introduzidas nos motores a diesel como o aumento da pressão de injeção do combustível e alteração da geometria dos pistões além, do desenvolvimento de novas tecnologias.

As duas principais tecnologias desenvolvidas para atender aos padrões P7 são a Redução Catalítica Seletiva (SCR) e a de Recirculação de Gases de Exaustão (EGR).

Nesse estudo o método proposto será aplicado às falhas apresentadas pelo sistema SCR visto que esse sistema tem sido amplamente adotado tanto no segmento automotivo quanto marítimo.

Independentemente da tecnologia, o propósito de qualquer uma delas é reduzir as emissões de MP, SO_x e NO_x e em especial a do NO_x para os limites estabelecidos pela legislação P7. Dessa forma, o evento indesejado considerado mais relevante pelo fato de ser um item de controle na legislação P7 é a emissão de NO_x acima do valor especificado. A figura 4.2 mostra os três principais eventos indesejados desse sistema com destaque para o evento selecionado para esse estudo.

Figura 4-2-Seleção do evento indesejado

4.1.2 Identificação das falhas potenciais

O SCR ou sistema de pós-tratamento dos gases de exaustão é assim conhecido por reduzir o NO_x fora da câmara de combustão, através da injeção de uma solução de água desmineralizada adicionada de 32,5% de uréia na saída dos gases de escapamento. A figura 4.3 ilustra o funcionamento sistema.

Figura 4-3-Configuração básica de um sistema SCR (adaptado de Gekas *et.al.* (2002))

Durante a combustão ocorre a emissão de dióxido de nitrogênio, óxido de nitrogênio e outros gases, a atuação do SCR é para reduzir as moléculas de NO_x através de um processo químico de redução catalítica (HELDEN et al., 2004). A solução aquosa à base de uréia (NH₂)₂CO, H₂O e outros elementos, conforme estabelecido na DIN 70070 e na ISO 22241 / 2008 e 2009, é injetada na tubulação de exaustão dos gases antes da entrada no catalisador por uma bomba dosadora controlada eletronicamente com base nas informações passadas pelos sensores de NO_x posicionados na saída do tubo de exaustão para a atmosfera.

Na primeira etapa do processo ocorre a hidrólise, que é a divisão de um composto químico pela reação com a água em elevadas temperaturas acima de 200°C (HELDEN et al., 2004) com isso a estrutura molecular da solução é separada formando moléculas de amônia (NH₃) e dióxido de carbono (CO₂). Na segunda etapa que ocorre na parte interna do reator catalítico é desencadeada a redução catalítica das moléculas de amônia NH₃ + NO_x através do contato com o material dos elementos catalíticos, produzindo moléculas de água e nitrogênio em uma temperatura entre 300°C e 400°C (DYRSCH; MOQVIST, 2009). A figura 4.4 ilustra as duas etapas do processo químico envolvido no sistema SCR.

Processo de conversão catalítica

Figura 4-4- Processo de conversão catalítica (adaptado de MAN, Diesel & Turbo (2010a))

A estrutura do reator catalítico usada em aplicações para tratamento de gases é monolítica (não porosa) e tem várias seções transversais unidas com canais na forma hexagonal ou quadrada (figura 4.5), e composta de materiais inertes como, o silicato de alumínio e magnésio $2\text{MgO} \cdot 2\text{Al}_2\text{O}_3 \cdot 5\text{SiO}_2$. Segundo Ericson (2007) esse tipo de estrutura fornece uma grande área superficial e impede grandes quedas de pressões que e por conseguinte afete o bom desempenho do motor.

Figura 4-5-Reator catalítico para aplicação SCR (adaptado de Ericson (2007))

A superfície dos canais da estrutura monolítica é coberta por um material poroso catalítico sendo os mais usados o dióxido de titânio (TiO_2), peróxido de vanádio (V_2O_5), tri-óxido de tungstênio (WO_3), tri-óxido de molibdênio (MoO_3), que vão exercer a função de adsorção dos gases do escapamento para transformá-los em gases inertes (ERICSON, 2007).

Segundo Silveira (2006), o vanádio é o responsável pela atividade na redução do NO_x , mas também na indesejável oxidação do SO_2 , por isso, mantém-se uma quantidade de vanádio geralmente baixa na presença de altas concentrações de SO_2 . O WO_3 ou o MoO_3 são empregados no intuito de aumentar a acidez da atividade e a estabilidade térmica do catalisador, assim como para limitar a oxidação do SO_2 . Esse sistema permite uma redução da emissão de NO_x em até 86% dos valores emitidos em 1990 (MAHR, 2002), desde que funcione adequadamente.

Por outro lado, mesmo sendo esse sistema comprovadamente eficaz para a redução do NO_x , seu alto desempenho somente é mantido a longo prazo desde que o diesel tenha teor de enxofre de no mínimo S50. Segundo a CNT (2011) sem tal condição os danos aos componentes internos do sistema são prováveis, com consequente comprometimento da função do sistema e do atendimento ao padrão P7. Nesse sentido, a resolução (ANP Nº 42 de 16 de dezembro de 2009) define a entrada em vigor do diesel S50 a partir de Janeiro de 2012 e o S10 em Janeiro de 2013 (KREMER, 2009; CNT, 2011).

Essa exigência decorre do fato do desempenho do sistema SCR ser extremamente sensível à variação da qualidade do diesel. Essa percepção é confirmada por um estudo realizado pela CNT (2008), qual demonstrou que a baixa qualidade do combustível é a principal causa de falhas no sistema de pós-tratamento de gases (SCR). Abaixo segue a relação das principais falhas apresentadas naquele trabalho:

- Corrosão dos sistemas;
- Formação de depósitos;
- Entupimento de catalisadores;

- Aumento da emissão de material particulado;
- Sobrecarga para o filtro de material particulado;
- Carbonização dos motores;
- Aumento no consumo de combustível;
- Aumento nas emissões;
- Pane por travamento de bomba de alta pressão e dos outros componentes, inclusive dosadores;
- Deficiência na funcionalidade do sistema de turbo-alimentação;
- Perda de durabilidade.

Outro estudo da CNT (2008) aponta que o enxofre é um elemento extremamente indesejável no diesel, pois, durante o processo de combustão ele se converte em tri-óxido de enxofre (SO_3) e este ao se juntar a água forma o ácido sulfúrico que contribui para a corrosão de partes metálicas do motor como mancais, guias de válvulas, tubulações entre outras.

Para a CNT (2008) e a TRANSPADATA (2011), as inovações tecnológicas de redução catalítica sem o uso de diesel de boa qualidade são insuficientes para que se alcancem alta confiabilidade nos sistemas e componentes envolvidos e atendimento duradouro aos limites de emissões impostos pela legislação.

☐ Análise dos dados de garantia do SCR no mercado europeu

Com base na análise dos dados de garantia dos veículos em operação no mercado europeu no período de 2006 á 2008 o SCR apresentou uma incidência de falha de 13,78%, ou seja, um valor extremamente elevado para qualquer sistema, quanto mais para um que tem a finalidade de garantir níveis de emissões dentro de patamares exigidos pela legislação.

O componente que mais contribuiu para a incidência de falha no SCR foi o dosador de uréia, atingindo 9,28%. O passo seguinte foi investigar se a falha afetava um lote específico ou se era encontrada em qualquer lote de veículos independente da sua data de produção. A resposta dessa investigação é essencial para se conhecer a categoria da falha; projeto, montagem, qualidade, ou operação do sistema.

O comportamento da incidência de falhas por lote de produção pode ser observada no gráfico 4.6. Nota-se um pico de incidência de falha de 29,6% no mês de produção de Dezembro de 2006 com vales antes e depois dessa data. No primeiro período que vai de Janeiro á Dezembro de 2006 somente 30% dos veículos produzidos estavam com a tecnologia SCR e isso é o que explica o baixo nível de incidência de falha, pois, logo que se atingiu a marca de 100% de veículos com SCR a taxa subiu para valores acima de 25%.

No período de Janeiro de 2007 á Dezembro de 2008 100% dos veículos produzidos já incorporavam a tecnologia SCR. A queda da incidência de falha até atingir o valor de 3% em dezembro de 2008 foi em função de inúmeras melhorias implementadas no dosador.

Figura 4-6-Incidência de falhas do dosador no período de 2006 a 2008

A análise dos dados mostra que a causa da falha não está relacionada a um problema no processo de produção, pois se o fosse, ela provavelmente estaria concentrada em um lote específico. Não sendo uma falha relacionada ao processo de produção a possibilidade que surge é que seja uma falha com origem no projeto, entretanto, a classificação precisa só pode ser determinada após a análise de outros aspectos do comportamento da falha como a distribuição das falhas.

Analisando a distribuição das falhas (figura 4.7) por faixa de quilometragem entre 0 e 50.000 e entre 50.000 e 100.000 constata-se que 70% de todas as falhas do dosador estão concentradas nesse período, indicando que se trata de uma falha que ocorre em baixas quilometragens, ou seja, é um tipo de falha prematura visto que pela política de garantia da organização espera-se que o componente não apresente falha até os 300.000km.

Figura 4-7- Falhas por faixa de quilometragem

Falhas que ocorrem com pouco tempo de uso em sistemas geralmente são classificadas como prematuras ou de infância e são associadas a problemas de montagem ou produção, porém, elas também podem ter origem no projeto na aplicação ou na operação do sistema (BORGES, 1979).

Nessa amostra de dados de falha analisado a indicação é de que existe falha de projeto, contudo, porém, essa confirmação apenas poderá vir depois da análise dos modos de falha e das respectivas causas raízes.

4.1.3 Análise dos modos das falhas dos componentes

Os modos de falha e as respectivas incidências de falha do componente dosador obtidos de dados de campo estão descritos na tabela 4.2.

Tabela 4-2-Principais modos de falhas do dosador

Descrição da falha	Qtde	Incidência (%)
Entupido/bloqueado	3.239	49,17%
Falha elétrica	1.526	23,17%
Não funciona	1.300	19,74%
Vazamento	522	7,92%

As análises da causa raiz do modo “entupido” apontaram para uma falha no projeto dos canais internos do dosador. O dosador tem a função de enviar quantidades pré-definidas de solução de uréia com determinada pressão para o bico injetor que está localizado na tubulação de escape, e, assim, assegurar que não haja excesso nem falta de ureia para reagir com os gases de escape, assim, se ocorrer entupimento dos canais internos do dosador poderá ocorrer a interrupção parcial ou total do envio de uréia para o injetor o e em pouco tempo afetará o alcance dos padrões de emissão de NO_x exigidos pela legislação.

Após análises adicionais verificou-se que as galerias internas ficavam entupidadas por cristais formados pela reação da solução de uréia com o material usado na construção do dosador. O fabricante realizou melhorias no projeto do dosador inclusive modificando o material da região dos canais. Assim, varias versões do dosador surgiram desde 2007 incorporando em cada uma delas alguma melhoria, até que no final de 2008 surgisse a versão definitiva usada até os dias atuais.

Porém, como o histórico de falhas do dosador foi crítico no mercado europeu surgiu a preocupação entre os engenheiros sobre qual seria o desempenho nas condições de aplicação brasileiras. Mesmo com as melhorias já incorporadas no dosador, havia ainda a preocupação de que devido as condições de operação no Brasil serem muito mais severas, quando comparadas ao mercado europeu, tanto no aspecto de aplicação quanto de operação esse item poderia apresentar defeito e, por essa razão decidiu-se testá-lo mais uma vez ,agora na aplicação brasileira.

4.1.4 Relação dos modos de falha com os eventos indesejados

Uma forma de reduzir a probabilidade de ocorrência do evento indesejado é através do aumento da confiabilidade dos componentes do sistema SCR. Para isso chegou-se, através da técnica da árvore de falhas aos eventos base e seus respectivos componentes cujo projeto deve assegurar alta confiabilidade. A figura 4.8 é a representação esquemática do resultado da análise da árvore de falha.

Figura 4-8-Árvore de falhas para o sistema SCR

Através do processo de dedução lógica combinado com simbologias e conectores, parte-se de um evento topo (indesejado) até se chegar aos eventos base que é onde nasce a ocorrência da falha que pode causar o evento indesejado. Para o dosador, foram identificados quatro eventos básicos como segue:

1. Solução de uréia não adequada,
- 2. Dosagem incorreta de uréia,**
3. Reator catalítico com baixa eficiência,
4. Falha no sinal eletrônico do sensor.

Para o evento dosagem incorreta de uréia, o componente responsável é o dosador e o modo de falha o “entupido”. Em uma análise completa de segurança de sistema às etapas de cálculo das quotas de falhas atuais e as respectivas metas devem ser realizadas para todos os eventos indesejados básicos, no entanto, como o propósito central desse trabalho é demonstrar a aplicação da técnica proposta, optou-se em aplicar o método para o evento de dosagem incorreta de uréia.

4.1.5 Estabelecimento da meta de quota de falha por modo de falha

Para esse estudo a meta de quota de falha para o componente dosador é o valor máximo de 10.000 *ppm* ou confiabilidade mínima de 99% para 500.000km. Esse valor foi definido com base nas diretrizes de projeto para itens de segurança, usados em uma empresa do setor automobilístico.

4.1.6 Demonstração da meta de quota de falha

A aplicação do método inicia-se com o estabelecimento da definição dos parâmetros dos testes e seus respectivos valores, conforme mostra a tabela 4.3:

Tabela 4-3-Parâmetros dos testes de planejamento estatístico

Parâmetro	Valor
Tempo de vida objetivo t_s	500.000 km
Quota falha q	10.000 ppm
Nível de confiança P_A	90%
Parâmetro de forma β	A definir
Tempo de teste em banco de provas (1) t_t	500h
Tempo de teste em banco de provas (2) t_t	750h
Tempo de teste de veículo em pista severa (3) t_t	40.000km
Tempo de teste de veículo em cliente (4) t_t	400.000km
Fator de aceleração r testes (1) e (2)	1000km/h
Fator de aceleração r testes (3)	10
Fator de aceleração r testes (3)	1

□ Cálculo do parâmetro de forma

O exato valor de β para o modo de falha de um componente não é conhecido entretanto, existem formas satisfatórias de se obter um valor estimado como as apresentadas por Nelson (1985):

1. Uso de dados históricos de sistemas similares;
2. Uso de parâmetros típicos, conhecidos pela indústria;
3. Assumir valores β em várias análises e compará-los os resultados das estimativas e limites de confiança.

Outra forma de se obter o parâmetro β é através de testes de banco de provas em que o sistema é submetido a um ciclo de cargas bem acima do requerido com o intuito de acelerar o surgimento de falhas (YAN et al.,2005). Nesse processo podem surgir

diferentes modos de falha, mas somente os modos de interesse é que têm utilidade para a estimativa da vida do novo sistema. Assim, se uma falha ocorrer durante o teste é preciso determinar se seu modo de falha corresponde mesmo ao parâmetro β .

Dessa forma com o auxílio de técnicas de estimativas de parâmetros como método da máxima verossimilhança (MLE), método dos mínimos quadrados e do papel de probabilidade de *Weibull*, uma razoável estimativa do verdadeiro valor de β pode ser obtida (NELSON, 1990; KROLO et al., 2002; YAN et al., 2005). Para este estudo, a estimativa do valor de beta é feita através do papel de probabilidade de *Weibull* com baseada nos dados de garantia dos veículos em operação na Europa.

A utilização de dados de garantia para a definição de estimativas de parâmetros de confiabilidade exige o conhecimento dos itens que falharam, assim como, as suspensões (unidades intactas) porém, em bancos de dados de garantia não constam as unidades suspensas sendo necessário estimá-las.

O processo de estimar dados suspensos segue o recomendado por Campean; Kuhn (2000), detalhado no Anexo B. De forma resumida, o método recomenda que para se obter a quantidade de unidades suspensas é preciso primeiramente delimitar o período da análise que se deseja e, em seguida, escolher um lote de unidades amostrais de testes de um determinado mês de produção. A partir daí somam-se todas as falhas que esse lote gerou durante o período da análise e, por fim, subtraem-se essas falhas do total de unidades produzidas no lote de produção selecionado.

Assim é possível obter a quantidade de dados suspensos. Porém, para obtenção das estimativas de confiabilidade é necessário a quilometragem dos dados suspensos, e, para isso, é usada a técnica de Campean; Kuhn (2000).

No exemplo prático o lote de produção escolhido para a contagem das falhas foi o de março de 2007, mês em que se produziram 2.408 veículos. Nesse período foram apuradas todas as falhas dos veículos das respectivas datas de produção até junho de

2010, as quais somaram um total de 510 falhas. Até o mês de censura foram 1898 suspensões e 510 falhas. A tabela 4.4 mostra as falhas por quilometragem sendo as suspensões estimadas pelo percentual recomendado por Campean; Kuhn (2000).

Tabela 4-4-Falhas e suspensões por faixa de quilometragem

Km x 10³	%	Suspensão	Falhas
0 - 20	1,50%	28	100
20 - 40	20,20%	383	130
40 - 60	27,1	514	91
60 - 80	25,3	480	58
80 -100	12,2	231	32
100 -120	5,6	106	28
120 -140	5,4	102	17
140 -160	2	38	17
160 -180	0,1	2	12
180 - 200	0,3	6	10
>200	0,3	6	15

A aplicação da técnica gráfica sobre os dados da tabela 4.4 possibilita estimar o parâmetro de forma. Essa técnica utiliza o conceito de *ranking* médio para calcular a probabilidade de falha F_i para cada faixa de quilometragem (Anexo A). As etapas resumidas do cálculo são estão descritas a seguir (BERTSCHE, 2008).

Rank médio $j(t_j)$ é igual ao *rank* anterior $j(t_{j-1})$ somado ao crescimento incremental $[n_f(t_j).N(t_j)]$, multiplicado pelo número de falhas no intervalo analisado:

$$J(t_j) = J(t_{j-1}) + [n_f(t_j).N(t_j)] \quad \text{eq. (3.1)}$$

O crescimento incremental $N(t_j)$ é dado pela equação:

$$N(t_j) = \frac{n+1-j(t_{j-1})}{1+(n-\text{número de unidades anteriores})} \quad \text{eq.(3.2)}$$

O número de unidades anteriores é a soma de todas as unidades suspensas mais às que falharam antes do intervalo em análise. A última etapa é o cálculo da $F(t_j)$ que é a média das estatísticas de ordem, esse valor é calculado usando a equação 3.3:

$$F_{\text{médio}}(t_j) \approx \frac{j(t_j) - 0,3}{n + 0,4} \cdot 100\% \quad \text{eq.(3.3)}$$

A tabela 4.5 mostra os valores de $J(t_j)$, $N(t_j)$ e $F_{\text{médio}}(t_j)$ para cada *ranking*, de 1 a 11.

Tabela 4-5- Valores consolidados para o cálculo da confiabilidade

Km x 10³	i	Ni	Ji	Fi [%]
0 - 20	1	1,01	101,2	4,19
20 - 40	2	1,22	259,33	10,76
40 - 60	3	1,72	415,47	17,25
60 - 80	4	2,92	585,09	24,29
80 -100	5	4,65	733,95	30,47
100 -120	6	6,6	918,74	38,15
120 -140	7	12,09	1124,2	46,69
140 -160	8	18,8	1443,84	59,96
160 -180	9	19,57	1678,62	69,72
180 - 200	10	23,09	1909,53	79,31
200>	11	31,98	2389,2	99,23

Conforme proposto por Berstche (2008) inserem-se os valores de $F_{\text{médio}}(t_j)$ no papel de probabilidades pela técnica de *Weibull*. Os parâmetros de forma β e de escala η da distribuição de *Weibull* podem ser obtidos conforme mostra a figura 4.9.

Figura 4-9-Papel de probabilidade de *Weibull* para o dosador.

O parâmetro de forma β encontrado é igual a 1,4 conforme demonstrado na figura 4.10.

□ Cenário 1- Cálculo da amostra efetiva

A partir dos valores de tempo de testes, fator de aceleração, razão dos tempos, tamanho da amostra e parâmetro de forma, é possível calcular a amostra efetiva.

No caso de quatro tipos diferentes de testes o n_{eff} é calculado separadamente para cada teste e depois somado para obtenção do n_{eff} total do programa de testes completo. Os valores calculados são apresentados na tabela 4.6.

Tabela 4-6-Programa de testes consolidado do dosador para calculo do n_{eff}

i	Tipo de Testes	Período de Testes (meses)	t_p	r	$L_{v,i}$	$L_{v,i} \cdot r$	$(L_{v,i} \cdot r)^b$	n_i	$n_{eff,i}$
1	Banco de Provas	(2 meses)	500 h	1000km/h	0,001	1	1,00	5	5,00
2	Banco de Provas	(3 meses)	750 h	1000km/h	0,0015	1,5	1,76	5	8,82
3	Veículo completo (Pista de Testes)	(12 meses)	40.000km	10	0,08	0,8	0,73	1	0,73
4	Veículo completo (Cliente)	(24 meses)	400.000km	1	0,80	0,8	0,73	1	0,73
									15,28

❑ Cálculo da confiabilidade

Inserindo o valor de amostra efetiva $n_{eff} = 15,28$ do programa de testes na equação de (2.14), obtêm-se o valor de $R(t_s)$:

$$R_s(500000) = (1 - 0,9)^{\frac{1}{15,28}} = 86,01\%$$

❑ Cálculo da quota de falha

A probabilidade de falha é $= 1 - 86,01\% = 13,99\%$. Isso significa uma quota de falha de 139.854 ppm. No gráfico 4.10, tem-se comportamento da taxa de falha durante os 30 meses de realização do projeto.

Figura 4-10-Evolução da taxa de falha ao longo do projeto

Observa-se, na figura, um grande afastamento da linha da quota de falha calculada (vermelha) em relação à linha da meta (azul), indicando que, durante o período do projeto, os testes planejados não foram suficientes para confirmar se o dosador tem condições de apresentar uma taxa de falha próxima a meta.

❑ Esforço de testes teoricamente necessário para se alcançar meta

A fim de orientar o ajuste do programa de testes na busca de um valor de quota de falha próximo à meta de 10.000 *ppm*, o valor de n_{eff} é calculado teoricamente com o $R(500.000) = 99\%$, $P_A = 90\%$. Aplicando a equação (2.15), têm-se:

$$n_{eff} = \frac{\ln(1-0,9)}{\ln(0,99)} = 229$$

❑ Proposta de aumento dos esforços de testes

Uma forma de aproximar a amostra efetiva dos testes com ao valor teórico é através do aumento de n . O aumento dos n de cada um dos testes segue restrições de recursos

do projeto. Para esse estudo procurou-se aumentar mais o n dos testes de banco de provas devido à empresa ter disponibilidade em oferecer um número elevado de celas de testes. Para veículos, como é necessário construir protótipos o que é considerado um custo muito elevado, o aumento do número de amostras foi menor quando comparado aos bancos de provas. A proposta simulada segue a seguinte configuração:

1-Banco de provas 1 - de 5 para 28

2-Banco de provas 2 - de 5 para 30

3-Veículo completo para pistas de testes - de 1 para 8

4-Veículo completo em uso no cliente - de 1 para 20

❑ Cenário 2- Cálculo da amostra efetiva

Tabela 4-7-Programa de testes consolidado com aumento das amostras

i	Tipo de Teste	Período de Testes (meses)	t_p	r	$L_{v,i}$	$L_{v,i} \cdot r$	$(L_{v,i} \cdot r)^b$	n_i	n_{eff}
1	Banco de Provas	(2 meses)	500 h	1000km/h	0,001	1	1,00	28	28,01
2	Banco de Provas	(3 meses)	750 h	1000km/h	0,0015	1,5	1,76	30	52,91
3	Veículo completo (Pista de Testes)	(12 meses)	40.000km	10	0,08	0,8	0,73	8	5,85
4	Veículo completo (Cliente)	(24 meses)	400.000km	1	0,8	0,8	0,73	20	14,61
									101,41

O novo valor de $n_{eff} = 101,41$.

❑ Cálculo da confiabilidade

A confiabilidade para o novo valor de $n_{eff} = 101,41$ é,

$$R(500000) = (1 - 0,9)^{\frac{1}{101,41}} = 97,76\%$$

❑ Cálculo da quota de falha

A probabilidade de falha é de 2,24% o que significa uma quota de falha de 22.450 ppm. A redução da taxa de falha durante os 30 meses da duração do projeto é mostrada no gráfico 4.11.

Figura 4-11-Redução da quota de falha após aumento do esforço de testes

Conforme indica a figura 4.11, o valor da quota de taxa de falha sofreu forte redução com o novo esforço de testes mostrando que o custo financeiro desse esforço pôde ser compensado pela aproximação da taxa de falha do componente dosador em relação à meta.

❑ Comparativo da quota de falha entre os cenários 1 e 2

Enquanto no cenário 1 a quota de taxa de falha calculada foi de cerca de quatorze vezes o valor da meta, no cenário 2 ela caiu para duas vezes, como ilustrado na figura 4.12, reduzindo com isso o nível de incerteza sobre o desempenho insatisfatório do componente dosador.

Figura 4-12- Comparativo entre a meta de quota de falha e os cenários 1 e 2.

Dessa forma, foi possível melhorar a qualidade decisão, com a maior precisão nas informações do desempenho do componente ao longo do tempo reduzindo assim, a incerteza associada ao atendimento da meta de confiabilidade.

☐ Redução do Esforço de Testes

A simulação apresentada no cenário número 2 mostra que o nível de atendimento da meta da confiabilidade pode ser aumentado durante o desenvolvimento do projeto caso haja ampliação dos esforços de testes o que, em outras palavras, significa mais recursos para a sua realização. Porém, esses recursos adicionais nem sempre podem ser disponibilizados para o projeto devido à restrição de tempo, pessoal, recursos financeiros, entre outros, aos quais o projeto está submetido.

Uma alternativa é reduzir o esforço de testes no cenário 2 sem alterar a quota de taxa de falha, e por meio de informações a priori. Nesse caso, o método de Beyer/ Lauster pode ser aplicado.

Adotou-se para confiabilidade a priori o valor de 97% para 500.000km. Através da equação de Beyer/Lauster equação (2.17) chegou-se ao valor da amostra efetiva $n_{eff} = 69$ que, sendo menor do que os $n_{eff} = 101,41$ calculados inicialmente para esse cenário demonstra a utilidade das informações a priori na redução dos custos dos testes.

4.1.7 Aplicação da Metodologia de análise de risco com base no FMEA

Uma empresa do setor automotivo aplica a metodologia de risco com base no FMEA há mais de cinco anos. Para o dosador essa metodologia foi aplicada e um resumo das etapas previstas no método é apresentado a seguir.

Com apoio de um aplicativo computacional desenvolvido pela própria empresa a metodologia de risco com base no FMEA calcula o risco com base nos fatores do NPR, ao quais valores foram atribuídos por um grupo de especialistas.

Para a severidade (S) cujo valor maior na escala significa maior gravidade do efeito da falha para aspectos de segurança, que para nesse estudo é o NO_x acima dos limites especificados pelos padrões P7, atribuiu-se 8,74.

Para a ocorrência (O) o grupo atribui o valor 7 que na escala das probabilidade de ocorrência esta associado a uma probabilidade de falha de 10.000 *ppm*. No caso da detecção (D) o valor foi de 8,34, pois, não se planejou testes para o componente por entender que ele já estaria maduro e, portanto, menos suscetível a falhas.

Os valores usados para cada critério foram obtidos com base na tabela 2.2 nela estão somente os números inteiros, as casas centesimais são do aplicativo usado em uma empresa do setor automotivo.

Através da multiplicação dos fatores chega-se ao $NPR = 7 \times 8,74 \times 8,34 = 510$. Esse valor no início do projeto foi considerado extremamente alto, para reduzi-lo os especialistas propuseram estabelecer ações para diminuir o risco através da variável detecção (D), pois, para agir na probabilidade de ocorrência dos modos de falha (O) seria preciso modificar aspectos construtivos do componente o que não seria uma alternativa em um primeiro momento uma vez que o componente é o mesmo utilizado atualmente no mercado europeu, o que significa que já contém as mais recentes melhorias de projeto, e para o fator (S) a classificação de consequência não é recomendável alhear, pois, é intrínseca a função do componente que caso falhe poderá produzir emissões acima do permitido com consequente prejuízo a saúde das pessoas.

Assim, foi estabelecido um cronograma de testes para aumentar o índice de detecção (D) para reduzir o NPR. Esse cronograma contém duas propostas de testes, que se diferenciam apenas na data de início dos testes de bancada de motores, conforme mostrado na figura 4.13.

Figura 4-13-Cronograma dos testes para o dosador

A proposta de antecipação dos testes é para evitar que a curva de risco planejada permaneça na região crítica até os 12 primeiros meses do início do projeto, situação essa indesejada, pois caso haja necessidade de alteração do projeto não haverá tempo suficiente para testar novas modificações. Com a inserção das informações do cronograma figura (4.13) e das opiniões dos especialistas no aplicativo chegou-se ao

valor de $NPR = 7 \times 8,74 \times 1 = 62$. A variação do NPR ao longo do projeto é mostrada na figura (4.14).

Figura 4-14-Curva de risco para o dosador

Porém como previsto a curva de risco com o cronograma original deixou a região crítica (vermelha) somente no mês oito, atingindo a meta de 62 NPR no mês onze. Com a antecipação dos testes a curva deixou a região vermelha no mês três alcançando a região verde no mês onze. Apesar da antecipação do atingimento da meta de NPR em um mês, o maior ganho foi em relação ao menor tempo para que o componente deixasse a região de alto risco. Segundo os especialistas da empresa as análises qualitativas muito mais que as quantitativas têm permitido que falhas de projeto fossem identificadas e solucionadas durante o desenvolvimento do sistema, gerando economia em custos de garantia além de preservar a reputação da imagem da marca. Por outro lado seu uso para dar suporte a tomada de decisão no nível gerencial tem apresentado fragilidades. Entre elas, destacam-se as dúvidas sobre a eficácia do método, por não oferecer uma medida de erro e com isso não permitir uma avaliação de quanto se pode confiar no resultado. Como o cálculo é obtido através de opinião de especialistas, é intrínseco a esse processo a presença de incertezas e, dessa forma, pode haver distorções no resultado do cálculo que o método não identifica.

4.1.8 Análise dos resultados

Antes de iniciar a comparação do método ressalta-se que o autor desse trabalho participou junto ao grupo de especialistas na aplicação da metodologia de risco com base no FMEA e, depois usando as mesmas informações de testes e de projeto usados nessa análise, aplicou-as no método proposto de planejamento estatístico de testes a fim de que fosse possível a comparação dos resultados. Na comparação dos dois métodos (figura 4.15), constata-se que os resultados não indicam a mesma direção para tomada de decisão.

Figura 4-15-Comparativo do resultado da aplicação das técnicas

Analisando os resultados verifica-se que enquanto a metodologia de gestão de risco baseada no FMEA apresenta um NPR de 62 apontando um caminho de baixo risco e, portanto, sinal verde para seguir adiante no projeto, a metodologia de planejamento estatístico de testes de confiabilidade sinaliza cautela quanto a conceder o sinal verde, devido sua quota de taxa de falha ser 14 vezes superior à meta (cenário I) o que dificultaria a aprovação do projeto.

O resultado desse comparativo foi apresentado à equipe de especialistas da empresa que somente aplica a metodologia com base no FMEA a fim de que pudessem avaliar qual metodologia deveria ser usada para melhorar a qualidade das decisões, visto que a metodologia atual tem sido severamente contestada no processo de aprovação de projetos.

Um argumento utilizado para auxiliar nessa escolha foi verificar o método que ofereceu uma medida de erro sobre os resultados apresentados, para mensurar a incerteza existente em qualquer análise que envolva previsão do desempenho futuro de um componente ou sistema. Nesse sentido, o método de planejamento estatístico forneceu uma informação de erro, representado pelo número de vezes em que o valor calculado ficou acima do valor da meta, e, por essa razão foi compreendido e aceito pela equipe com uma ferramenta mais completa.

4.2 Aplicação Marítima

4.2.1 Identificação do evento indesejado

O setor de transporte marítimo é considerado uma das principais fontes de poluição atmosférica. Pesquisas apresentadas por Cobertt et al. (2007) indicam que anualmente, esse segmento emite entre 1,2 e 1,6 milhões de toneladas de material particulado (MP), com diâmetros de 10µm ou menores, de 4,7 a 6,5 milhões de toneladas de Óxido

Sulfúrico (SO_x), e de 5 a 6,9 de Óxidos de Nitrogênio (NO_x). Outros estudos estimam que 60% de toda emissão global de SO_x é originada em transporte de carga, assim como, 15% de todo NO_x emitido pela ação humana sendo que quase 40% do total de emissão de NO_x vem do transporte marítimo e 70% se concentram em até 400 km do continente tornando os navios uma fonte poluidora das regiões costeiras (GOLDSWORTHY, 2010).

Essa quantidade de poluente despejado na atmosfera está relacionada ao tipo de propulsão das embarcações conforme aponta um estudo realizado por Corbett e Koehler (2003). Nesse estudo levantou-se a frota mundial de navios mercantes acima de 100 GT (toneladas brutas), os quais correspondem ao universo de 88.660. Esses navios estavam equipados com 116.280 motores produzindo 280.100MW, sendo 67% de motores de quatro tempos e 26% de dois tempos, ambos movidos a óleo combustível pesado (HFO) e 7% distribuídos entre gás, gasolina e outros tipos de propulsões.

O estudo também mostrou que o tipo de motor mais poluente é o de dois tempos. Essa conclusão veio após a verificação de que do total de motores 84.000 eram de quatro tempos e geravam 109.000 MW, e 27.000 de dois tempos 164.000MW. Como a potência instalada é o fator preponderante para emissão de poluentes os motores de dois tempos nessa amostra apesar de estarem em menor número é o maior emissor de poluição.

Estudos realizados sobre as emissões de poluentes (MOXIM et al., 1996; CORBETT; KOEHLER, 2003) apontam por uma lado que os motores movidos a óleo pesado estão entre os mais eficientes, e, por outro, que são uma fonte significativa para a poluição do ar e um fator de contribuição para impactos à saúde das pessoas e para mudanças climáticas globais.

Nos últimos anos pesquisas estabeleceram consistentes elos entre poluição do ar e prejuízos à saúde (CORBETT et al., 2007; GOLDSWORTHY, 2010). Ambientes com

alta concentração de material particulado (MP) estão relacionados a um grande número de doenças respiratórias, incluindo asma e câncer de pulmão e, de doenças cardíacas, como infarto (CORBETT et al., 2007). O MP com diâmetro menor que $2,5\ \mu\text{m}$ é um fator de aumento da mortalidade prematura devido sua capacidade de atingir as porções mais inferiores do trato respiratório, prejudicando as trocas gasosas e, por isso, ele vem sendo associado ao aumento do câncer de pulmão nas populações expostas a essa fumaça. Estudos recentes estimam aproximadamente 800 mil mortes por ano em ambientes expostos a MP menores que $2,5\ \mu\text{m}$, ou 1,2% das mortes prematuras globais por ano (COHEN et al., 2005).

❑ Controle das emissões

No sentido de reduzir o impacto da poluição emitida pelo transporte marítimo na saúde das pessoas a comunidade internacional e os órgãos de classe entre eles a IMO, iniciaram discussões para a definição de padrões de emissões mais restritivos para controle do SO_x e o NO_x (MAN DIESEL&TURBO,2010a).

Em maio de 1997 foi divulgado pela IMO na Convenção Internacional para Prevenção da Poluição Marítima Emitidas por Embarcações (MARPOL) 73/78, Anexo VI, definindo os limites de emissão de óxido de enxofre (SO_x) e óxidos de nitrogênio (NO_x), porém esses limites somente entraram com força de lei no ano de 2005 (IMO,2010).

Para o NO_x os padrões seguem uma escala que vai do Tier I ao III; quanto maior o valor mais restritivas são as emissões (IMO,2010). O Tier I foi estabelecido em 1997 enquanto que os padrões II e III em 2008. De acordo com a IMO (2010 os motores fabricados antes de 2000 devem atender ao padrão I sendo que o padrão II estabelece novos limites para motores fabricados a partir de janeiro de 2011, e o padrão III a partir de Janeiro de 2016 (figura 4.16), válidos inicialmente nas áreas de controle de emissões (ECA's) essas áreas compreendem regiões na costa dos Estados Unidos, Japão, países da Europa, onde há elevado tráfego de embarcações de grande porte, e, portanto, maior concentração de poluentes.

Figura 4-16-Cronograma de implementação dos limites de NOx (adaptado de IMO (2008))

Outra mudança é a dos limites globais de enxofre (S) no óleo combustível marítimo para reduzir as partículas finas de material particulado (GOLDSWORTHY,2010). Os padrões atuais de enxofre passarão de 4,5% para 3,5% a partir de Janeiro de 2012 com redução progressiva até 0,5% em Janeiro de 2020. Os limites de controle para ECA's são ainda mais rigorosos partindo dos atuais 1,5% para 1% a partir de julho de 2010 com meta de queda para 0,1%, a partir de Janeiro de 2015 (IMO, 2010).

Os limites de enxofre e as respectivas datas de introdução são apresentados na figura 4.17.

Figura 4-17-Cronograma de implementação dos limites de emissão de SOx (adaptado de IMO,(2010))

Um resumo das principais datas de introdução dos padrões de emissões de poluentes e de enxofre no diesel é apresentado por Goldsworthy (2010):

- 2005 - Nível I de NO_x para motores fabricados a partir de 2000;

- 2010 - Máximo de 1% de enxofre no diesel nas áreas de controle de emissões (ECA's);
-
- 2011 - Nível II de NO_x para novos motores;
- 2012 - 3,5% de enxofre no diesel global;
- 2015 - 0,1% de enxofre no diesel;
- 2016 - Nível III de NO_x para novos motores nas ECA's;
- 2020 - 0,5% de enxofre no diesel global.

Assim como na aplicação automotiva, na marítima o NO_x é um gás que se busca controlar devido as altas concentrações observadas no setor, o que pode conforme demonstrado trazer sérios prejuízos à saúde das pessoas.

Por essa razão o evento indesejado que se quer evitar é a emissão de NO_x acima dos limites especificados pelos padrões estabelecidos pela Marpol.

4.2.2 Identificação das falhas potenciais do sistema e o modo de falha

As tecnologias atuais para redução do NO_x agem de duas formas: na redução da temperatura da câmara de combustão ou no tratamento dos gases após a saída do motor (GOLDSWORTHY, 2005). Algumas dessas tecnologias são apresentadas a seguir (MAN DIESEL & TURBO, 2010a).

As tecnologias atuais para redução do NO_x agem de duas formas: na redução da temperatura da câmara de combustão ou no tratamento dos gases após a saída do motor (GOLDSWORTHY, 2005). Algumas dessas tecnologias são apresentadas a seguir (MAN DIESEL & TURBO, 2010a).

❑ Ajustes no Motor

São efetuados ajustes na combustão por meio de geometrias específicas dos bicos injetores também pelo aumento na pressão de injeção do diesel e pela maior eficiência nos turbos compressores. Essa solução traz redução de 20% na emissão de NO_x .

❑ Injeção de emulsão de água

Nessa solução a redução do NO_x é decorrente da injeção de água na câmara de combustão provocando a redução do pico máximo de temperatura no processo de combustão por evaporação da água, resultando na melhor atomização do combustível e consequente diminuição da emissão de NO_x . O uso de emulsão ou injeção direta de água pode reduzir entre 20 e 50% o NO_x .

❑ Método do ar umedecido (HAM)

Esse método modifica o ar utilizado na combustão através da adição de vapor d'água. Com a mistura atinge-se 70% de redução de NO_x .

❑ EGR (Sistema de Recirculação dos Gases de Exaustão)

É um sistema com o mesmo princípio do HAM, ou seja, modifica o ar de admissão porém, nesse caso pela reutilização de parte dos gases de exaustão que através de uma tubulação inserida no coletor de escape retorna para a entrada do coletor de admissão de ar do motor passando por um radiador para reduzir a temperatura. Assim, gases com nível mínimo de oxigênio são misturados ao ar limpo da admissão e, com isso, aumenta a capacidade calorífica de carga do cilindro reduzindo assim o pico de temperatura na câmara de combustão e alcançando em até 70% na redução de NO_x .

❑ SCR (Redução Catalítica Seletiva)

Também conhecido como Sistema de Pós-Tratamento de Gases de Exaustão, possui o mesmo princípio de funcionamento apresentado na seção anterior para o caso automotivo. Do ponto de vista de redução do NO_x o SCR é o que alcança os melhores índices, acima de 95%. Também conta a seu favor o impacto na economia de combustível que é de ca 2 g/KWh na escala de consumo de combustível específico em ensaios de banco de provas (BSFC) – escala adotada pela IMO para a certificação de motores (SCHMID; WEISSER, 2005).

A comparação dos sistemas em relação à capacidade de redução do NO_x e ao consumo de combustível estar representada na figura 4.18:

Figura 4-18- NO_x e consumo de combustível para várias tecnologias (adaptado de Schmid; Weisser 2005)

Embora o sistema SCR seja preferível quanto ao critério de desempenho técnico ele tem custo de aquisição mais alto em relação às outras tecnologias. Isso ocorre principalmente pelo uso da uréia e do custo de instalação. Apesar disso é a tecnologia

preferida para atender ao nível III e em operar embarcações em regiões de legislação ambiental restritiva como as ECA's.

O sistema SCR já é conhecido pelos fabricantes de motores de grande porte desde a década de 70 sendo usado desde essa época em aplicações industriais para a geração de energia. Mas, foi somente nos últimos anos que ele passou a ser empregado em aplicações marítimas (GOLDSWORTHY, 2005).

O funcionamento do SCR é basicamente o mesmo já apresentado o que difere são as características construtivas dos componentes e os parâmetros de funcionamento, também na aplicação marítima temperatura exerce papel central para a eficiência do sistema (MAN DIESEL& TURBO, 2010a). Na figura 4.19, tem-se um *layout* típico do SCR em um sistema de propulsão marítima:

Figura 4-19-*Layout* típico de um sistema SCR em uma aplicação marítima (adaptado de MAN DIESEL & TURBO 2010 ab)

Para obtenção de alta eficiência na conversão catalítica da aplicação marítima um dos desafios de projeto é manter a temperatura de entrada no reator SCR na faixa entre 300 °C e 400 °C (MAN DIESEL& TURBO, 2010a). Isso é necessário devido a redução de NO_x estar diretamente associada a condição de temperatura no componente reator.

O reator é constituído de vários blocos cataliticamente ativos com grande número de canais paralelos (figura 4.5). O diâmetro desses canais tem influência no gradiente de pressão e no tempo de saturação de impurezas no canal. Por essa razão o diâmetro é otimizado segundo a velocidade da saturação dos gases de exaustão e o gradiente de pressão do reator. Nesse sistema a temperatura é uma característica crítica pois, se for muito alta o NH₃ queimarão ao invés de reagir com o NO_x, e se for muito baixa a taxa de reação também será muito baixa e por conseguinte haverá condensação de sulfatos de amônia, o que entupirá o reator. Esse tipo de defeito provoca o mau funcionamento do SCR até sua completa parada (MAN DIESEL& TURBO, 2010a).

Além dessa questão outras análises apontam que mesmo com a temperatura dentro dos limites recomendáveis os sulfatos de amônia podem surgir através do baixo nível de pureza da uréia e da alta concentração de enxofre e vanádium no óleo combustível pesado (HFO).

Contudo, o componente crítico susceptível a falha é o reator catalítico e o modo de falha principal é entupimento dos canais do reator.

4.2.3 Relação das falhas com os eventos indesejados

Na aplicação marítima utiliza-se a mesma árvore de falhas da aplicação automotiva, havendo diferenças apenas nos eventos básicos analisados, neste caso, o reator catalítico (figura 4.20). A escolha desse componente baseou-se no resultado de alguns testes do sistema SCR em aplicações marítimas realizados por fabricantes de motores (MAN DIESEL& TURBO, 2010a).

Figura 4-20-Árvore de falhas para o sistema SCR

4.2.4 Estabelecimento da meta de taxa de falha q por modo de falha

Neste estudo os dados sobre o projeto do sistema SCR foram extraídos de relatórios técnicos publicados e disponibilizados por empresas do setor e complementados com artigos e outras publicações sobre o tema. No entanto, informações mais detalhadas sobre os parâmetros dos testes não foram encontradas nesses relatórios e nem disponibilizadas por outras fontes. Diante disso foi necessário fazer algumas suposições e assumir valores sobre os parâmetros dos testes com o intuito de mostrar como seria a execução do planejamento estatístico em uma aplicação marítima.

Em relação à expectativa de vida do sistema SCR a tentativa inicial foi obter essa informação dos fabricantes de motores marítimos que estão trabalhando no

desenvolvimento do SCR, mas isso também não foi possível devido à confidencialidade do projeto. Outra tentativa foi buscar na literatura estudos sobre o sistema SCR em aplicações marítimas. Pesquisas bibliográficas foram realizadas, mas nenhum estudo de taxa de falhas do SCR foi encontrado.

Uma possível explicação para isso é que esse sistema ainda é pouco utilizado nas embarcações e estudos específicos ainda estão no âmbito dos centros de desenvolvimento de algumas empresas e estas por sua vez, não desejam divulgá-los nesse momento, pois estão em plena preparação dos sistemas para atender aos índices de emissão do Nível III estabelecido pela legislação MARPOL (IMO, 2010) e que entrará em vigor em 2016. Para evitar que os valores de desempenho do sistema SCR na aplicação marítima fossem arbitrariamente adotados sem qualquer embasamento factual que refletisse, mesmo que parcialmente o estado real de aplicação, foram pesquisados na literatura estudos sobre o sistema SCR na aplicação industrial.

Entre os estudos considerados está o trabalho de Rubin et al. (2004) que aborda as inovações tecnológicas para a redução do NO_x em instalações industriais de geração de energia, destacando a tecnologia SCR na obtenção dessa redução. Quanto às taxas de falha foram considerados os dados fornecidos pelo trabalho de Kiriya (2001).

❑ Determinação da expectativa de vida do sistema SCR

A primeira suposição em estabelecer a expectativa de vida mínima aceitável para o reator catalítico. O primeiro passo foi levantar o perfil de operação dos motores. O sistema SCR tem aplicação em motores estacionários e marítimos por isso, foi pesquisado o tempo em que o motor fica em operação em horas/ano para ambos os casos.

Segundo Hafner (2008) nos motores estacionários estima-se cerca de 7.300 horas/ano, enquanto que para navios graneleiros o tempo médio está em 6.500 horas/ano (tabela 4.8), com expectativa de vida está entre 20 e 30 anos.

Tabela 4-8-Perfil de operação dos motores navais (CORBETT; KOEHLER, 2003)

Tipo de barcos	Tipo de motores	Horas de operação média por ano	Carga média do motor % da potência instalada
Navios graneleiros e tanques	Dois tempos:91% Quatro tempos:6%	6.500	55% taxa de frete se for baixa e 80% se for normal
Grandes Navios Containers (> 1.500 TEU)	Dois tempos:100%	6.700 - 7.200	80%
Pequenos Navios Containers(< 1.500 TEU)	Dois tempos:55% Quatro tempos:45%	6.300 - 6.700	80%
Navios de transporte de óleo bruto	Dois tempos:80% Quatro tempos:19%	6.700 - 7.300	75%
Navios (Lift-on Lift-off)	Dois tempos:55% Quatro tempos:32%	6.000	80%
Navios (Roll-on Roll-off)	Dois tempos:11% Quatro tempos:17%	6.500 - 7.000	80-85%
Navios de passageiros	Quatro tempos 100%	4.000	55%
Barcos de pesca	Dois tempos:3% Quatro tempos:69%	6.000 - 7.000	70%

Neste exemplo, adota-se o tempo médio de operação de 6.500 horas. O passo seguinte necessário para definir a meta de confiabilidade coerente com as exigências do mercado passa pelo conhecimento da expectativa de vida que esse mercado exige para o componente reator.

Segundo Rubin et al. (2004), a expectativa de vida do sistema SCR aumentou significativamente nos últimos anos, como mostra a tabela 4.9.

Tabela 4-9-Estimativa de vida do sistema SCR em aplicações industriais (RUBIN et al., 2004)

Ano	Média de horas em operação
1984	7.541
1987	17.082
1991	22.776
1994	19.929
1997	36.000

O valor referência de expectativa de vida usado é de 36.000 horas relativo ao ano de 1997, esse tempo equivale entre nove e dez anos de operação (RUBIN *et al.*, 2004). Uma correção nesse tempo para a aplicação marítima é necessária devido a diferença de tempo de operação quando comparada às aplicações industriais que são em média 12,5% maior (HAFNER, 2008). Assim, para um período entre nove e dez anos as horas de operação marítima atingem em média 32.000 horas.

Corroborando com a estimativa de vida de 32.000 horas para o reator SCR está o plano de manutenção de um dos principais fabricantes de motores marítimos, o qual estabelece 32.000 horas entre nove e dez anos de operação como o intervalo de manutenções de componentes e sistemas periféricos do motor (TBO) (MAN DIESEL& TURBO, 2010b).

❑ Determinação da taxa de falha e confiabilidade atuais

Para a determinação de valores referência de taxa de falha e confiabilidade foi utilizado o estudo realizado por Kiriya (2001). Nesse estudo Kiriya avaliou 114.000 falhas referentes a 376 navios no período de 1982 a 1997 (tabela 4.10). A partir dessa avaliação foi construída uma lista com os itens (componente/sistema) que mais falharam e suas respectivas taxas de falhas. O item que está no topo da lista é o motor a diesel principal com mais de 7.032 falhas atingindo 9,12% de incidência e uma taxa instantânea de falha de 0,86 falhas /1.000 horas de operação. Na segunda posição,

está a caldeira com 7.116 casos ou 9,23% de incidência e taxa de falha instantânea de 0,84 falhas/1.000 horas de operação. As taxas de falhas calculadas que aparecem na tabela seguem a distribuição exponencial (KIRIYA, 2001).

Tabela 4-10-Dados de falha consolidados (KIRIYA, 2001)

Item	Número de falhas	Incidência	Taxa de falhas (casos/1.000 horas)
Motor principal (diesel)	7032	9,12%	0,86
Caldeira	7116	9,23%	0,84
Motor gerador	5235	6,79%	0,75
Equipamentos elétricos	4097	5,31%	0,53
Equipamentos de controle I	10761	13,95%	1,14
Equipamentos de controle II	5097	6,61%	0,61
Sistemas de transmissão	424	0,55%	0,22
Sistemas periféricos I	33049	42,86%	3,21
Equipamentos em geral II	2918	1,80%	0,4
Equipamento de navegação e comunicação	1385	3,78%	0,74
Total	77114	100%	

Na falta de dados de falha de campo e do projeto do reator SCR foi necessário selecionar um componente com características funcionais próximas. Mas como nenhum dos itens da tabela 4.10 se aproximou das características do SCR adotou-se o critério de que o item fosse um componente mecânico e estivesse localizado no fluxo de saída dos gases de exaustão, pois estaria submetido às mesmas condições de variação de pressão e temperatura. No sentido apenas de se obter um componente como referência, optou-se pela caldeira que possui uma taxa de falha instantânea de 0,84 falhas/1.000 horas de operação. A partir dessa taxa de falha é possível obter a confiabilidade da caldeira e verificar se é um valor aceitável para um tempo de vida esperado de 32.000 para o sistema SCR. Em Kiriya (2001) a taxa de falha é calculada a partir de uma distribuição de confiabilidade exponencial $R(t) = e^{-\lambda t}$. Usando essa

distribuição para $\lambda = 0,84$ e o tempo objetivo $t = 32.000$ horas a quota de taxa é calculada e os valores mostrados na tabela 4.11.

Tabela 4-11- Quota de falha por horas de operação.

(x1000)horas	R(t)	1 - R(t)	ppm
0,001	99,92%	0,08%	840
0,01	99,16%	0,84%	8.365
0,1	91,94%	8,06%	80.569
1	43,17%	56,83%	568.289
4	3,47%	96,53%	965.265
8	0,12%	99,88%	998.793
12	0,00%	100,00%	999.958
16	0,00%	100,00%	999.999
20	0,00%	100,00%	1.000.000
24	0,00%	100,00%	1.000.000
28	0,00%	100,00%	1.000.000
32	0,00%	100,00%	1.000.000

Observa-se na tabela que a probabilidade de falha atinge 100% a partir de 12.000 horas, ou seja, um desempenho extremamente insatisfatório para o projeto do sistema do reator catalítico SCR. Como a taxa de falha instantânea de 0,84 apresenta um desempenho muito ruim para o sistema, adotou-se uma taxa de falha que pudesse oferecer uma probabilidade de falha para $t = 32.000$ horas de no máximo 5% ou uma confiabilidade de $R(t) = 95\%$. A partir da distribuição exponencial têm-se:

$$\lambda = -\frac{\ln(R(t) = 95\%)}{32.000} = 0,0016 \text{ Falhas / 1.000 horas de operação}$$

O valor de 0,0016 falhas/1.000 horas é o que fornecerá um valor de quota de falha de 50.000 *ppm* sendo esse o valor definido como meta para o projeto.

❑ Cálculo da confiabilidade

A confiabilidade $R(t_s)$ é calculada a partir do valor do n_{eff} usando a equação (2.14),

$$R(32.000) = (1 - 0,9)^{\frac{1}{0,6}} = 2,17\%$$

❑ Cálculo da quota de falha

Probabilidade de falha de 97,83% significa uma quota de falha de 978.342ppm. O gráfico da figura 4.21 mostra o comportamento durante os 30 meses do projeto:

Figura 4-21-Comportamento da quota de falha durante o período de testes

❑ Esforço de testes teoricamente necessário para se alcançar meta

Utiliza-se aqui o valor meta de confiabilidade $R(32.000) = 95\%$ e o de nível de confiança

$P_A = 90\%$, com o uso da equação (2.15) a amostra efetiva torna-se n_{eff} :

$$n_{eff} = \frac{\ln(0,1)}{\ln(0,95)} = 45$$

❑ Proposta de aumento dos esforços de testes

O valor encontrado de $n_{eff} = 45$ exige um aumento do esforço de testes. A proposta consiste do uso de 10 motores de instalações industriais com o sistema SCR.

❑ Cenário 2- Cálculo da amostra efetiva

Para esses motores o fator de aceleração r utilizado é 10. Com esse novo planejamento de testes, o n_{eff} obtido é:

Tabela 4-14- Programa de testes consolidado com esforço adicional– Marítima

i	Tipo de teste	t_t (h)	r	$L_{V,i}$	$L_{V,i} \cdot r$	$(L_{V,i} \cdot r)^{\beta}$	n	$n_{eff,i}$
1	Cliente A	3500	3	0,11	0,33	0,11	4	0,43
2	Cliente B	2200	3	0,07	0,21	0,04	4	0,17
3	Motores de aplicação industrial	3500	10	0,11	1,09	1,2	14	16,75
								17,35

❑ Cálculo da confiabilidade

Inserindo o novo valor de amostra efetiva na equação 2.14 obtém-se o valor de confiabilidade:

$$R(32000) = (1 - 0,9)^{\frac{1}{17,34}} = 85,57\%$$

❑ Cálculo da quota de falha

Probabilidade de falha de 87,57% significa uma quota de falha de 124.291ppm. No gráfico da figura 4.22 tem-se a redução da taxa durante o projeto.

Figura 4-22-Comportamento da quota da taxa de falha durante o projeto

❑ Comparativo da quota de falha entre os cenários 1 e 2

A redução da quota de taxa de falha com o esforço de testes adicional foi significativo, é o que mostra o comparativo entre os cenários em relação à meta da figura 4.23. No cenário 1 a quota de taxa de falha encontrada foi de cerca de 20 vezes superior a meta, no cenário 2 essa relação caiu para 2,5 acima.

Figura 4-23-Comparativo entre a meta de quota de falha e os cenários 1 e 2

❑ Redução do esforço de testes

A redução da quota de falha no cenário 2 foi obtida com maior esforço de testes através do aumento do tamanho de amostras, no entanto, esse esforço pode se tornar impraticável quando se verifica seu impacto do orçamento do projeto.

Nesse caso a técnica Beyer/Lauster poder ser aplicada para reduzir o esforço de testes sem alterar o atendimento da quota de falha. Com uso da equação (2.17) e do valor $R_0 = 90\%$, calcula-se o novo valor de amostra efetiva para alcançar o nível de quota de falha 124.292 ppm alcançado no cenário 2.

$$n_{eff} \cong 8$$

A redução do esforço de testes de $n_{eff} \cong 17$ para $n_{eff} \cong 8$ com o uso da informação a priori é uma demonstração de que o conhecimento que se tem sobre o projeto pode significar economia de recursos de projeto.

5 CONCLUSÕES

Conforme o objetivo estabelecido foi desenvolvido um método com base no planejamento estatístico de testes de confiabilidade, para instrumentalizar quantitativamente a abordagem “Padrões Baseados em Metas” (GBS) em seus níveis I e II quanto à verificação das metas de segurança.

Destaca-se o aspecto inovador da introdução de uma abordagem de tratamento quantitativo para a estrutura GBS a partir de métodos e ferramentas de confiabilidade para fornecer uma medida de risco com base no nível de demonstração das metas de confiabilidade, que pode ser usada no processo de tomada de decisão em projetos.

No primeiro exemplo buscou-se comparar a aplicação do método baseado no FMEA com o método proposto, para o um mesmo componente do sistema SCR. Pode-se com esse exemplo verificar que decisões baseadas exclusivamente no FMEA podem induzir a estimativas subestimadas da probabilidade de ocorrência de falhas catastróficas no sistema.

Constata-se que decisões de projeto tomadas com base em medidas de risco que são destituídas de um criterioso embasamento estatístico podem indicar incorretamente um cenário de risco aceitável. A incerteza quanto ao atendimento das metas de desempenho não mensurada pelo método baseado no FMEA foi tratada pelo método aqui proposto no qual o objetivo foi fornecer uma medida apropriada de maturidade do projeto ao levar em consideração o tamanho da amostra e o tempo de duração dos testes.

Através dos exemplos práticos demonstrou-se a aplicação dos métodos para análise de sistemas mecânicos em dois segmentos de transporte que possuem diferentes condições de testes. O método também permitiu otimizar os recursos de testes para a avaliação de confiabilidade, situação mais favorável do que a encontrada na análise

tradicional de confiabilidade onde há necessidade de elevado tamanho de amostra e condições controladas de testes que implicam em elevação do custo do projeto.

Outra contribuição do trabalho refere-se à utilização do método Beyer / Lauster que conforme demonstrado é de simples aplicação com apoio de uma planilha computacional. Porém é preciso ressaltar que existem algumas limitações, particularmente quando se considera a informação *a priori* por completo e não se faz distinção entre os sistemas comparados, com isso, pode-se produzir supervalorização da informação. Esse efeito ocorre devido à dificuldade de transferir o conhecimento para um de um sistema em uso para um novo projeto, sem adicionar certo nível de incerteza.

Como trabalhos futuros sugere-se a pesquisa de outros métodos como o de Kleyner *et al.* (1997) que trata as informações *a priori* em nível de modos de falha e que estabelece fatores que refletem informações de simulações computacionais análise de experimentos e históricos de projeto.

6 REFERÊNCIAS BIBLIOGRÁFICAS

Associação Brasileira de Normas Técnicas. NBR 5462, Confiabilidade –terminologia. Rio de Janeiro, 1981, 17p.

_____.NBR ISO 9001:2000. Sistemas de gestão da qualidade – fundamentos e vocabulário.. Rio de Janeiro, 2000.

AGUMYA, A;HUNTER,G. J.A Risk-Based Approach to Assessing the ‘Fitness for Use’ of Spatial Data.In: URISA Journal,vol. 11, no. 1, Spring 1999.

AUTODATA. Óleo Diesel Limpo na Pista. In: *Revista Autodata*. São Paulo: Autodata Editora, edição 263,julho de 2011, p. 58-62.

AYYUB, B.M.; KARASZEWSKI, Z.J.;WADE, M. Probabilistic Risk Analysis of Diesel Power Generators Onboard Ships. In: *Marítima Engineers Journal*, May 1999.

AYYUB, B. M.;BEACH, J. E.;SARKANI, S.;ASSAKKAF, I. A. Risk Analysis and Management for Marine Systems. In:*Marítima Engineers Journal*, ASNE, 2002.

BAE, Y, K; SILVA, H.B. Do Vehicle Recalls Reduce the Number of Accidents? The Case of the U.S. Car Market. Disponível em:<[http // ms.cc.sunysb.edu](http://ms.cc.sunysb.edu)>. Acesso em 05 de maio de 2011.

BERTSCHE, B. *Reliability in Automotive and Mechanical Engineering*. Berlin: Springer, 2008.501p.

BIROLINI, A. *Reliability Engineering: theory and practice*. Springer-Verlag Berlin Heidelberg, 2004.

BINDER, K.; SCHWARZ,V. Present and future of heavy duty engine strategies for compliance to the emission legislation.In: Conf. on Thermo and Fluid Dynamic Processes in Diesel Engines (THIESEL).Valencia, Spain, 2002.

BORGES, W. S.;PEREIRA, L.A.A.; SALDIVA, P.H.N. *Modelos Probabilísticos em Confiabilidade*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, v. 1,1979.

BRAGA, A. et. al. *Poluição Atmosférica e seus Efeitos na Saúde Humana*. Faculdade de Medicina, USP, São Paulo, 2003.

BRAUN, E. *Technology in context: technology assessment for managers*.London: Routledge, 1998,165 p.

CAMPEAN, I.F.;KUHN,F.P. *Reliability Analysis of Automotive Field Failure Warranty Data*.University of Bradford, Richmond Building, West Yorkshire, UK, 2000.

CARBONE, T.A.; TIPPETT, D.D. Project risk management using the Project risk FMEA. In: *Engineering Management Journal*, v.16, n.4, 2004, p.28-35.

CNT – Conselho Nacional de Transporte - Coordenação de Projetos Especiais (CPE). *Estudo Técnico: A Qualidade do Diesel no Brasil*. Brasília, novembro de 2008.

CNT – Conselho Nacional de Transporte. A fase P7 do PROCONVE e o Impacto no setor de transporte. CNT: SEST/SENAT. In: *Revista Despoluir*. Brasília, 2011.

COHEN, A. J.; ANDERSON, H. R.; OSTRO, B.; PANDEY, K. D.; KRZYZANOWSKI, M.; KÜNZLI, N.; GUTSCHMIDT, K.; POPE, A.; ROMIEU, I.; SAMET, J. M.; SMITH, K. The global burden of disease due to outdoor air pollution. In: *J. Toxicol. Environ. Health. Part A*, 68, 2005, p.1301–1307.

COIT, D.W.; DEY, K.A. Analysis of grouped data from field-failure reporting systems. In: *Reliability Engineering and System Safety*, 65. Elsevier, 1998, p. 95-101 .

CORBETT, J.J.; KOEHLER, H.K. Updated emissions from ocean shipping. In: *Journal of geophysical research*, vol. 108, no. d20, 4650, 2003.

CORBETT, J.J. et. al. Mortality from ship emissions: a global assessment. In: *Environmental Science & Technology*, vol. 41, 2007, p.8512–8518.

CROSBY, P.B. *Quality is free: The art of making quality certain*. New York: McGraw Hill Custom Publishing, 1979, 309 p.

DELONGA, M. *Zuverlässigkeitsmanagementsystem auf Basis von Felddaten*. Institut für Maschinenelemente. Thesis (Doktor). Universität Stuttgart, 2007.

DEMING, W.E. *Quality, productivity, and competitive position*. Cambridge, MA: MIT, Center for Advanced Engineering Study, 1982, 373 p.

DEPARTAMENTO NACIONAL DE TRÂNSITO DENATRAN. Disponível em <http://www.denatran.gov.br/frota.htm>. Acesso em 01 março de 2012.

DIMITRI, K. *Reliability Engineering Handbook*. vol. 1. New Jersey: Prentice Hall Inc., Englewood Cliffs 1991.

Det Norske Veritas. Marpol 73/78 Annex: Technical and Operational Implications, 2009.

DYRSCH, R; MOQVIST, C. Temperature Modeling and Control in SCR-systems for Heavy Trucks. Department of Signals and Systems, Division of Automatic Control, Automation and Mechatronics, Chalmers University of Technology, Göteborg, Sweden, February, 2009.

EEA- European Environmental Agency. COUNCIL DIRECTIVE 1999/30/EC. Official Journal of the European Communities, 1999.

ERICSON, C. NO_x Modelling of a Complete Diesel Engine/SCR System. Licentiate Thesis, Division of Combustion Engines, Department of Energy Sciences, Lund Institute of Technology, Sweden, 2007.

FISCHHOFF et al. Defining Risk. Policy Sciences, 17, pp. 123-139. 1984.

GAVIN, A. Safety, Politics and Crime. Proceedings of the 16th International Ship and Offshore Structures Congress. Southampton, UK, 20-25 August 2006, vol. 3, p. 1-7.

GALOR, O. AND O. MOAV. Natural Selection and the Evolution of Life Expectancy, CEPR Discussion Paper No. 5373. 2005.

GEKAS, I.; GABRIELSSON, P.; JOHANSEN, P. K.; NYENGAARD, L.; LUND, T. Urea-SCR Catalyst System Selection for Fuel and PM Optimized Engines and a Demonstration of a Novel Urea Injection System. SAE, 2002.

GOLDSWORTHY, L. Exhaust emissions from ship engines – significance, regulations, control technologies. In: *Australian and New Zealand maritime law journal*, volume 24, issue 1, June, 2010.

GOODCHILD, M. F. Final Report of Research Initiative 1: Accuracy of Spatial Databases. Santa Barbara: National Center for Geographic Information and Analysis. 1992.

GUIMARÃES, L. S. *Gerenciamento de Riscos e Segurança de Sistemas*. São Paulo: iEditora, 2003.

HAFFNER, A. *Ein Modell zur Bestimmung der monetären Einsparungspotenziale bei der Durchführung einer Fehlermöglichkeits- und Einflussanalyse (FMEA)*. Thesis (Doktor). Universität Stuttgart, 2005.

HAFNER, H. Retrofit of DPF and SCR-DeNO_x Systems on Locomotives, Ships and Gensets. Course CARB/SCAQM. 12–14. Nov., 2008.

HAVIARAS, G.J. *Metodologia para análise de confiabilidade de pneus radiais em frotas de caminhões de longa distância*. Dissertação de Mestrado. Escola Politécnica da Universidade de São Paulo, São Paulo, 2005.

HELDEN, R. van; VERBEEK, R.; WILLEMS, F.; WELLE, R. van. Optimization of Urea SCR deNO_x Systems for HD Diesel Engines. SAE International, 2004-01-0154.

HITZIGER, T. *Übertragbarkeit von Vorkenntnissen bei der Zuverlässigkeitstestplanung*. Dissertation. Institut für Maschinenelemente, Universität Stuttgart, 2007.

HOPPE, H. Goal-based standards – a new approach to the International Regulation of Ship Construction. In: *WMU Journal of Maritime Affairs*, vol. 4, n. 2, October 2005.

HUSS, M. Status at IMO: Where are we heading with goal-based standards?. In: *SAFEDOR – The Mid Term Conference*, May 2007.

IACS. Overview and IACS Experience in Formal Safety Assessment. Presentation at MSC 75, 16 maio de 2002.

INTERNATIONAL MARITIME ORGANIZATION -. Goal-based new ship construction standards. In: *MSC 78/6/2 (Bahamas, Greece, IACS)*, 5 February 2004.

_____. Report of the Maritime Safety Committee on its eightieth session', MSC 80/24, 24 May 2005.

_____. Goal-based new ship construction standards – Safety level approach – Worked example. In: *MSC 81/6/14*, Germany, May 2006.

_____. FORMAL SAFETY ASSESSMENT – Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process. In: *MSC 83/INF.2*, 14 May 2007.

_____. Goal-based new ship construction standards – Report of the Working Group. In: *MSC 84/WP.4*, 15 May 2008.

_____. Pollution Prevention, Air Pollution and CHG emissions. Disponível em: <<http://www.imo.org/OurWork/Environment/PollutionPrevention/AirPollution>>. Acesso em 10.de agosto de 2010.

_____. Goal-based construction standards for new ships. Disponível em: <<http://www.imo.org/OurWork/Safety/SafetyTopics/Pages/Goal-BasedStandards.aspx>>. Acesso em 15.02.2011.

ISSC. Design principles and criteria. In: *Proceedings of the 17th international ship and offshore structures congress*. Seoul, Korea, 16-21 august 2009, vol. 1, p. 597-612.

IRESON, W.; COOMBS, C.; MOSS, R. *Handbook of Reliability Engineering and Management Publisher*. 2 ed. New York: McGraw-Hill Professional, 1995, 816 p.

JÄGER, P. Zuverlässigkeitsbewertung mechatronischer Systeme in frühen Entwicklungsphasen. Thesis. Institut für Maschinenelemente, Universität Stuttgart, 2007.

JOSEPH JR, H. *PROCONVE (PROGRAMA DE CONTROLE DA POLUIÇÃO DO AR POR VEÍCULOS AUTOMOTORES) – As Fases Passadas e Futuras*. Seminário sobre Emissões de Veículos Diesel– ANFAVEA, 27 de Outubro de 2009.

JURAN, J. M. *Juran on Planning for Quality*. New York: Free Press, 1988, 551 p.

_____. *A qualidade desde o projeto*. Trad. Nivaldo Montingelli Jr. São Paulo: Pioneira, 1992, 551 p.

KAO, J. H. K. The Beta Distribution in Reliability and Quality Control. In: *Proc. seventh national symposium on reliability & quality control*. Philadelphia, 1961, p.496-511.

KAPLAN, S.; GARRICK, B. J. On The Quantitative Definition of Risk. In: *Risk Analysis*, Vol. I, No. I, 1981.

KIRIYA, N. Statistical Study on Reliability of Ship Equipment and Safety Management – Reliability Estimation for Failures on Main Engine System by Ship Reliability Database System. In: *Bulletin of the JIME*, Vol. 29, No.2, 2001.

KLEYNER, et al. Bayesian techniques to reduce the sample size in automotive electronics attribute testing. In: *Microelectron. Rehab.*, vol. 37, No. 6, 1996, p 879-883.

KNIGHT, F. Risk, Uncertainty, and Profit, Boston: Houghton Mifflin, 1921. *apud* AGUMYA, A; HUNTER, G. J. A Risk-Based Approach to Assessing the ‘Fitness for Use’ of Spatial Data. In: *URISA Journal*, vol. 11, no. 1, Spring 1999.

KONTOVAS, C.A. Formal Safety Assessment: Critical Review and Future Role. Diploma Thesis, NTUA, June 2005.

KONTOVAS, C. A.; PSARAFTIS, H. N.; ZACHARIADIS, P. The Two C’s of the Risk-Based Approach to Goal - based Standards: Challenges and Caveats. In: *International Symposium on Maritime Safety, Security and Environmental Protection*. Athens, Greece, 20-21 September 2007a.

KONTOVAS, C.A.; PSARAFTIS, H.N.; ZACHARIADIS, P. Improving FSA as a prerequisite for risk-based GBS. In: *PRADS 2007– The 10th International Symposium on Practical Design of Ships and Other Floating Structures*. Houston, TX, USA, Oct. 2007b.

KONTOVAS, C.A.; PSARAFTIS, H.N. Formal Safety Assessment: A critical review. In: *Marine Technology*. Vol. 46, No 1, January 2009.

KRAFTFAHRZEUG-BUNDESAMT JAHRESBERICHT. Germany, 2007. 52 p.

KREMER, F. Ações para Atendimento aos Novos Limites de Emissões do Proconve - Fase 7 - O Diesel: Especificações e Suprimento. In: *Seminário sobre emissões de veículos Diesel - ANFAVEA*. São Paulo, 27 de outubro de 2009.

KROLO, A.; FRITZ, A.; BERTSCHE, B. Correlation between the Failure Behavior of Automotive Components under Taxi & Field Operating Conditions. In: *Proc. Annual Reliability and Maintainability Symposium*. 2001, p. 314-321.

KROLO, A.; RZEPKA, B.; BERTSCHE, B. Considering Prior Information for Accelerated Tests with a Lifetime-Ratio. In: *Proc. 3rd International Conference on Mathematical Methods in Reliability: Methodology and Practice*. Norway, June 17-20, 2002, p. 349-352.

KROLO, A. BERTSCHE, B. An Approach for the Advanced Planning of a Reliability Demonstration Test based on a Bayes Procedure. In: *Proceedings –Annual Reliability and Maintainability Symposium*. 2003.

KROLO, A. *Planung von Zuverlässigkeitstests mit weitreichender Berücksichtigung von Vorkenntnissen*. Thesis. Institut für Maschinenelemente, Universität Stuttgart, 2004.

_____. Application of Bayes Statistics to Reduce Sample-Size, Considering a Lifetime-Ratio, 2002 apud 3. BEYER, R.; LUSTER, E.: "Statistische Lebensdauerprüfpläne bei Berücksichtigung von Vorkenntnissen". QZ 35 (1990), Heft 2, pp 93-98.

KUMAMOTO, H. *Satisfying Safety Goals By Probabilistic Risk Assessment*. London: Springer-Verlag London Ltd, 2007, 269p.

LEE, J.C.; McCORMICK, N.J. *Risk and Safety Analysis of Nuclear Systems*. New York: Wiley, 2011.

MARTZ, H.F.; Waller, R.A.: "Bayesian Reliability Analysis". Jon Wiley & Sons, Inc., 1982..

MADDOXX, M.E. Error apparent. In: *Industrial Engineer*. v.37, n.5, 2005, p.40-44.

MAHR, B. Future and Potential of Diesel Injection Systems. In: *THIESEL 2002 – Conference on Thermo- and Fluid-Dynamic Processes in Diesel Engines*. Spain, 2002.

MAN Diesel & Turbo. Two-stroke Low Speed Diesel Engines. Technical papers, 25/05/2009.

_____. Tier III Compliance – Low Speed Engines. Technical papers, 25/08/2010a.

_____. Service Experience in Low Speed Diesel Engines. Technical papers, 25/08/2010b.

_____. PrimeServ Retrofits First SCR System. Press Release. Man Diesel, 29/01/2010c.

MANNAN, S. *Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*. 3rd ed. Elsevier, 2005.

MEEKER, W.Q.; ESCOBAR, L.A. *Statistical Methods for Reliability Data*. New York: Wiley, 1998.

MILITARY HANDBOOK - 338B- *Electronic Reliability Design Handbook*., United States: Department of Defense, October 1998.

MOXIM, W. J. et al. Simulated Global Troposphere PAN. Its transport and Impact on NO_x. *J. Geophys. Res.*, 95, 5717–5729. 1990.

MADDOXX, M.E. Error apparent. *Industrial Engineer*, v.37, n.5, p. 40-44, 2005.

NAGEL, T; DIRINGER, J. Minimum Test Requirements for High Cell-Density, Ultra-Thin-Wall Catalyst Supports; Part I. Emitec GmbH Lohmar.Society of Automotive Engineers, 2000.

NELSON, W. Weibull analysis of reliability data with few or no failures. In: *Journal of Quality Technology*, 17, 1985, p.1410-146.

_____. Accelerated Testing: Statistical Models, Test Plans, and Data Analyses. New York: Wiley, 1990.

_____. Accelerated Testing: Statistical Models, Test Plans, and Data Analyses. New York: Wiley, 1990

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY : e-Handbook of Statistical Methods. Website: <http://www.itl.nist.gov/div898/handbook>. Stand: December 2008.

NIEHAUS, F.; LEDERMAN, L. PSA as a tool for decision making. In: *Nuclear Engineering and Design*, Volume 93, Issues 2-3, 2 May 1986, p. 349-356.

O'CONNOR , P. et al. *Practical reliability engineering*. 2002, 513 p.

O'CONNOR , P. Testing for Reliability .QUALITY AND RELIABILITY ENGINEERING INTERNATIONAL; 19:73–84 (DOI: 10.1002/qre.509) .Whitney Drive, Stevenage, Herts SG1 4BJ, U.K. 2003.

_____. T. et al. *Practical reliability engineering*. 4th edition, New York: Wiley, 2003.

PAPANIKOLAOU, A. Risk-Based Ship Design Methods, Tools and Applications. New York: Springer-Verlag, 2009, 376 p.

PILLAY A.; WANG J. Technology and safety of marine systems. UK: Elsevier (Ocean Engineering Book Series), 2003, 320 p.

PIDGEON et al. Risk perception. In: Risk: analysis, perception and management. Report of a Royal Society Study Group. London, Royal Society: 89–134 (1992).

PROCOM – Fundação de Proteção e Defesa do Consumidor. Recall – Chamamento. Disponível em < <http://www.procon.sp.gov.br/recall.asp> >. Acesso em 10 de Fevereiro de 2010.

PUENTE, J.; PINO, R.; PRIORE, P.; FUENTE, D. A decision support system for applying failure mode and effects analysis. In: *The International Journal of Quality & Reliability Management*, v.19, 2002, p.137-150.

RAZ, T.; SHENHAR, A.J.; DVIR, D. Risk management, project success, and technological uncertainty.. In: *R&D Management*, 32,2, 2002.

RELIABILITY ANALYSIS CENTER. *FRACAS – Failure Reporting, Analysis and Corrective Action System – Application Guidelines*, 1999.

ROVERE, E.L.L.; SILVA, H.V.O.; MENDES, F.E.; SZWARCFITER, L. *Avaliação do Programa de Controle da Poluição do Ar por Veículos Automotores*, v. 1.1ª ed. Brasília: Ministério do Meio Ambiente, 2006, 128 p.

RUBIN, E.S.; TAYLOR, M.R.; YEH, S.; HOUNSHELL, D.A. Learning Curves for Environmental Technology and Their Importance for Climate Policy Analysis. In: *Energy*, 29, June 2004, p.1551–1559.

SAGE, A. P. Systems Engineering for Risk Management. In: BEROGGI, E. G.; WALLACE, W. A. (eds.). *Computer Supported Risk Management*. Rotterdam: Kluwer, 1995, p.3-3..

SATKUNAS, F. Recalls no Brasil já envolveram mais de 1 milhão de veículos neste ano. Disponível em http://www.smabc.org.br/smabc/blog.asp?id_CON=21835&id_SUB=77 Acesso em 20 de maio de 2011.

SCHMID, H.; WEISSER, G. *Marine Technologies for Reduced Emissions*. Switzerland: Winterthur Wärsilä Corporation, 2005.

SEGISMUNDO, A.; MIGUEL, P.A.C. Gerenciamento de riscos em projetos: Proposição inicial de um conceito integrado para as fases de desenvolvimento de produto – Estudo em uma empresa automotiva. Artigo aceito para o XIV SIMPÓSIO INTERNACIONAL DE ENGENHARIA AUTOMOTIVA; SIMEA, São Paulo, 2006.

SEGISMUNDO, A.; MIGUEL, P.A.C. O papel do FMEA no processo de tomada de decisão em desenvolvimento de novos sistemas. In: *Sistema & Produção*, vol. 9, n. 2, fev. 2008, p.106-119.

SHTUB, A.; BARD, J.F.; GLOBERSON, S. *Project Management, Engineering, Technology, and Implementation*. New Jersey: Prentice-Hall, 1994, 561p.

SIMÕES, S.F. Aplicação de FMEA e FMECA na Tecnologia Submarina. In: CENPES/PDP/TS PETROBRAS, São Paulo, 2004.

SKJONG, R. Elements of a Goal-Based Regulatory Framework. In: *SAFER EURORO II*, Hamburg, January 27, 2005.

SOUZA, G.F.M. *Análise de Confiabilidade Aplicada ao Projeto de Sistemas Mecânicos*. São Paulo: EDUSP, 2003, 210 p. Apostila para a disciplina de Pós-Graduação PMR-5201- Análise de Confiabilidade Aplicada ao Projeto de Sistemas Mecânicos.

STARR C. Social Benefit vs. Technical Risk." *Science*, Vol. 165, #1232-1238. 1969.

TAGUCHI, G. Introduction to Quality Engineering. White Plains, NY: Asian Productivity Organization, UNIPUB, 1986.

THE OXFORD ENGLISH DICTIONARY. Disponível em: <http://oxforddictionaries.com/definition/standard?q=standard>. Acesso em 22. de fevereiro de 2012.

THOMPSON, J. R. Engineering Safety Assessment: An Introduction. New York: Wiley, 1987.

TRAMMELL, S.R.; LORENZO, D.K.; DAVIS, B.J. Integrated hazard analysis: Using the strengths of multiple methods to maximize the effectiveness. In: *Professional Safety*, v.49, n.5, 2004, p.29-37.

TRANSPODATA. Poluição sem volta. In: *Revista Transpodata*. São Paulo: Autodata Editora, n.33, junho de 2011, p.34-39.

VDA. Qualitätsmanagement in der Automobilindustrie – Zuverlässig. Springer-Verlag, 1999. Keitssicherung bei Automobilherstellern und Lieferanten. Verband der Automobilindustrie e.V. (VDA), 3. überarbeitete und erweiterte Auflage, Frankfurt, 2000.

WEBSTER, New Collegiate Dictionary (G. & C. Merriam Co., Springfield, 1977).

WORLD BANK. *World development indicators 2007*. Washington, D.C.: World Bank, 2007, 402p.

WORLD HEALTHY ORGANIZATION - Life expectancy at birth. Disponível em http://gamapserver.who.int/gho/interactive_charts/mbd/life_expectancy/atlas.html. Acesso em 22. fevereiro de 2012.

YAN, W.; CHEN, J.; HERFAT, A.T. Designing a reliability test plan using customer usage and bench life test data. In: *Proceedings – Reliability and Maintainability Symposium*, 2005, Annual.

ZACHARIADIS, P., PSARAFTIS, H.N.; KONTOVAS, C.A. Risk Based Rulemaking and Design: Proceed with Caution. RINA (Royal Institution of Maritime Architects, UK) conference on Developments in Classification and International Regulations. London, Jan. 2007.

A ANEXO – Fundamentos da Confiabilidade

Introdução

O primeiro passo ao se estudar a confiabilidade é definir de forma clara e precisa o que vem a ser falha. Na teoria da confiabilidade falha é tratada como um evento e o tempo como uma variável aleatória. Em algumas situações a definição de falha já é clara, mas em outras pode assumir sentidos ambíguos.

De acordo com o Centro de Análise de Confiabilidade (FRACAS, 1999) falha é definida como um evento no qual um item não executa uma ou mais de duas funções objetivas dentro de limites e condições especificados.

Uma falha pode ser catastrófica quando o equipamento rapidamente deixa de funcionar ou quando este se deteriora gradativamente com o tempo, de modo que, algumas vezes existe apenas uma fina linha divisória entre continuar cumprindo sua função e a falha. Assim, para partes críticas a falha pode ser o surgimento de uma pequena trinca, enquanto que para partes menos críticas ela ocorre quando a trinca atinge certo tamanho. Uma forma razoável de defini-la é através da visão do consumidor ,ou seja, o sistema falha quando o consumidor diz que ele falhou.

Definição de confiabilidade estatística

Segundo Bertsche (2008), é possível dar um tratamento estatístico à forma pela qual a confiabilidade lida com a falha. Na teoria da confiabilidade a probabilidade de sobrevivência é chamada de $R(t)$ e sempre inicia com 100% desde que nenhuma falha tenha ocorrido no $t=0$. A função $R(t)$ decresce monotonicamente e termina com $R(t) = 0$, depois de todas as unidades terem falhado (BERTSCHE, 2008). A probabilidade de sobrevivência $R(t)$ é, então, o complemento da probabilidade de falha $F(t)$:

$$R(t) = 1 - F(t)$$

Dessa forma confiabilidade é uma probabilidade que depende do tempo de um componente ou sistema que não falhou. Deve ser ressaltado que para se fazer obter uma definição sobre confiabilidade de um sistema não apenas o período de tempo considerado é importante, mas também as condições de aplicação do sistema em análise.

Taxa de falha

Se o comportamento da falha do componente é descrito pela função densidade de probabilidade, $f(t)$, então a probabilidade de falha em um tempo t_x é dada pela integral:

$$F(t_x) = \int_0^{t_x} f(t) dt$$

Assim, a função confiabilidade pode ser determinada por:

$$R(t_x) = \int_{t_x}^{\infty} f(t) dt$$

Para descrever o comportamento da falha, usa-se o conceito de taxa de falha $\lambda(t)$ que é obtido pelas unidades com falha até o instante t dividido pelas unidades ainda intactas:

$$\lambda(t) = \frac{\text{falhas (no ponto } t \text{ ou na classe } i)}{\text{soma das unidades ainda intactas (no ponto } t \text{ ou na classe } i)}$$

Outra forma de calcular a taxa de falha $\lambda(t)$ é dividindo a função densidade $f(t)$ pela função confiabilidade $R(t)$:

$$\lambda(t) = \frac{f(t)}{R(t)}$$

A $\lambda(t)$ é geralmente usada para descrever falhas em três estágios diferentes da vida do componente, infância ou prematura, randômica e desgaste. Segundo Borges (1979), o

resultado será sempre parecido com uma curva de características similares ou típicas da curva da banheira (figura A-1):

Figura A-1-Curva da banheira (adaptada de Ireson *et al.*(1995))

A região 1 é caracterizada pela taxa de falha decrescente em que o risco de um componente falhar diminui com o aumento do tempo – também conhecida como falhas de infância. Na região 2, tem-se a taxa de falha constante, ou seja, o risco se mantém o mesmo com o passar do tempo e, com isso, dificulta o processo de pré-estimação. Por último na região 3, o risco de uma peça falhar aumenta rapidamente com o tempo, pois componentes mecânicos apresentam desgaste, fadiga, envelhecimento, sulcos etc.

Para cada uma das três seções são aplicadas diferentes ações para o aumento da confiabilidade. Para a seção 1 diversos testes e ensaios pilotos são recomendados, a produção e a qualidade das peças também devem ser controladas. Na seção 2 deve-se realizar a correta operação e manutenção dos componentes, assim como, respeitar os tipos de aplicação para os quais o sistema foi projetado. Na seção 3 executa-se cálculos exatos para componentes e planos de testes adequados que possam representar aplicações mais extremas. As ações tomadas nas seções 1 e 2 devem ser asseguradas pelos passos tomados previamente no processo do projeto. As melhorias na seção 3, entretanto, acontecem no estágio de dimensionamento construtivo no qual o projetista pode ter uma forte influência.

Definição de probabilidade

Conforme descrito em seções anteriores os tempos de falhas dos componentes podem ser vistos como variáveis randômicas e, portanto, as leis da teoria da probabilidade podem-lhe ser aplicadas.

A história da probabilidade começa no século XVII. Matemáticos como Blaise Pascal (1623-1662), Pierre Fermat (1601-1665), Karl Gauss (1777-1855), Pierre Laplace (1749-1827) e Andrei Kolmogorov (1903-1987) deram importantes contribuições nessa área (BORGES, 1979).

Na engenharia da confiabilidade o conceito de probabilidade tem sido aplicado desde os anos 1930 (NESLSON, 1990) com maior interesse no estudo de distribuições de probabilidade de falha. Como o comportamento das falhas de diferentes sistemas pode não seguir a mesma distribuição, é necessário escolher dentre um elenco de distribuições a que melhor descreve aquela falha, elas são chamadas de *técnicas paramétricas*. Uma vez escolhida a distribuição de probabilidade que melhor descreve o comportamento do tempo de falha do sistema é possível estimar seus parâmetros.

Modelos probabilísticos para os tempos de falha

O comportamento da falha pode ser representado graficamente por varias funções. Nesta seção serão apresentadas algumas distribuições de probabilidade para os tempos de vidas:

- Distribuição Exponencial
- Distribuição de *Weibull*
- Distribuição Binomial
- Distribuição Beta

Distribuição exponencial

Esta distribuição é amplamente adotada em análise de confiabilidade devido à sua taxa de falha ter comportamento constante e boa aceitação em aplicação para componentes eletrônicos, em que geralmente as falhas são consideradas intermitentes (Dimitri, 1991).

A função exponencial tem apenas um parâmetro a taxa de falha λ . A taxa de falha λ é o inverso do tempo médio da falha t_m :

$$\lambda = \frac{1}{t_m}$$

Esse parâmetro introduzido na função de densidade de probabilidade $f(t)$ e de distribuição cumulativa $F(t)$ tem-se,

$$f(t) = \lambda e^{(-\lambda t)}, \lambda > 0 \text{ e } t \geq 0$$

onde,

$$F(t) = 1 - e^{(-\lambda t)}$$

sendo a função de confiabilidade:

$$R(t) = e^{(-\lambda t)}$$

O parâmetro λ é uma característica significativa para uma distribuição exponencial. Deve ser observado que λ tem o mesmo valor e é independente do tempo, ou seja, a mesma proporção de componentes que falharam é esperada para os itens ainda restantes sem falha.

Distribuição de Weibull

A distribuição de *Weibull* foi proposta originalmente por Waloddi Weibull (1954) em estudos relacionados ao tempo de falha por fadiga dos metais (BORGES, 1979). A popularidade em aplicações industriais deve-se à sua grande variedade de formas, todas com uma propriedade básica, a função de taxa de falha é monótona e descreve

adequadamente a vida de mancais e o desgaste em componentes estruturais, eletrônicos, entre outros. A distribuição de *Weibull* também é adequada para sistemas formados de vários elementos cuja falha decorre daquela da primeira parte. Nessa situação todas as partes devem ter a mesma distribuição para que o tempo de vida do sistema siga a distribuição de *Weibull*.

Outro motivo pela preferência por esse modelo está na flexibilidade para aplicações práticas em que se pretende descrever os processos aleatórios e permitir ampla variedade de formas sendo que todas apresentam uma propriedade básica, a função de taxa de falha monotônica. Esta pode ser decrescente, constante ou crescente, sendo a única distribuição de probabilidade de ser utilizada na descrição de processos que correspondem aos três períodos da curva da banheira (WEIBULL, 1939 *apud* HAVIARAS,2005).

A distribuição da *Weibull* é matematicamente definida pela sua equação de densidade de probabilidade (pdf). A expressão mais geral dessa equação é dada pela distribuição de três parâmetros:

$$f(T) = \frac{\beta}{\eta} \left(\frac{T-\gamma}{\eta} \right)^{\beta-1} e^{-\left(\frac{T-\gamma}{\eta} \right)^{\beta}}, \text{ onde}$$

$$f(T) \geq 0, \quad T \geq 0 \quad \text{ou} \quad \gamma, \quad \beta > 0, \quad \eta > 0, \quad -\infty < \gamma < \infty, \quad \text{onde,}$$

β é o parâmetro de forma, também conhecido como inclinação da *Weibull*;

η é o parâmetro de escala;

γ é o parâmetro de localização.

Frequentemente o parâmetro de localização é assumido como zero o que permite transformar a equação em dois parâmetros:

$$f(T) = \frac{\beta}{\eta} \left(\frac{T}{\eta} \right)^{\beta-1} e^{-\left(\frac{T}{\eta} \right)^{\beta}}$$

A distribuição de *Weibull* de dois parâmetros exibe o tempo de vida característico T (parâmetro de escala) e o parâmetro de forma β . O tempo de vida característico é uma estimativa da média e mostra a localização da distribuição. O parâmetro de forma β é a medida para a distribuição dos tempos de falhas e para a forma da densidade de falha, que sempre descreve o início das falhas no $t = 0$.

Características do parâmetro beta β

$\beta < 1$: A taxa de falha decresce com o aumento do tempo de vida e descreve falhas prematuras.

$\beta = 1$: A taxa de falha é constante. O parâmetro $\beta = 1$ é adequado para descrever falhas randômicas na faixa de falhas constantes.

$\beta > 1$: A taxa de falha aumenta com valores de b maiores do que 1.

As equações para a distribuição de *Weibull* incluem a variável estatística t na forma relativa t/T ou $(t - t_0) / (T - t_0)$. Se o tempo $t = T$ for igual a 1 a probabilidade de falha pode ser calculada como:

$$F(T) = 1 - e^{-1} = 0.632$$

O tempo de vida característico T estabelece uma probabilidade de falha de $F(T) = 0.632$ que corresponde à probabilidade de sobrevivência $R(t) = 36,8\%$. Similar à mediana, com $F(t) = 50\%$, o tempo de vida característico T pode ser interpretado como uma média especial.

A distribuição de *Weibull* também pode ser tri-paramétrica, se for dada pelo parâmetro de T , b e T_0 , sendo que o último é conhecido como parâmetro de localização, vida mínima; ou seja, antes de T_0 não ocorreriam falhas.

Confiabilidade: $R(t) = e^{-\left(\frac{t}{T}\right)^\beta}$

Probabilidade de falha: $\lambda(t) = \frac{f(t)}{R(t)} = \frac{\beta}{T} \cdot \left(\frac{t}{T}\right)^{\beta-1}$

Taxa de falha: $\lambda(t) = \frac{f(t)}{R(t)} = \frac{\beta}{T} \cdot \left(\frac{t}{T}\right)^{\beta-1}$

Parâmetros:

t : Variável estatística (Km, Ciclos de tempo, de carga etc.) > 0

T : Tempo de vida característico, “parâmetro de escala”. Para $t = T$, $F(t) = 63,2\%$ ou $R(t) = 36,8\%$. $T > t_0$

β : Parâmetro de forma. Determina a forma da curva. > 0

t_0 : tempo de falha em um determinado instante, parâmetro de localização. O parâmetro t_0 determina o ponto no tempo em que a falha começa a ocorrer.

Distribuição Binomial

A distribuição binomial é provavelmente a distribuição mais utilizada para dados discretos. Ela permite determinar a probabilidade quando se está interessado em apenas dois resultados – fracasso ou sucesso –, ou seja, resultados mutuamente exclusivos.

Segundo Nelson (1990), essa distribuição permite obter a probabilidade de se observar x sucessos em n tentativas ou unidades em testes. A probabilidade de sucesso em uma única tentativa é denotada por p , em que p é fixo para todas as tentativas.

A função de densidade de probabilidade binomial para x sucessos é dada por,

$$f(x; n, p) = \binom{n}{x} p^x (1-p)^{n-x} \text{ com, } x = 0, 1, 2, \dots, n$$

Onde,

$$\binom{n}{x} = \frac{n!}{x!(n-x)!}$$

A equação para a função de probabilidade acumulada é dada por:

$$f(x; n, p) = \sum_{i=0}^x \binom{n}{i} (p)^i (1-p)^{n-i}$$

Essa distribuição é amplamente usada em planejamento de testes de confiabilidade que atendem aos três princípios básicos para que um experimento se enquadre na lei binomial (BERTSCHE, 2008).

1. Em cada experimento pode acontecer um sucesso ou um fracasso;
2. Os experimentos podem ser repetidos, nas mesmas condições, um número n de vezes;
3. Os experimentos repetidos são independentes, ou seja, cada falha ou sobrevivência de um elemento da amostra deve ser independente das demais.

O planejamento estatístico de testes é baseado nessa distribuição.

Distribuição Beta

A distribuição beta é uma distribuição discreta de variáveis aleatórias para valores no intervalo $[0, 1]$. Seu uso mais comum é para obter uma distribuição aproximada da verdadeira, quando não se dispõe de dados de falha suficientes (KROTO, 2004). Em estatística, uma distribuição beta é uma distribuição de probabilidade contínua, com dois parâmetros, A e B , cuja função de densidade para valores $0 < x < 1$ é.

$$f(x) = \begin{cases} \frac{1}{\beta(A, B)} x^{A-1} (1-x)^{B-1} & 0 \leq x \leq 1; A, B > 0 \\ 0 & \text{diferente} \end{cases}$$

Com os dois parâmetros, A e B, a função beta se torna:

$$\beta(A, B) = \int_0^1 x^{A-1} (1-x)^{B-1} dx, A, B > 0$$

Sendo mais facilmente calculada com a ajuda da função gama:

$$\beta(A, B) = \frac{\Gamma(A)\Gamma(B)}{\Gamma(A+B)}$$

A integração da função de densidade obtém-se e a função de distribuição:

$$F(x) = \int_0^x \frac{1}{\beta(A, B)} x^{A-1} (1-x)^{B-1} dx$$

A integral da função de densidade não é analiticamente resolvida (KAO, 1961). No entanto, com o auxílio da função de distribuição beta no Microsoft Excel TM ©, função DISTBETA = (x, A, B, 0, 1), é possível obter um resultado aproximado (HILTZGER, 2007).

Intervalos de Confiança

Quando se calcula a probabilidade de falha com base em amostras, o resultado encontrado é uma aproximação do valor verdadeiro. O valor exato somente poderia ser obtido com os tempos de falha de toda a população, o que é considerada uma situação não realística. Então, o que se busca é estimar a confiabilidade baseada em uma amostra, conforme mostra a figura A-2.

Figura A-2-Representação da relação *amostra* e *população* na análise de tempo de vida

A realização de testes de confiabilidade para diferentes amostras produz variações nos valores dos parâmetros da distribuição e diferenças nas estimativas de confiabilidade. Como o valor de cada parâmetro é desconhecido o emprego de limites de confiança se torna necessário para se ter uma faixa dentro da qual valores ocorrerão certo numero de vezes. Isso permite fornecer uma medida de precisão dos resultados estimados de confiabilidade.

O intervalo de confiança pode ser bilateral, e unilateral.

Limites Bilaterais

Limites de confiança bilaterais indicam a localização de certa porcentagem da população, isto é, os limites pelos quais se circunscreve uma porcentagem especificada da população. No exemplo da figura A-3, um intervalo de confiança bilateral de 90% significa que 90% da população estão entre X e Y, com 5% menor do que X e 5% maior do que Y.

Figura A-3-Intervalo de confiança Bilateral (adaptado de Nelson (1990))

Limites Unilaterais

Esse tipo de intervalo define a região onde certa porcentagem da população é maior ou menor do que o ponto definido no eixo do tempo. Por exemplo, se X está do lado esquerdo da linha média ele indica que 95% da população têm valores maiores do que X, e o inverso indica que 95% da população é menor do que Y, como mostra a figura A-4:

Figura A-4-Limite unilateral, inferior e superior (adaptado de Nelson (1990))

O intervalo de confiança é sempre associado a uma probabilidade. Um exemplo de 90% de confiança significa que uma variável aleatória tem 90% de probabilidade de estar dentro do intervalo, e 10% fora.

Os valores das falhas observadas correspondem sempre ao nível de confiança de 50%. A probabilidade dentro do intervalo corresponde à certeza estatística, e a de fora, ao erro. Quanto maior for o número dos elementos da amostra, mais se aproximará do universo total da população, e, portanto, o intervalo de confiança torna-se mais estreito e o prognóstico, mais exato (figura A-5).

Figura A-5-Representação gráfica de um exemplo de intervalo de confiança para o tamanho de amostra n e o intervalo para $< n$. (adaptado de Hitziger (2007))

Dados de vida

São informações que permitem a realização de estimativas de confiabilidade mais precisas. Tais informações podem se originar de fontes internas ou externas à organização, das seguintes formas:

- Internas
 - Testes bancos de provas
- Externas

- Testes de Campo
- Dados de Garantia

Segundo Ireson et al. (1995) apesar da vasta disponibilidade de dados de diversas fontes externas a mais importantes continuam sendo as que são geradas dentro da própria organização durante o processo de desenvolvimento de produtos.

Estrutura dos dados de testes

A melhor condição para estimar a confiabilidade de sistemas e componentes na fase de projeto é quando se tem testes completos (BERTSCHE, 2008), porém, esses testes são demorados e caros. Mesmo sendo demorados são terminados antes que todos os itens falhem, resultando na presença de observações incompletas ou censuradas. Para Borges (1997) quando se busca um esforço de testes mais baixo o teste censurado pode ser uma alternativa, embora os resultados não sejam tão significativos como quando comparados ao teste completo. A figura A-6 ilustra os mecanismos de censura e de testes completos; a letra x indica ocorrência de falha.

Figura A-6-Diferentes estruturas de dados de falha (adaptado de Delonga (2007))

Dados Completos

É quando todos os componentes da amostra n são submetidos ao teste de vida até que o último componente da amostra falhe (r), ou seja, $n=r$.

Dados censurados Tipo I e Tipo II

É o teste finalizado após certo período preestabelecido de tempo. Apenas os tempos de falha para $r < n$ unidades de teste são conhecidos. A única coisa que se conhece sobre o restante $n-r$ ("sobreviventes") é que eles ainda estão intactos após a interrupção do ensaio. A quantidade de falhas r é uma variável randômica e desconhecida antes de o teste iniciar.

Se o teste for finalizado após a ocorrência de certo número de falhas predeterminadas, diz-se que é um ensaio censurado Tipo II. Nesse caso o ponto no tempo em que r ocorre é considerado uma variável aleatória, nessa condição o tempo para a finalização dos ensaios está em aberto.

Então, de uma amostra de tamanho n obtêm-se diferentes tempos de falha t_i nos quais i varia de $1 \leq i \leq r$, com $r \rightarrow n_f$. Os tempos de falha serão ordenados segundo o tamanho da amostra:

$$t_1 < t_2 < t_3, \dots, t_{n_f} \quad t_i \leq t_{i+1} \quad i = 1 \dots n_f$$

Para ambos os casos, $F(t_i)$ pode ser calculada por meio de uma equação aproximada (DELONGA, 2007):

$$F(t_i) \cong \frac{i - 0,3}{n + 0,4} \quad i = 1(1)n_f, \text{ onde } n_f < n.$$

Na análise dos dados censurados Tipos I e II, as unidades intactas são levadas em conta na aproximação pelo fato de a equação incluir n , ao invés de r , no denominador.

Múltiplos dados censurados

Um terceiro tipo é conhecido como múltiplos dados censurados ou censura aleatória, este ocorre quando as unidades são removidas do teste em diferentes tempos sem que

falha tenha ocorrido. Contrariamente a censura Tipo I na qual as unidades de testes sobreviventes são todas retiradas do ensaio no mesmo momento, na censura aleatória a remoção pode ser feita em momentos diferentes ou randômicos em que x indica a falha.

A flecha aponta que a unidade permaneceu intacta em relação ao mecanismo de falha observado até o ponto de sua remoção do teste. Esse caso é comum quando sistemas são testados no âmbito do modo de falha em que uma falha ocorre como consequência de outro modo de falha.

Esse tipo de censura pode ser feito com a ajuda do método da morte súbita, que se divide em três casos:

- a) Não foram disponibilizadas informações das quilometragens das unidades ainda intactas;
- b) Não foram disponibilizados os tempos exatos das quilometragens das unidades ainda intactas;
- c) Há a distribuição da quilometragem das unidades ainda intactas.

Não é incomum a falta de informações precisas da quilometragem das unidades ainda intactas (a). Devido a isso as n_s unidades intactas são distribuídas uniformemente entre as unidades que falharam n_f . Todo o conjunto de unidades é constituído portanto, de:

$$n = n_f + (n_s + 1).k,$$

Onde k é o número de unidades intactas que se encontra entre as unidades que falharam. Então, conhecidos o número de falhas e o tamanho da população, k pode ser determinado:

$$k = \frac{n - n_f}{n_f - 1}$$

Outra característica desse método é que ele estabelece lotes de n itens a serem testados. A observação em cada lote é feita até que a primeira falha ocorra a partir daí, cria-se um *ranking* dos tempos de falhas somente das primeiras unidades que falharam.

Porém como não é possível assegurar que não tenha havido uma segunda falha é necessário criar um *ranking* hipotético que leve esse fenômeno em consideração. Segundo Berstche (2008), o *rank* médio é calculado da seguinte forma:

$$j(t_j) = j(t_{j-1}) + [n_f(t_f).N(t_j)]$$

O *rank* médio $j(t_j)$ é igual ao *rank* anterior $j(t_{j-1})$ somado ao crescimento incremental $[n_f(t_f).N(t_j)]$.

O crescimento incremental $N(t_j)$ é dado pela equação:

$$N(t_j) = \frac{n+1-j(t_{j-1})}{1 + (\text{número de unidades restantes})}$$

O número de peças restantes refere-se ao número de unidades de teste remanescentes, incluindo as unidades consideradas com falha. Assim, $N(t_j)$ também pode ser determinada como:

$$N(t_j) = \frac{n+1-j(t_{j-1})}{1 + (n - \text{número de peças anteriores})}$$

O cálculo da $F(t_j)$ para a média das estatísticas de ordem é obtido através da equação:

$$F_{\text{médio}}(t_j) \approx \frac{j(t_j) - 0,3}{n + 0,4} \cdot 100\%$$

Para determinar os termos do *ranking* hipotético os dados devem ser tabulados no caso de grandes quantidades de dados é preciso o auxílio de programas computacionais.

B ANEXO – Análise de Garantia

Os dados de garantia frequentemente são a única informação disponível para refletir o desempenho e as solicitações a que o sistema é submetido nas condições de uso normal pelo cliente (COIT; DEY, 1998).

No entanto, seu uso deve ser cauteloso, visto que não se pode garantir a boa qualidade dos dados registrados. Segundo Campean (2000) dúvidas são levantadas quanto aos dados de garantia para as análises de confiabilidade em geral pois, as informações extraídas do banco de dados não são consistentes no sentido de não serem precisas, completas ou exatas.

Um dos motivos é que os registros das falhas são realizados por pessoas que possuem grau de capacitação e comprometimento distintos, enquanto aquele que é mais preparado e comprometido descreve corretamente o local da falha, o modo da falha e como ela ocorreu, outros simplesmente colocam descrições padrões que não refletem a falha e com isso, contaminam o conjunto dos dados coletados.

Outro ponto destacado pelo autor é que os registros disponíveis de falhas se referem basicamente ao período de garantia, de modo que pouca ou nenhuma informação está disponível para as unidades que não apresentaram reclamações.

Assim os dados de garantia extraídos de bancos de dados devem ser considerados censurados e, para que a análise de confiabilidade possa ser realizada é preciso encontrar o tempo (km) que o componente operou sem apresentar falhas. Esse tempo de operação é diferente para cada unidade, pois, nem todas entram em operação no mesmo instante e, dessa forma, vão acumular quilometragens diferentes ao término do período de garantia. Logo, para se obter tais quilometragens das unidades intactas seria preciso identificar o proprietário de cada unidade vendida, tentar localizá-lo e perguntar qual era a quilometragem do sistema ao término do período de garantia.

Mas isso seria muito oneroso tanto do ponto de vista financeiro quanto de tempo, visto que, dependendo do tipo de sistema a produção em um período curto de tempo pode significar milhares de unidades fabricadas, dificultando ainda mais sua localização no campo.

Então, uma maneira de se estimar a quilometragem das unidades intactas é usando a distribuição de km (*12 MIS*) sugerida por Campean (2000). O gráfico da figura B1 é resultado de uma pesquisa realizada com 353 veículos no período de garantia, em que se alcança no máximo 80.000 km.

Figura B-1-Distribuição de quilometragem para veículos que não apresentaram falhas durante o período de garantia (CAMPEAN, 2000).

Segundo o autor, essa estimativa pode ser estendida para outros períodos de garantia e quantidades de veículos expostos.