Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

NORMA
BRASILEIRA

ABNT NBR ISO/IEC 31010

Primeira edição
04.04.2012

Válida a partir de
04.05.2012

Gestão de riscos — Técnicas para o processo de avaliação de riscos

Risk management — Risk assessment techniques

ICS 03.100.01

ISBN 978-85-07-03360-8

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 31010:2012
96 páginas

© ISO/IEC 2009 - © ABNT 2012

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009
Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT, único representante da ISO no território brasileiro.

© ABNT 2012
Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT.

ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Sumário

Página

Prefácio Nacional iv
Introdução vi
1 Escopo 1
2 Referências normativas 1
3 Termos e definições 1
4 Conceitos do processo de avaliação de riscos 1
4.1 Finalidade e benefícios 1
4.2 Processo de avaliação de riscos e estrutura da gestão de riscos 2
4.3 Processo de avaliação de riscos e o processo de gestão de riscos 3
4.3.1 Generalidades 3
4.3.2 Comunicação e consulta 3
4.3.3 Estabelecimento do contexto 3
4.3.4 Processo de avaliação de riscos 5
4.3.5 Tratamento de riscos 6
4.3.6 Monitoramento e análise crítica 6
5 Processo de avaliação de riscos 6
5.1 Visão geral 6
5.2 Identificação de riscos 7
5.3 Análise de riscos 8
5.3.1 Generalidades 8
5.3.2 Avaliação dos controles 9
5.3.3 Análise de consequências 9
5.3.4 Análise e estimativa de probabilidades 10
5.3.5 Análise preliminar 11
5.3.6 Incertezas e sensibilidades 11
5.4 Avaliação de riscos 11
5.5 Documentação 12
5.6 Monitoramento e análise crítica do processo de avaliação de riscos 13
5.7 Aplicação do processo de avaliação de riscos durante as fases do ciclo de vida 13
6 Seleção de técnicas para o processo de avaliação de riscos 14
6.1 Generalidades 14
6.2 Seleção de técnicas 14
6.3 Disponibilidade de recursos 15
6.4 A natureza e o grau de incerteza 15
6.5 Complexidade 16
6.6 Aplicação do processo de avaliação de riscos durante as fases do ciclo de vida 16
6.7 Tipos de técnicas do processo de avaliação de riscos 16
Bibliografia 96

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Anexos

Anexo A (informativo) **Comparação das técnicas para o processo de avaliação de riscos** 17
A.1 **Tipos de técnicas** 17
A.1.1 **Fatores que influenciam na seleção das técnicas para o processo de avaliação de riscos** 17
Anexo B (informativo) **Técnicas para o processo de avaliação de risco** 24
B.1 ***Brainstorming*** 24
B.1.1 **Visão geral** 24
B.1.2 **Utilização** 24
B.1.3 **Entradas** 24
B.1.4 **Processo** 24
B.1.5 **Saídas** 25
B.1.6 **Pontos fortes e limitações** 25
B.2 **Entrevistas estruturadas ou semi-estruturadas** 25
B.2.1 **Visão geral** 25
B.2.2 **Utilização** 26
B.2.3 **Entradas** 26
B.2.4 **Processo** 26
B.2.5 **Saídas** 26
B.2.6 **Pontos fortes e limitações** 26
B.3 **Técnica Delphi** 27
B.3.1 **Visão geral** 27
B.3.2 **Utilização** 27
B.3.3 **Entradas** 27
B.3.4 **Processo** 27
B.3.5 **Saídas** 27
B.3.6 **Pontos fortes e limitações** 28
B.4 **Listas de verificação** 28
B.4.1 **Visão geral** 28
B.4.2 **Utilização** 28
B.4.3 **Entradas** 28
B.4.4 **Processo** 28
B.4.5 **Saídas** 29
B.4.6 **Pontos fortes e limitações** 29
B.5 **Análise preliminar de perigos (APP)** 29
B.5.1 **Visão geral** 29
B.5.2 **Utilização** 29
B.5.3 **Entradas** 29
B.5.4 **Processo** 30
B.5.5 **Saídas** 30
B.5.6 **Pontos fortes e limitações** 30
B.6 **Estudo de perigos e operabilidade (HAZOP)** 30
B.6.1 **Visão geral** 30

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.6.2 Utilização 31
B.6.3 Entradas 31
B.6.4 Processo 31
B.6.5 Saídas 33
B.6.6 Pontos fortes e limitações 33
B.6.7 Documento de referência 34
B.7 Análise de perigos e pontos críticos de controle (APPCC) 34
B.7.1 Visão geral 34
B.7.2 Utilização 34
B.7.3 Entradas 34
B.7.4 Processo 34
B.7.5 Saídas 35
B.7.6 Pontos fortes e limitações 35
B.7.7 Documento de referência 36
B.8 Avaliação da toxicidade 36
B.8.1 Visão geral 36
B.8.2 Utilização 36
B.8.3 Entradas 36
B.8.4 Processo 36
B.8.5 Saídas 37
B.8.6 Pontos fortes e limitações 38
B.9 *Técnica estruturada "E se"* (SWIFT) 38
B.9.1 Visão geral 38
B.9.2 Utilização 38
B.9.3 Entradas 38
B.9.4 Processo 39
B.9.5 Saídas 39
B.9.6 Pontos fortes e limitações 40
B.10 Análise de cenários 40
B.10.1 Visão geral 40
B.10.2 Utilização 41
B.10.3 Entradas 41
B.10.4 Processo 41
B.10.5 Saídas 42
B.10.6 Pontos fortes e limitações 42
B.11 Análise de impactos nos negócios (BIA) 43
B.11.1 Visão geral 43
B.11.2 Utilização 43
B.11.3 Entradas 43
B.11.4 Processo 44
B.11.5 Saídas 44
B.11.6 Pontos fortes e limitações 45
B.12 Análise de causa-raiz (RCA) 45

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.12.1 Visão geral 45
B.12.2 Utilização 45
B.12.3 Entradas 46
B.12.4 Processo 46
B.12.5 Saídas 47
B.12.6 Pontos fortes e limitações 47
B.13 Análise de modo e efeito de falha (FMEA) e análise de modo, efeito e criticidade de falha (FMECA) 47
B.13.1 Visão geral 47
B.13.2 Utilização 48
B.13.3 Entradas 48
B.13.4 Processo 49
B.13.5 Saídas 50
B.13.6 Pontos fortes e limitações 50
B.13.7 Documento de referência 51
B.14 Análise de árvore de falhas (FTA) 51
B.14.1 Visão geral 51
B.14.2 Utilização 52
B.14.3 Entradas 52
B.14.4 Processo 52
B.14.5 Saídas 53
B.14.6 Pontos fortes e limitações 53
B.14.7 Documento de referência 54
B.15 Análise de árvore de eventos (ETA) 54
B.15.1 Visão geral 54
B.15.2 Utilização 55
B.15.3 Entradas 55
B.15.4 Processo 56
B.15.5 Saídas 56
B.15.6 Pontos fortes e limitações 56
B.16 Análise de causa e consequência 57
B.16.1 Generalidades 57
B.16.2 Utilização 57
B.16.3 Entradas 57
B.16.4 Processo 57
B.16.5 Saída 58
B.16.6 Pontos fortes e limitações 59
B.17 Análise de causa e efeito 59
B.17.1 Visão geral 59
B.17.2 Utilização 59
B.17.3 Entradas 60
B.17.4 Processo 60
B.17.5 Saída 61

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.17.6 Pontos fortes e limitações 62
B.18 Análise de camadas de proteção (LOPA) 62
B.18.1 Visão geral 62
B.18.2 Utilização 62
B.18.3 Entradas 63
B.18.4 Processo 63
B.18.5 Saída 64
B.18.6 Pontos fortes e limitações 64
B.18.7 Documentos de referência 64
B.19 Análise de árvore de decisões 65
B.19.1 Visão geral 65
B.19.2 Utilização 65
B.19.3 Entradas 65
B.19.4 Processo 65
B.19.5 Saídas 65
B.19.6 Pontos fortes e limitações 65
B.20 Avaliação da confiabilidade humana (ACH) 66
B.20.1 Visão geral 66
B.20.2 Utilização 66
B.20.3 Entradas 66
B.20.4 Processo 66
B.20.5 Saídas 67
B.20.6 Pontos fortes e limitações 67
B.21 Análise *bow tie* 68
B.21.1 Visão geral 68
B.21.2 Utilização 69
B.21.3 Entradas 69
B.21.4 Processo 69
B.21.5 Saída 70
B.21.6 Pontos fortes e limitações 70
B.22 Manutenção centrada em confiabilidade 70
B.22.1 Visão geral 70
B.22.2 Utilização 71
B.22.3 Entradas 71
B.22.4 Processo 71
B.22.5 Saída 72
B.22.6 Documentos de referência 72
B.23 *Sneak analysis (SA) e sneak circuit analysis* (SCA) 72
B.23.1 Visão geral 72
B.23.2 Utilização 72
B.23.3 Entradas 72
B.23.4 Processo 73
B.23.5 Saída 73

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.23.6 Pontos fortes e limitações 73
B.24 Análise de Markov 74
B.24.1 Visão geral 74
B.24.2 Utilização 74
B.24.3 Entradas 74
B.24.4 Processo 75
B.24.5 Saídas 77
B.24.6 Pontos fortes e limitações 77
B.24.7 Comparações 77
B.24.8 Documentos de referência 78
B.25 Simulação de Monte Carlo 78
B.25.1 Visão geral 78
B.25.2 Utilização 78
B.25.3 Entradas 78
B.25.4 Processo 78
B.25.5 Saídas 80
B.25.6 Pontos fortes e limitações 80
B.25.7 Documentos de referência 81
B.26 Estatística Bayesiana e Redes de Bayes 81
B.26.1 Visão geral 81
B.26.2 Utilização 82
B.26.3 Entradas 82
B.26.4 Processo 82
B.26.5 Saídas 84
B.26.6 Pontos fortes e limitações 84
B.27 Curvas FN 85
B.27.1 Visão geral 85
B.27.2 Utilização 85
B.27.3 Entradas 86
B.27.4 Processo 86
B.27.5 Saídas 86
B.27.6 Pontos fortes e limitações 86
B.28 Índices de risco 87
B.28.1 Visão geral 87
B.28.2 Utilização 87
B.28.3 Entradas 87
B.28.4 Processo 87
B.28.5 Saídas 88
B.28.6 Pontos fortes e limitações 88
B.29 Matriz de probabilidade/consequência 88
B.29.1 Visão geral 88
B.29.2 Utilização 89
B.29.3 Entradas 89

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.29.4 Processo 91
B.29.5 Saídas 91
B.29.6 Pontos fortes e limitações 91
B.30 Análise de custo/benefício (ACB) 92
B.30.1 Visão geral 92
B.30.2 Utilização 92
B.30.3 Entradas 92
B.30.4 Processo 92
B.30.5 Saída 93
B.30.6 Pontos fortes e limitações 93
B.31 Análise de decisão por multicritérios (MCDA) 94
B.31.1 Visão geral 94
B.31.2 Utilização 94
B.31.3 Entradas 94
B.31.4 Processo 94
B.31.5 Saída 95
B.31.6 Pontos fortes e limitações 95

Figuras

Figura 1 – Contribuição do processo de avaliação de riscos para o processo de gestão de riscos 7
Figura B.1 – Curva dose-resposta 37
Figura B.2 – Exemplo de uma análise de árvore de falhas (FTA) da IEC 60300-3-9 52
Figura B.3 – Exemplo de uma árvore de eventos 55
Figura B.4 – Exemplo de análise causa e conseqüência 58
Figura B.5 – Exemplo de diagrama de Ishikawa ou espinha de peixe 61
Figura B.6 – Exemplo de formulação de árvore de análise de causa e efeito 61
Figura B.7 – Exemplo de avaliação da confiabilidade humana 68
Figura B.8 – Exemplo de diagrama de "*bow tie*" para consequências indesejadas 70
Figura B.9 – Exemplo de diagrama de Markov do sistema 75
Figura B.10 – Exemplo de diagrama de transição de estado 76
Tabela B.4 – Exemplo de simulação de Monte Carlo 79
Figura B.11 – Exemplo de rede de Bayes 83
Figura B.12 – O conceito ALARP 85

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Tabelas

Tabela A.1 – Aplicabilidade das ferramentas utilizadas para o processo de avaliação de riscos 18
Tabela A.2 – Atributos de uma seleção de ferramentas de avaliação de riscos 20
Tabela B.1 – Exemplo de palavras-guia *HAZOP* possíveis 32
Tabela B.2 – Matriz de Markov 75
Tabela B.3 – Matriz de Markov final 76
Tabela B.5 – Dados da tabela de Bayes 82
Tabela B.6 – Probabilidades *a priori* para os nós A e B 83
Tabela B.7 – Probabilidades condicionais para o nó C com o nó A e o nó B definidos 83
Tabela B.8 – Probabilidades condicionais para o nó D com o nó A e o nó C definidos 83
Tabela B.9 – Probabilidade *a posteriori* para os nós A e B com o nó D e o nó C definidos 84
Tabela B.10 – Probabilidade *a posteriori* para o nó A, com o nó D e o nó C definidos 84
Figura B.13 – Exemplo de parte de uma tabela critérios de consequência 90
Figura B.14 – Exemplo de parte de uma matriz de classificação de riscos 90
Figura B.15 – Exemplo de parte de uma matriz de critérios de probabilidade 90

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretiva ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR ISO/IEC 31010 foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos (ABNT/CEE-63). O Projeto circulou em Consulta Nacional conforme Edital nº 11, de 25.11.2011 a 10.01.2012, com o número de Projeto 63:000.01-002.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 31010:2009, que foi elaborada pelo *Technical Committee Dependability* (IEC/TC 56) em conjunto com ISO TMB "*Risk management*", conforme ISO/IEC Guide 21-1:2005.

A seguir são relacionadas as siglas e seus respectivos significados:

a) ALARP – *As Low As Reasonably Practicable*;

b) BIA – *Business Impact Analysis;*

c) *Bow Tie Analysis* (Análise *Bow Tie*);

d) CHAZOP – *Control Hazards and Operability Analysis;*

e) ETA – *Event Tree Analysis;*

f) FMEA – *Failure Mode and Effect Analysis;*

g) FMECA – *Failure Mode and Effect Criticality Analysis;*

h) FTA – *Fault Tree Analysis;*

i) HAZOP – *Hazard and Operability Studies;*

j) IPL – *Independent Protection Layers;*

k) LOPA – *Layer Protection Analysis;*

l) MCDA – *Multi-criteria Decision Analysis;*

m) NOAEL – *No Observable Adverse Effect Level;*

n) NOEL – *No Observable Effect Level;*

o) RCA – *Root Cause Analysis;*

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

p) RCFA – *Root Cause Failure Analysis;*

q) RCM – *Reliability Centred Maintenance;*

r) SA – *Sneak analysis*;

s) SCA – *Sneak Circuit Analysis;*

t) SIL – *Safety Integrity Levels;*

u) SWIFT – Structured What If Technique.

O Escopo desta Norma Brasileira em inglês é o seguinte.

Scope

This Standard is a supporting standard for ABNT NBR ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.

Risk assessment carried out in accordance with this standard contributes to other risk management activities.

The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail.

This Standard is not intended for certification, regulatory or contractual use.

This Standard does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application.

This Standard does not refer to all techniques, and omission of a technique from this standard does not mean it is not valid. The fact that a method is applicable to a particular circumstance does not mean that the method should necessarily be applied.

NOTE This Standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Introdução

Organizações de todos os tipos e tamanhos enfrentam uma série de riscos que podem afetar a realização de seus objetivos.

Estes objetivos podem estar relacionados a uma série de atividades da organização, desde iniciativas estratégicas até suas operações, processos e projetos, e se refletir em termos de resultados para a sociedade, ambientais, tecnológicos, de segurança, medidas comerciais, financeiras e econômicas, bem como impactos sociais, culturais, políticos e na reputação.

Todas as atividades de uma organização envolvem riscos que devem ser gerenciados. O processo de gestão de riscos auxilia a tomada de decisão, levando em consideração as incertezas e a possibilidade de circunstâncias ou eventos futuros (intencionais ou não intencionais) e seus efeitos sobre os objetivos acordados.

A gestão de riscos inclui a aplicação de métodos lógicos e sistemáticos para

- comunicação e consulta ao longo de todo processo;
- estabelecimento do contexto para identificar, analisar, avaliar e tratar o risco associado a qualquer atividade, processo, função ou produto;
- monitoramento e análise crítica de riscos;
- reporte e registro dos resultados de forma apropriada.

O processo de avaliação de riscos é a parte da gestão de riscos que fornece um processo estruturado para identificar como os objetivos podem ser afetados, e analisa o risco em termos de consequências e suas probabilidades antes de decidir se um tratamento adicional é requerido.

O processo de avaliação de riscos tenta responder às seguintes questões fundamentais:

- o que pode acontecer e por quê (pela identificação de riscos)?
- quais são as consequências?
- qual é a probabilidade de sua ocorrência futura?
- existem fatores que mitigam a consequência do risco ou que reduzam a probabilidade do risco?
- o nível de risco é tolerável ou aceitável e requer tratamento adicional?

Esta Norma destina-se a refletir as boas práticas atuais na seleção e utilização das técnicas para o processo de avaliação de riscos e não se refere a conceitos novos ou em evolução que não tenham atingido um nível satisfatório de consenso profissional.

Esta Norma é geral por natureza, de forma que pode dar orientações para muitos setores e tipos de sistemas. Pode haver normas mais específicas em vigor dentro desses setores que estabelecem metodologias preferidas e níveis de avaliação para aplicações específicas. Se essas normas estiverem em harmonia com esta Norma, as normas específicas geralmente serão suficientes.

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Gestão de riscos — Técnicas para o processo de avaliação de riscos

1 Escopo

Esta Norma é uma norma de apoio à ABNT NBR ISO 31000 e fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos.

O processo de avaliação de riscos conduzido de acordo com esta Norma contribui para outras atividades de gestão de riscos.

A aplicação de uma série de técnicas é introduzida, com referências específicas a outras normas onde o conceito e a aplicação de técnicas são descritos mais detalhadamente.

Esta Norma não se destina à certificação, uso regulatório ou contratual.

Esta Norma não fornece critérios específicos para identificar a necessidade de análise de riscos, nem especifica o tipo de método de análise de riscos que é requerido para uma aplicação específica.

Esta Norma não se refere a todas as técnicas, e a omissão de uma técnica nesta Norma não significa que ela não é válida. O fato de um método ser aplicável a uma determinada circunstância particular não significa que esse método seja necessariamente aplicado.

NOTA Esta Norma não trata especificamente de segurança. Esta é uma Norma genérica de gestão de riscos e quaisquer referências à segurança são puramente de natureza informativa. Orientação sobre a introdução de aspectos de segurança em normas IEC é estabelecida no ISO/IEC Guide 51.

2 Referências normativas

Os documentos relacionados a seguir são indispensáveis à aplicação deste documento. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

ABNT NBR ISO 31000, *Gestão de riscos – Princípios e diretrizes*

ABNT ISO Guia 73, *Gestão de riscos – Vocabulário*

3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições do ABNT ISO Guia 73.

4 Conceitos do processo de avaliação de riscos

4.1 Finalidade e benefícios

A finalidade do processo de avaliação de riscos é fornecer informações baseadas em evidências e análise para tomar decisões informadas sobre como tratar riscos específicos e como selecionar entre opções.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Alguns dos principais benefícios da realização do processo de avaliação de riscos incluem:

- entender o risco e seu potencial impacto sobre os objetivos;
- fornecer informações aos tomadores de decisão;
- contribuir para o entendimento dos riscos a fim de auxiliar na seleção das opções de tratamento;
- identificar os principais fatores que contribuem para os riscos e os elos fracos em sistemas e organizações;
- comparar riscos em sistemas, tecnologias ou abordagens alternativos;
- comunicar riscos e incertezas;
- auxiliar no estabelecimento de prioridades;
- contribuir para a prevenção de incidentes com base em investigação pós-incidente;
- selecionar diferentes formas de tratamento de riscos;
- atender aos requisitos regulatórios;
- fornecer informações que ajudarão a avaliar a conveniência da aceitação de riscos quando comparados com critérios predefinidos;
- avaliar os riscos para o descarte ao final da vida útil.

4.2 Processo de avaliação de riscos e estrutura da gestão de riscos

Esta Norma considera que o processo de avaliação de riscos é realizado no âmbito da estrutura e do processo de gestão de riscos descritos na ABNT NBR ISO 31000.

A estrutura da gestão de riscos fornece políticas, procedimentos e arranjos organizacionais que incorporarão a gestão de riscos através da organização em todos os níveis.

Como parte desta estrutura, convém que a organização tenha uma política ou estratégia para decidir quando e como avaliar os riscos.

Em particular, convém que aqueles que realizam processos de avaliações de risco tenham clareza sobre

- o contexto e os objetivos da organização,
- a extensão e o tipo de riscos que são toleráveis e como tratar os riscos inaceitáveis,
- como o processo de avaliação de riscos se integra nos processos organizacionais,
- os métodos e técnicas a serem utilizados no processo de avaliação de riscos e sua contribuição para o processo de gestão de riscos,
- os recursos disponíveis para realizar o processo de avaliação de riscos,
- como o processo de avaliação de riscos será reportado e analisado criticamente.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

4.3 Processo de avaliação de riscos e o processo de gestão de riscos

4.3.1 Generalidades

O processo de avaliação de riscos engloba os elementos centrais do processo de gestão de riscos que são definidos na ABNT NBR ISO 31000 e contém os seguintes elementos:

- comunicação e consulta;
- estabelecimento do contexto;
- processo de avaliação de riscos (abrangendo a identificação de riscos, a análise de riscos e a avaliação de riscos);
- tratamento de riscos;
- monitoramento e análise crítica.

O processo de avaliação de riscos não é uma atividade autônoma e convém que seja totalmente integrado aos outros componentes do processo de gestão de riscos.

4.3.2 Comunicação e consulta

O processo de avaliação de riscos bem-sucedido depende de comunicação e consulta eficazes com as partes interessadas.

O envolvimento das partes interessadas no processo de gestão de riscos irá auxiliar

- no desenvolvimento de um plano de comunicação,
- na definição do contexto de forma apropriada,
- a assegurar que os interesses das partes interessadas são compreendidos e considerados,
- a reunir diferentes áreas de conhecimento especializado para a identificação e análise de riscos,
- a assegurar que diferentes pontos de vista sejam devidamente considerados na avaliação de riscos,
- a assegurar que os riscos sejam devidamente identificados,
- a assegurar aprovação e apoio para um plano de tratamento.

Convém que as partes interessadas contribuam para a interface do processo de avaliação de riscos com outras disciplinas de gestão, incluindo a gestão de mudanças, gestão de projetos e programas, e também a gestão financeira.

4.3.3 Estabelecimento do contexto

O estabelecimento do contexto define os parâmetros básicos para a gestão de riscos e define o escopo e os critérios para o resto do processo. O estabelecimento do contexto inclui considerar os parâmetros internos e externos relevantes para a organização como um todo, bem como o conhecimento dos riscos específicos a serem avaliados.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Ao se estabelecer o contexto, os objetivos do processo de avaliação de riscos, os critérios de risco e o programa para o processo de avaliação de riscos são determinados e acordados.

Para um processo de avaliação de riscos específico, convém que o estabelecimento do contexto inclua a definição do contexto externo, interno e de gestão de riscos e a classificação dos critérios de risco:

a) Estabelecer o contexto externo envolve a familiarização com o ambiente em que a organização e o sistema operam, incluindo:

- os fatores culturais, políticos, legais, regulatórios, financeiros, econômicos e ambientais competitivos, seja em nível internacional, nacional, regional ou local;
- fatores-chave e tendências que tenham impacto sobre os objetivos da organização; e
- percepções e valores das partes interessadas externas.

b) Estabelecer o contexto interno envolve o entendimento

- das capacidades da organização em termos de recursos e conhecimento,
- dos fluxos de informação e processos de tomada de decisão,
- das partes interessadas internas,
- dos objetivos e das estratégias que estão em vigor, a fim de atingi-los,
- das percepções, valores e cultura,
- das políticas e processos,
- de normas e modelos de referência adotados pela organização, e
- das estruturas (por exemplo, governança, papéis e responsabilizações)

NOTA BRASILEIRA	Foi utilizado o termo “responsabilizações” para a tradução de “accountabilities”.

c) Estabelecer o contexto do processo de gestão de riscos inclui

- a definição de responsabilizações e responsabilidades,
- a definição da extensão das atividades de gestão de riscos a serem conduzidas, contemplando inclusões e exclusões específicas,
- a definição da extensão do projeto, processo, função ou atividade em termos de tempo e local,
- a definição das relações entre um projeto ou atividade específicos e outros projetos ou atividades da organização,
- a definição das metodologias do processo de avaliação de riscos,
- a definição dos critérios de risco,
- a definição de como o desempenho na gestão de riscos é avaliado,

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- a identificação e a especificação das decisões e ações que precisam ser tomadas, e
- a identificação dos estudos necessários para o escopo ou enquadramento, sua extensão, e objetivos, e os recursos requeridos para tais estudos.

d) Definir os critérios de risco envolve decidir

- a natureza e os tipos de consequências a serem incluídos e como eles serão medidos,
- a forma como as probabilidades devem ser expressas,
- como um nível de risco será determinado,
- os critérios pelos quais será decidido quando um risco necessita de tratamento,
- os critérios para decidir quando um risco é aceitável e/ou tolerável,
- se e como as combinações de riscos serão levadas em consideração.

Os critérios podem ser baseados em fontes como

- objetivos acordados do processo,
- critérios identificados em especificações,
- fontes gerais de dados,
- critérios setoriais geralmente aceitos, tais como os níveis de integridade de segurança,
- apetite ao risco da organização,
- requisitos legais e outros requisitos para equipamentos ou aplicações específicos.

4.3.4 Processo de avaliação de riscos

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos.

Os riscos podem ser avaliados em nível organizacional, em nível departamental, para projetos, atividades individuais ou riscos específicos. Diferentes ferramentas e técnicas podem ser apropriadas em diferentes contextos.

O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidades. Isto proporciona uma entrada para decisões sobre:

- se convém que uma atividade seja realizada;
- como maximizar oportunidades;
- se os riscos necessitam ser tratados;
- a escolha entre opções com diferentes riscos;
- a priorização das opções de tratamento de riscos;
- a seleção mais apropriada de estratégias de tratamento de riscos que trará riscos adversos a um nível tolerável.

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

4.3.5 Tratamento de riscos

Completado um processo de avaliação de riscos, o tratamento de riscos envolve selecionar e acordar uma ou mais opções pertinentes para alterar a probabilidade de ocorrência, o efeito dos riscos, ou ambos, e a implementação destas opções.

Isto é acompanhado por um processo cíclico de reavaliação do novo nível de risco, tendo em vista a determinação de sua tolerabilidade em relação aos critérios previamente definidos, a fim de decidir se tratamento adicional é requerido.

4.3.6 Monitoramento e análise crítica

Como parte do processo de gestão de riscos, convém que os riscos e os controles sejam regularmente monitorados e analisados criticamente para verificar que

- as premissas sobre os riscos permanecem válidas;
- as premissas nas quais o processo de avaliação de riscos é baseado, incluindo o contexto externo e interno, permanecem válidas;
- os resultados esperados estão sendo alcançados;
- os resultados do processo de avaliação de riscos estão alinhados com a experiência corrente;
- as técnicas do processo de avaliação de riscos estão sendo aplicadas de maneira apropriada;
- os tratamentos de risco são eficazes.

Convém que seja estabelecida a responsabilização pelo monitoramento e pela realização de análises criticas.

5 Processo de avaliação de riscos

5.1 Visão geral

O processo de avaliação de riscos fornece aos tomadores de decisão e às partes responsáveis um entendimento aprimorado dos riscos que poderiam afetar o alcance dos objetivos, bem como a adequação e eficácia dos controles em uso. Isto fornece uma base para decisões sobre a abordagem mais apropriada a ser utilizada para tratar os riscos. A saída do processo de avaliação de riscos é uma entrada para os processos de tomada de decisão da organização.

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos (ver Figura 1). A maneira como este processo é realizado é dependente não somente do contexto do processo de gestão de riscos, mas também dos métodos e técnicas utilizados para conduzir o processo de avaliação de riscos.

Documento impresso em 03/04/2019 15:27:41, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

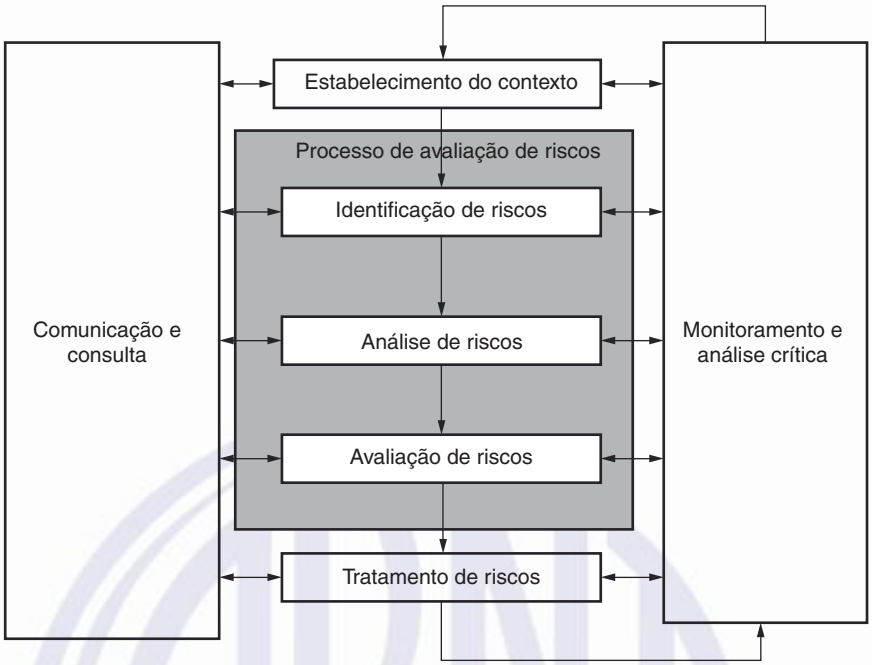

Figura 1 – Contribuição do processo de avaliação de riscos para o processo de gestão de riscos

O processo de avaliação de riscos pode requerer uma abordagem multidisciplinar, uma vez que os riscos podem abranger uma ampla gama de causas e consequências.

5.2 Identificação de riscos

A identificação de riscos é o processo de encontrar, reconhecer e registrar os riscos.

O propósito da identificação de riscos é identificar o que poderia acontecer ou quais situações poderiam existir que poderiam afetar o alcance dos objetivos do sistema ou da organização. Uma vez que um risco é identificado, convém que a organização identifique quaisquer controles existentes, tais como funcionalidades projetadas, pessoas, processos e sistemas.

O processo de identificação de riscos inclui a identificação das causas e fontes do risco (perigo no contexto de dano físico), eventos, situações ou circunstâncias que poderiam ter um impacto material sobre os objetivos e a natureza desse impacto

Os métodos de identificação de riscos podem incluir:

- métodos baseados em evidências, exemplos como listas de verificação e análises críticas de dados históricos;
- abordagens sistemáticas de equipe onde uma equipe de especialistas segue um processo sistemático para identificar os riscos por meio de um conjunto estruturado de instruções ou perguntas;
- técnicas de raciocínio indutivo tais como *HAZOP*.

Várias técnicas de apoio podem ser utilizadas para melhorar a exatidão e completeza na identificação de riscos, incluindo "*brainstorming*" e o método Delphi.

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Independentemente das técnicas efetivamente empregadas, é importante que o devido reconhecimento seja dado a fatores humanos e organizacionais na identificação de riscos. Assim sendo, convém que os desvios dos fatores humanos e organizacionais em relação ao esperado sejam incluídos no processo de identificação de riscos, da mesma forma que os eventos de "*hardware*" ou "*software*".

5.3 Análise de riscos

5.3.1 Generalidades

A análise de riscos diz respeito ao entendimento do risco. Ela fornece uma entrada para o processo de avaliação de riscos e às decisões sobre se os riscos necessitam ser tratados e sobre as estratégias e métodos de tratamento mais apropriados.

A análise de riscos consiste na determinação das consequências e suas probabilidades para eventos identificados de risco, levando em consideração a presença (ou não) e a eficácia de quaisquer controles existentes. As consequências e suas probabilidades são então combinadas para determinar um nível de risco.

A análise de riscos envolve a consideração das causas e fontes de risco, suas consequências e a probabilidade de que essas consequências possam ocorrer. Convém que os fatores que afetam as consequências e a probabilidade sejam identificados. Um evento pode ter múltiplas consequências e pode afetar múltiplos objetivos. Convém que controles de risco existentes e sua eficácia sejam levados em consideração.

Vários métodos para estas análises estão descritos no Anexo B. Mais de uma técnica pode ser requerida para aplicações complexas.

A análise de riscos normalmente inclui uma estimativa da gama de consequências potenciais que podem surgir de um evento, situação ou circunstância, e suas probabilidades associadas, a fim de medir o nível de risco. Entretanto, em alguns casos, tais como quando as consequências prováveis são insignificantes, ou a probabilidade esperada é extremamente baixa, uma única estimativa pode ser suficiente para uma tomada de decisão.

Em algumas circunstâncias, uma consequência pode ocorrer como resultado de uma gama de diferentes eventos ou condições, ou onde o evento específico não é identificado. Neste caso, o foco do processo de avaliação de riscos está na análise da importância e vulnerabilidade dos componentes do sistema com uma visão para definição de tratamentos que se relacionam com os níveis de proteção ou estratégias de recuperação.

Os métodos utilizados na análise de riscos podem ser qualitativos, semi-quantitativos ou quantitativos. O grau de detalhe requerido dependerá da aplicação em particular, da disponibilidade de dados confiáveis e das necessidades de tomada de decisão da organização. Alguns métodos e o grau de detalhe da análise podem ser prescritos pela legislação.

A avaliação qualitativa define consequência, probabilidade e nível de risco por níveis de significância, tais como "alto","médio" e "baixo", pode combinar consequência e probabilidade, e avalia o nível de risco resultante em comparação com os critérios qualitativos.

Os métodos semi-quantitativos utilizam escalas de classificação numérica para consequência e probabilidade e as combinam para produzir um nível de risco utilizando uma fórmula. As escalas podem ser lineares ou logarítmicas, ou podem ter alguma outra relação; as fórmulas utilizadas também podem variar.

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

A análise quantitativa estima valores práticos para consequências e suas probabilidades, e produz valores do nível de risco em unidades específicas definidas quando se desenvolveu o contexto. A análise quantitativa completa pode nem sempre ser possível ou desejável devido a informações insuficientes sobre o sistema ou atividade que está sendo analisado, à falta de dados, à influência dos fatores humanos etc., ou porque o esforço da análise quantitativa não é justificável ou requerido. Em tais circunstâncias uma classificação comparativa semi-quantitativa ou qualitativa de riscos por especialistas, conhecedores em suas respectivas áreas, pode também ser eficaz.

Em casos em que a análise é qualitativa, convém que exista uma explicação clara de todos os termos empregados e que a base para todos os critérios seja registrada.

Mesmo onde uma completa quantificação tenha sido conduzida, é preciso reconhecer que os níveis de risco calculado são estimativas. Convém que se tome cuidado para assegurar que não seja atribuído um nível de exatidão e precisão incompatível com a exatidão dos dados e métodos empregados.

Convém que os níveis de risco sejam expressos nos termos mais adequados para cada tipo de risco e numa forma que auxilie a avaliação de riscos. Em alguns casos, a magnitude de um risco pode ser expressa como uma distribuição da probabilidade sobre uma faixa de consequências.

5.3.2 Avaliação dos controles

O nível de risco dependerá da adequação e eficácia dos controles existentes. As questões a serem abordadas incluem:

- quais são os controles existentes para um risco em particular?
- São esses controles capazes de tratar adequadamente o risco, de modo que ele seja controlado a um nível que seja tolerável?
- na prática, os controles estão operando na forma pretendida e pode ser demonstrado que são eficazes quando requerido?

Estas questões somente podem ser respondidas com confiança se houver documentação e processos de garantia apropriados e implementados.

O nível de eficácia para um controle particular, ou conjunto de controles relacionados, pode ser expresso qualitativa, semi-quantitativa ou quantitativamente. Na maioria dos casos, um alto nível de exatidão não é justificável. Entretanto, pode ser valioso expressar e registrar uma medida de eficácia de controle de riscos de modo que julgamentos possam ser efetuados sobre se o esforço é melhor despendido melhorando um controle ou fornecendo um tratamento de risco diferente.

5.3.3 Análise de consequências

A análise de consequências determina a natureza e o tipo de impacto que pode ocorrer assumindo que uma particular situação, evento ou circunstância ocorreu. Um evento pode ter uma gama de impactos de diferentes magnitudes e afetar uma gama de diferentes objetivos e de diferentes partes interessadas. Os tipos de consequência a serem analisados e as partes interessadas afetadas terão sido decididos quando o contexto foi estabelecido.

A análise de consequências pode variar de uma descrição simples de resultados até uma modelagem quantitativa ou análise de vulnerabilidade detalhadas.

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Os impactos podem ter uma baixa consequência, porém alta probabilidade, ou uma alta consequência e baixa probabilidade, ou algum resultado intermediário. Em alguns casos, é apropriado focar sobre os riscos com resultados potencialmente muito grandes, uma vez que estes são muitas vezes de maior preocupação para os gestores. Em outros casos, pode ser importante analisar os riscos de alta e baixa consequências separadamente. Por exemplo, um problema frequente, porém de baixo impacto (ou crônico) pode ter grandes efeitos cumulativos ou de longo prazo. Além disso, as ações de tratamento para lidar com esses dois tipos distintos de riscos são muitas vezes bastante diferentes, portanto é útil analisá-los separadamente.

A análise de consequências pode envolver:

- levar em consideração os controles existentes para tratar as consequências, juntamente com todos os fatores contributivos pertinentes que tenham um efeito sobre as consequências;
- relacionar as consequências do risco aos objetivos originais;
- considerar tanto as consequências imediatas quanto aquelas que podem surgir após um certo tempo decorrido, se isto for compatível com o escopo da avaliação;
- considerar as consequências secundárias, tais como aquelas que impactam os sistemas, atividades, equipamentos ou organizações associados.

5.3.4 Análise e estimativa de probabilidades

Três abordagens gerais são comumente empregadas para estimar a probabilidade; elas podem ser utilizadas individual ou conjuntamente:

a) A utilização de dados históricos pertinentes para identificar eventos ou situações que ocorreram no passado e, assim, capazes de extrapolar a probabilidade de sua ocorrência no futuro. Convém que os dados utilizados sejam pertinentes ao tipo de sistema, instalação, organização ou atividade que está sendo considerado e também às normas operacionais da organização envolvida. Se historicamente há uma frequência muito baixa de ocorrência, então qualquer estimativa da probabilidade será muito incerta. Isso se aplica especialmente para ocorrências zero, quando não se pode assumir que o evento, situação ou circunstância não ocorrerá no futuro.

b) Previsões de probabilidade utilizando técnicas preditivas tais como análise de árvore de falhas e análise de árvore de eventos (ver Anexo B). Quando os dados históricos forem indisponíveis ou inadequados, é necessário deduzir a probabilidade pela análise do sistema, atividade, equipamento ou organização e seus estados bem sucedidos ou com falha associados. Os dados numéricos para equipamentos, pessoas, organizações e sistemas a partir da experiência operacional ou fontes de dados publicados, são então combinados para produzir uma estimativa da probabilidade do evento principal. Ao utilizar técnicas preditivas, é importante assegurar que a devida consideração tenha sido efetuada na análise para a possibilidade de modos de falha em comum envolvendo a coincidência de falha de um número de partes ou componentes diferentes dentro do sistema, resultantes da mesma causa. Técnicas de simulação podem ser requeridas para gerar a probabilidade de falhas no equipamento ou estruturais devido ao envelhecimento e outros processos de degradação, pelo cálculo dos efeitos das incertezas.

c) A opinião de especialistas pode ser utilizada em um processo sistemático e estruturado para estimar a probabilidade. Convém que os julgamentos dos especialistas recorram a todas as informações pertinentes disponíveis, incluindo informações históricas, específicas do sistema, específicas da organização, experimentais, de projeto etc. Existem diversos métodos formais para induzir o julgamento dos especialistas que fornecem um auxílio para a formulação das questões apropriadas. Os métodos disponíveis incluem a abordagem Delphi, comparações emparelhadas, classificação de categorias e julgamentos de probabilidade absoluta.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

5.3.5 Análise preliminar

Os riscos podem ser filtrados a fim de identificar os riscos mais significativos ou para excluir riscos menos significativos ou menores de análises adicionais. O objetivo é assegurar que os recursos serão focados sobre os riscos mais importantes. Convém que se tome cuidado para não deixar de fora riscos baixos que ocorrem com frequência e tenham um efeito cumulativo significativo.

Convém que a seleção seja baseada em critérios definidos no contexto. A análise preliminar determina um ou mais dos seguintes modos de ação:

- decidir tratar os riscos sem avaliação adicional;
- excluir riscos insignificantes que não justificariam tratamento;
- proceder a um processo de avaliação de riscos mais detalhado.

Convém que as premissas iniciais e os resultados sejam documentados.

5.3.6 Incertezas e sensibilidades

Muitas vezes há incertezas consideráveis associadas à análise de riscos. Um entendimento das incertezas é necessário para interpretar e comunicar os resultados da análise de riscos eficazmente. A análise das incertezas associadas aos dados, métodos e modelos utilizados para identificar e analisar o risco desempenha um papel importante na sua aplicação. A análise de incertezas envolve a determinação da variação ou imprecisão nos resultados, decorrentes da variação coletiva nos parâmetros e premissas utilizados para definir os resultados. Uma área estreitamente relacionada à análise de incertezas é a análise de sensibilidade.

A análise de sensibilidade envolve a determinação do tamanho e significância da magnitude do risco resultante de alterações nos parâmetros de entrada individuais. Ela é utilizada para identificar aqueles dados que necessitam ser exatos e aqueles que são menos sensíveis e, assim tem, menos efeito sobre a exatidão total.

Convém que a completeza e a exatidão da análise de riscos sejam estabelecidas tão completamente quanto possível. Convém que as fontes de incerteza sejam identificadas onde possível e convém que abordem tanto as incertezas dos dados quanto as do modelo/método. Convém que os parâmetros para os quais a análise é sensível, e o grau de sensibilidade, sejam explicitados.

5.4 Avaliação de riscos

A avaliação de riscos consiste em comparar os níveis estimados de risco com critérios de risco definidos quando o contexto foi estabelecido, a fim de determinar a significância do nível e do tipo de risco.

A avaliação de riscos utiliza a compreensão do risco, obtida durante a análise de riscos, para tomar decisões sobre as ações futuras. Considerações éticas, legais, financeiras e outras, incluindo as percepções do risco, são também dados de entrada para a decisão.

As decisões podem incluir:

- se um risco necessita de tratamento;
- as prioridades para o tratamento;

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- se uma atividade deve ser realizada;
- qual de um número de caminhos alternativos deve ser seguido.

A natureza das decisões que necessitam ser tomadas e os critérios que serão utilizados para tomar essas decisões foram decididos no estabelecimento do contexto, mas precisam ser revistos em mais detalhes nesta fase, agora que se sabe mais sobre os riscos identificados em particular.

A estrutura mais simples para a definição dos critérios de risco é um nível único que divide os riscos que necessitam de tratamento daqueles que não necessitam. Isso fornece resultados atrativamente simples, porém não reflete as incertezas envolvidas na estimativa de riscos e na definição da fronteira entre aqueles que necessitam de tratamento e aqueles que não necessitam.

A decisão sobre se e como tratar o risco pode depender dos custos e benefícios de assumir o risco e os custos e benefícios da implementação de controles melhorados.

Uma abordagem comum é dividir os riscos em três faixas:

a) uma faixa superior, onde o nível de risco é considerado intolerável quaisquer que sejam os benefícios que possam trazer à atividade, e o tratamento de risco é essencial qualquer que seja o seu custo;

b) uma faixa intermediária (ou área “cinzenta”) onde os custos e benefícios são levados em consideração, e oportunidades são comparadas com potenciais consequências;

c) uma faixa inferior, onde o nível de risco é considerado desprezível ou tão pequeno que nenhuma medida de tratamento de risco seja necessária.

O sistema de critérios tão baixo quanto for razoavelmente praticável ou *ALARP* (*As Low As Reasonably Practicable*) utilizado em aplicações de segurança segue esta abordagem, onde, na faixa intermediária, há uma escala móvel para baixos riscos – onde os custos e benefícios podem ser diretamente comparados –, enquanto que para altos riscos o potencial de danos tem que ser reduzido até que o custo de redução adicional seja inteiramente desproporcional ao benefício de segurança adquirido.

5.5 Documentação

Convém que o processo de avaliação de riscos seja documentado juntamente com os resultados do processo de avaliação. Convém que os riscos sejam expressos em termos compreensíveis, e convém que as unidades em que o nível de risco é expresso sejam claras.

A extensão do relatório dependerá dos objetivos e do escopo da avaliação. Exceto para avaliações muito simples, a documentação pode incluir:

- objetivos e escopo;
- descrição de partes pertinentes do sistema e suas funções;
- um resumo dos contextos externo e interno da organização e como eles se relacionam com a situação, sistema ou circunstâncias que estão sendo avaliados;
- os critérios de risco aplicados e sua justificativa;
- limitações, premissas e justificativa de hipóteses;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- metodologia de avaliação;
- resultados da identificação de riscos;
- dados, premissas e suas fontes e validação;
- resultados da análise de riscos e sua avaliação;
- análise de sensibilidade e de incerteza;
- premissas críticas e outros fatores que necessitam ser monitorados;
- discussão dos resultados;
- conclusões e recomendações;
- referências.

Se o processo de avaliação de riscos apoia um processo sistemático de gestão de riscos, convém que seja realizado e documentado de tal forma que possa ser mantido durante o ciclo de vida do sistema, organização, equipamento ou atividade. Convém que a avaliação seja atualizada sempre que novas informações significativas estejam disponíveis e o contexto se altere, de acordo com as necessidades do processo de gestão.

5.6 Monitoramento e análise crítica do processo de avaliação de riscos

O processo de avaliação de riscos destacará o contexto e outros fatores que se pode esperar que variem ao longo do tempo e que poderiam alterar ou invalidar o processo de avaliação de riscos. Convém que estes fatores sejam especificamente identificados para o contínuo monitoramento e análise crítica, de modo que o processo de avaliação de riscos possa ser atualizado quando necessário.

Convém também que os dados a serem monitorados para refinar o processo de avaliação de riscos sejam identificados e coletados.

Convém que a eficácia dos controles também seja monitorada e documentada a fim de fornecer dados para uso na análise de riscos. Convém que as responsabilidades para a criação e análise crítica das evidências e da documentação sejam definidas.

5.7 Aplicação do processo de avaliação de riscos durante as fases do ciclo de vida

Muitas atividades, projetos e produtos podem ser considerados como tendo um ciclo de vida que se inicia a partir do conceito e definição iniciais, passa pela realização até uma conclusão final que pode incluir o descomissionamento e descarte final do *hardware*.

O processo de avaliação de riscos pode ser aplicado a todos os estágios do ciclo de vida e é normalmente aplicado muitas vezes com diferentes níveis de detalhe para auxiliar nas decisões que precisam ser tomadas em cada fase.

As fases dos ciclos de vida têm requisitos diferentes e necessitam de diferentes técnicas. Por exemplo, durante a fase de conceito e definição, quando uma oportunidade é identificada, o processo de avaliação de riscos pode ser utilizado para decidir se se quer continuar ou não.

Onde diversas opções estiverem disponíveis, o processo de avaliação de riscos pode ser utilizado para avaliar conceitos alternativos para auxiliar na decisão sobre quais proporcionam o melhor balanço entre os riscos positivos e negativos.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Durante a fase de projeto e desenvolvimento, o processo de avaliação de riscos contribui para

- assegurar que os riscos do sistema são toleráveis,
- o processo de refinamento do projeto,
- os estudos de do custo-eficácia,
- identificação dos riscos que impactam as fases subsequentes do ciclo de vida.

Conforme a atividade progride, o processo de avaliação de riscos pode ser utilizado para fornecer informações que auxiliem no desenvolvimento de procedimentos para condições normais e de emergência.

6 Seleção de técnicas para o processo de avaliação de riscos

6.1 Generalidades

Esta Seção descreve como as técnicas para o processo de avaliação de riscos podem ser selecionadas. Os anexos listam e explicam em detalhes uma gama de ferramentas e técnicas que podem ser utilizadas para realizar um processo de avaliação de riscos ou auxiliar no processo de avaliação de riscos. Algumas vezes pode ser necessário empregar mais de um método de avaliação.

6.2 Seleção de técnicas

O processo de avaliação de riscos pode ser conduzido em vários graus de profundidade e detalhe e utilizando um ou muitos métodos que vão do simples ao complexo. Convém que a forma de avaliação e sua saída sejam compatíveis com os critérios de risco, desenvolvidos como parte do estabelecimento do contexto. O Anexo A ilustra a relação conceitual entre as amplas categorias das técnicas para o processo de avaliação de riscos e os fatores presentes numa determinada situação de risco e fornece exemplos ilustrativos de como as organizações podem selecionar as técnicas apropriadas para o processo de avaliação de riscos para uma situação em particular.

Em termos gerais, convém que as técnicas apropriadas apresentem as seguintes características:

- convém que sejam justificáveis e apropriadas à situação ou organização em questão;
- convém que proporcionem resultados de uma forma que amplie o entendimento da natureza do risco e de como ele pode ser tratado;
- convém que sejam capazes de utilizar uma forma que seja rastreável, repetível e verificável.

Convém que as razões para a escolha das técnicas sejam dadas com relação a pertinência e adequação. Ao integrar os resultados de diferentes estudos, convém que as técnicas utilizadas e as saídas sejam comparáveis.

Uma vez que a decisão tenha sido tomada para realizar um processo de avaliação de riscos e os objetivos e o escopo tenham sido definidos, convém que as técnicas sejam selecionadas com base em fatores aplicáveis, tais como:

- os objetivos do estudo. Os objetivos do processo de avaliação de riscos terão uma influência direta sobre as técnicas utilizadas. Por exemplo, se um estudo comparativo entre as diferentes opções está sendo realizado, pode ser aceitável utilizar modelos menos detalhados de consequência para partes do sistema não afetadas pela diferença;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- as necessidades dos tomadores de decisão. Em alguns casos, um alto nível de detalhe é necessário para tomar uma boa decisão, em outros um entendimento mais geral é suficiente;
- o tipo e a gama de riscos que estão sendo analisados;
- a magnitude potencial das consequências. Convém que a decisão sobre a profundidade em que o processo de avaliação de riscos é conduzido reflita a percepção inicial das consequências (embora isto possa ter que ser modificado uma vez que uma avaliação preliminar foi concluída);
- o grau de conhecimento especializado, recursos humanos e outros recursos necessários. Um método simples e bem feito pode fornecer melhores resultados do que um procedimento mais sofisticado e mal feito, contanto que atenda aos objetivos e o escopo do processo de avaliação. Normalmente, convém que o esforço aplicado ao processo de avaliação seja compatível com o nível potencial de risco que está sendo analisado;
- a disponibilidade de informações e dados. Algumas técnicas requerem mais informações e dados do que outras;
- a necessidade de modificação/atualização do processo de avaliação de riscos. O processo de avaliação pode necessitar ser modificado/atualizado no futuro e algumas técnicas são mais ajustáveis do que outras a este respeito;
- quaisquer requisitos regulatórios e contratuais.

Vários fatores influenciam a seleção de uma abordagem ao processo de avaliação de riscos, tais como a disponibilidade de recursos, a natureza e o grau de incerteza nos dados e informações disponíveis, bem como a complexidade da aplicação (ver Tabela A.2).

6.3 Disponibilidade de recursos

Os recursos e as capacidades que podem afetar a seleção de técnicas do processo de avaliação de riscos incluem:

- as habilidades, experiência, capacidade e competência da equipe do processo de avaliação de riscos;
- as restrições de tempo e outros recursos dentro da organização;
- o orçamento disponível, se recursos externos forem requeridos.

6.4 A natureza e o grau de incerteza

A natureza e o grau de incerteza requerem um entendimento da qualidade, quantidade e integridade das informações disponíveis sobre o risco em consideração. Isto inclui quão disponíveis e suficientes são as informações sobre o risco, suas fontes e causas, e suas consequências para o atendimento dos objetivos. A incerteza pode ser proveniente da qualidade pobre dos dados ou da falta de dados essenciais e confiáveis. Para ilustrar, os métodos de coleta de dados podem se modificar, a forma que as organizações utilizam tais métodos pode ser alterada ou a organização pode simplesmente não ter um método de coleta eficaz implementado, para coleta de dados sobre o risco identificado.

A incerteza também pode ser inerente aos contextos externo e interno da organização. Os dados disponíveis nem sempre fornecem uma base confiável para a previsão do futuro. Para tipos singulares de riscos, os dados históricos podem não estar disponíveis ou pode haver diferentes interpretações de dados disponíveis por diferentes partes interessadas. Os encarregados do processo de avaliação

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

de riscos precisam entender o tipo e a natureza da incerteza e interpretar suas implicações para a confiabilidade dos resultados do processo de avaliação de riscos. Convém que isto seja sempre comunicado aos tomadores de decisão.

6.5 Complexidade

Os riscos podem ser complexos em si mesmos, como, por exemplo, em sistemas complexos que precisam ter seus riscos avaliados em todo o sistema ao invés de tratar cada componente separadamente e ignorando as interações. Em outros casos, tratar um risco individual pode ter implicações em outros locais e pode impactar outras atividades. Os impactos resultantes e as dependências do risco necessitam ser entendidos para assegurar que na gestão de um determinado risco, uma situação intolerável não seja criada em outros locais. Entender a complexidade de um risco individual ou de um portfólio de riscos de uma organização é crucial para a seleção do método adequado ou técnicas para o processo de avaliação de riscos.

6.6 Aplicação do processo de avaliação de riscos durante as fases do ciclo de vida

Muitas atividades, projetos e produtos podem ser considerados como tendo um ciclo de vida que se inicia a partir do conceito e definição inicial, passa pela realização e vai até o encerramento final que poderá incluir a desmontagem e descarte do *equipamento*.

O processo de avaliação de riscos pode ser aplicado em todos os estágios do ciclo de vida e é normalmente aplicado muitas vezes com diferentes níveis de detalhe para auxiliar nas decisões que precisam ser tomadas em cada fase.

As fases dos ciclos de vida têm necessidades diferentes e requerem diferentes técnicas. Por exemplo, durante a fase de concepção e definição, quando uma oportunidade é identificada, o processo de avaliação de riscos pode ser utilizado para decidir se convém continuar ou não.

Quando diversas opções estiverem disponíveis, o processo de avaliação de riscos pode ser utilizado para avaliar conceitos alternativos a fim de auxiliar na decisão sobre quais proporcionam o melhor equilíbrio de riscos.

Durante a fase de projeto e desenvolvimento, o processo de avaliação de riscos contribui para

- assegurar que os riscos do sistema são toleráveis,
- o processo de refinamento do projeto,
- os estudos de eficácia do custo,
- identificação dos riscos que impactam as fases subsequentes do ciclo de vida.

Conforme a atividade progride, o processo de avaliação de riscos pode ser utilizado para fornecer informações que auxiliem no desenvolvimento de procedimentos para condições normais e de emergência.

6.7 Tipos de técnicas do processo de avaliação de riscos

As técnicas do processo de avaliação de riscos podem ser classificadas de várias formas para auxiliar no entendimento de seus pontos fortes e fracos relativos. As tabelas no Anexo A correlacionam algumas técnicas potenciais e suas categorias para fins ilustrativos.

Cada uma das técnicas é descrita com mais detalhes no Anexo B quanto à natureza da avaliação que elas fornecem e a orientação para sua aplicabilidade em certas situações.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Anexo A
(informativo)

Comparação das técnicas para o processo de avaliação de riscos

A.1 Tipos de técnicas

A primeira classificação mostra como as técnicas se aplicam para cada etapa do processo de avaliação de riscos conforme descrito a seguir:

- identificação de riscos;
- análise de riscos – análise de consequências;
- análise de riscos – estimativa qualitativa, semi-quantitativa ou quantitativa da probabilidade;
- análise de riscos – avaliação da eficácia de quaisquer controles existentes;
- análise de riscos – estimativa do nível de risco;
- avaliação de riscos.

Para cada etapa no processo de avaliação de riscos, a aplicação do método é descrita como sendo fortemente aplicável, aplicável ou não aplicável (ver Tabela A.1).

A.1.1 Fatores que influenciam na seleção das técnicas para o processo de avaliação de riscos

Em seguida os atributos dos métodos são descritos em termos

- da complexidade do problema e os métodos necessários para analisá-lo,
- da natureza e o grau de incerteza do processo de avaliação de riscos baseado na quantidade de informações disponíveis e o que é requerido para atender aos objetivos,
- da extensão de recursos requeridos em termos de tempo e nível de conhecimento especializado, necessidades de dados ou custo,
- se o método pode fornecer uma saída quantitativa.

Os exemplos de tipos de métodos disponíveis para o processo de avaliação de riscos estão listados na Tabela A.2, onde cada método é classificado como alto, médio ou baixo em função desses atributos.

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Tabela A.1 – Aplicabilidade das ferramentas utilizadas para o processo de avaliação de riscos

Ferramentas e técnicas	Processo de avaliação de riscos					Ver Anexo
	Identificação de riscos	Análise de riscos			Avaliação de riscos	
		Consequência	Probabilidade	Nível de risco		
Brainstorming	FA [1]	NA [2]	NA	NA	NA	B 01
Entrevistas estruturadas ou semi-estruturadas	FA	NA	NA	NA	NA	B 02
Delphi	FA	NA	NA	NA	NA	B 03
Listas de verificação	FA	NA	NA	NA	NA	B 04
Análise preliminar de perigos (APP)	FA	NA	NA	NA	NA	B 05
Estudo de perigos e operabilidade (HAZOP)	FA	FA	A [3]	A	A	B 06
Análise de perigos e pontos críticos de controle (APPCC)	FA	FA	NA	NA	FA	B 07
Avaliação de risco ambiental	FA	FA	FA	FA	FA	B 08
Técnica estruturada "E se" (SWIFT)	FA	FA	FA	FA	FA	B 09
Análise de cenários	FA	FA	A	A	A	B 10
Análise de impactos no negócio	A3	FA	A	A	A	B 11
Análise de causa-raiz	NA	FA	FA	FA	FA	B 12
Análise de modos de falha e efeito	FA	FA	FA	FA	FA	B 13
Análise de árvore de falhas	A	NA	FA	A	A	B 14
Análise de árvore de eventos	A	FA	A	A	NA	B 15
Análise de causa e conseqüência	A	FA	FA	A	A	B 16
Análise de causa e efeito	FA	FA	NA	NA	NA	B 17
Análise de camadas de proteção (LOPA)	A	FA	A	A	NA	B 18
Árvore de decisões	NA	FA	FA	A	A	B 19
Análise da confiabilidade humana	FA	FA	FA	FA	A	B 20
Análise *Bow tie*	NA	A	FA	FA	A	B 21
Manutenção centrada em confiabilidade	FA	FA	FA	FA	FA	B 22

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Tabela A.1 (continuação)

Ferramentas e técnicas	Processo de avaliação de riscos					Ver Anexo
	Identificação de riscos	Análise de riscos			Avaliação de riscos	
		Consequência	Probabilidade	Nível de risco		
Sneak analysis (SA) e sneak circuit analysis (SCA)	A	NA	NA	NA	NA	B 23
Análise de Markov	A	FA	NA	NA	NA	B 24
Simulação de Monte Carlo	NA	NA	NA	NA	FA	B 25
Estatística Bayesiana e Redes de Bayes	NA	FA	NA	NA	FA	B 26
Curvas FN	A	FA	FA	A	FA	B 27
Índices de risco	A	FA	FA	A	FA	B 28
Matriz de probabilidade/ consequência	FA	FA	FA	FA	A	B 29
Análise de custo/benefício	A	FA	A	A	A	B 30
Análise de decisão por multicritérios (MCDA)	A	FA	A	FA	A	B 31

1 FA - Fortemente aplicável.

2 NA - Não aplicável.

3 A - Aplicável.

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Tabela A.2 – Atributos de uma seleção de ferramentas de avaliação de riscos

Tipo de técnica para o processo de avaliação de riscos	Descrição	Pertinência da influência de fatores			Pode fornecer resultados quantitativos?
		Recursos e capacidade	Natureza e grau de incerteza	Complexidade	
MÉTODOS DE CONSULTA					
Listas de verificação (*checklists*)	Uma forma simples de identificação de riscos. Uma técnica que fornece uma lista de incertezas típicas que precisam ser consideradas. Os usuários consultam uma lista, códigos ou normas previamente desenvolvidos	Baixo	Baixo	Baixa	Não
Análise preliminar de perigos	Um método simples de análise indutiva cujo objetivo é identificar os perigos e situações e eventos perigosas que podem causar danos para uma determinada atividade, instalação ou sistema	Baixo	Alto	Média	Não
MÉTODOS DE APOIO					
Entrevista estruturada e *brainstorming*	Um meio da coletar um amplo conjunto de idéias e avaliação, classificando-o por uma equipe. O *brainstorming* pode ser estimulado através de instruções ou por técnicas de entrevista	Baixo	Baixo	Baixa	Não
Técnica de Delphi	Um meio de combinar opiniões de especialistas que possam apoiar a fonte e influenciar a estimativa de identificação, probabilidade e consequência e a avaliação de riscos. É uma técnica colaborativa para a construção de um consenso entre os especialistas. Envolve a análise independente e voto dos especialistas	Médio	Médio	Média	Não
SWIFT *Structured What If Technique*	Um sistema para solicitar uma equipe para identificar os riscos. Normalmente é utilizada dentro de um *workshop* facilitado. Normalmente associada a uma técnica de análise e avaliação de riscos	Médio	Médio	Qualquer	Não
Análise de confiabilidade humana (ACH)	A avaliação da confiabilidade humana (HRA) trata do impacto de humanos sobre o desempenho do sistema e pode ser utilizada para avaliar as influências de erro humano no sistema	Médio	Médio	Média	Sim
ANÁLISE DE CENÁRIO					
	Uma única perda que ocorreu é analisada a fim de entender as causas contributivas e como o sistema ou processo pode ser melhorado para evitar perdas futuras. A análise deve considerar quais controles estavam em prática no momento da perda ocorrida e como os controles podem ser melhorados	Médio	Baixo	Média	Não

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Tabela A.2 (continuação)

Tipo de técnica de avaliação de risco	Descrição	Relevância da influência de fatores			Pode prover resultados quantitativos?
		Recursos e capacidade	Natureza e grau de incerteza	Complexidade	
Análise de cenário	Possíveis cenários futuros são identificados através da imaginação ou extrapolação dos riscos atuais e diferentes considerados, presumindo que cada um desses cenários pode ocorrer. Isto pode ser feito formal ou informalmente, qualitativa ou quantitativamente	Médio	Alto	Média	Não
Avaliação de risco toxicológico	Os perigos são identificados e analisados e os possíveis caminhos pelos quais um alvo especificado pode ser exposto ao perigo são identificados. Informações sobre o nível de exposição e a natureza dos danos causados por um determinado nível de exposição são combinados para dar uma medida da probabilidade de que o dano especificado ocorrerá	Alto	Alto	Média	Sim
Análise de impacto nos negócios	Provê uma análise de como os principais riscos de quebra podem afetar as operações de uma organização e identifica e quantifica as capacidades que seriam requeridas para gerenciá-los	Médio	Médio	Média	Não
Análise de árvore de falhas	Uma técnica que se inicia com o evento indesejado (evento de topo) e determina todas as formas em que ele poderia ocorrer. Estes são apresentados graficamente em um diagrama de árvore lógica. Uma vez que a árvore de falhas foi desenvolvida, consideração deve ser dada às formas de reduzir ou eliminar as causas/fontes potenciais	Alto	Alto	Média	Sim
Análise de árvore de eventos	Utilizando o raciocínio indutivo para traduzir as probabilidades de diferentes eventos iniciais em resultados possíveis	Médio	Médio	Média	Sim
Análise de causa e consequência	Uma combinação da análise de árvore de falhas e eventos que permite a inclusão de atrasos no tempo. Ambas as causas e consequências de um evento inicial são consideradas	Alto	Médio	Alta	Sim
Análise de causa e efeito	Um efeito pode ter um número de fatores contributivos que podem ser agrupados em diferentes categorias. Os fatores contributivos são identificados muitas vezes através de *brainstorming* e apresentados em um diagrama de estrutura de árvore ou espinha de peixe	Baixo	Baixo	Média	N 20ão

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Tabela A.2 (continuação)

Tipo de técnica de avaliação de risco	Descrição	Relevância da influência de fatores			Pode prover resultados quantitativos?
		Recursos e capacidade	Natureza e grau de incerteza	Complexidade	
FMEA e FMECA	A FMEA (Análise de modos de falha e efeitos) é uma técnica que identifica os modos e os mecanismos de falha e seus efeitos. Existem diversos tipos de FMEA: FMEA de Projeto (ou produto) que é utilizada para componentes e produtos, FMEA de Sistema que é utilizada para sistemas, FMEA de Processo que é utilizada para processos de manufatura e montagem, FMEA de Serviço e FMEA de *Software* A FMEA pode ser seguida por uma análise de criticidade que define a significância de cada modo de falha, qualitativamente, semi-qualitativamente ou quantitativamente (FMECA). A análise de criticidade pode ser baseada na probabilidade de que o modo de falha resultará em falha do sistema, ou o nível de risco associado com o modo de falha, ou um número prioritário do risco	Médio	Médio	Média	Sim
Manutenção centrada em confiabilidade	Um método para identificar as políticas que devem ser implementadas para gerenciar as falhas de modo a atingir com eficiência e eficácia a segurança, disponibilidade e economia de operação requeridas para todos os tipos de equipamento.	Médio	Médio	Média	Sim
Análise transitória (Análise de circuitos ocultos)	Uma metodologia para a identificação de erros de projeto. A condição transitória é um *hardware*, *software* ou condição integrada latente que pode causar um evento indesejado de ocorrer ou pode inibir um evento desejado e não é causada pela falha do componente. Essas condições são caracterizadas por sua natureza aleatória e da capacidade de escapar à detecção durante os mais rigorosos ensaios de sistemas padronizados. As condições transitórias podem causar operação imprópria, perda de disponibilidade do sistema, atrasos no programa ou mesmo a morte ou ferimento às pessoas	Médio	Médio	Média	Não
HAZOP[3] Estudo de perigos e operabilidade	Um processo geral de identificação de riscos para definir possíveis desvios do desempenho esperado ou pretendido. Ela utiliza um sistema baseado em palavras–guia. As criticidades dos desvios são avaliadas	Médio	Alta	Alta	Não

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Tabela A.2 (continuação)

Tipo de técnica de avaliação de risco	Descrição	Relevância da influência de fatores			Pode prover resultados quantitativos?
		Recursos e capacidade	Natureza e grau de incerteza	Complexidade	
APPCC Análise de perigos e pontos críticos de controle	Um sistema proativo, preventivo e sistemático para assegurar a qualidade do produto, confiabilidade e segurança de processos através da medição e monitoramento das características específicas que são requeridas para estarem dentro dos limites definidos	Médio	Médio	Média	Não
AVALIAÇÃO DE CONTROLES					
LOPA[4] Análise de camadas de proteção	(Também pode ser chamada de análise de barreira). Ela permite que os controles e a sua eficácia sejam avaliados	Médio	Médio	Média	Sim
Análise da gravata borboleta (*Bow tie*)	Uma forma esquemática simples de descrever e analisar os caminhos de um risco dos perigos até os resultados e a revisão de controles. Ela pode ser considerada uma combinação da lógica de uma árvore de falhas analisando a causa de um evento (representada pelo nó de uma gravata borboleta) e uma árvore de eventos analisando as consequências	Médio	Alto	Média	Sim
MÉTODOS ESTATÍSTICOS					
Análise de Markov	A análise de Markov, algumas vezes chamada de análise de *Estado espacial*, é comumente utilizada na análise de sistemas complexos reparáveis que podem existir em múltiplos estados, incluindo vários estados degradados	Alto	Baixo	Alta	Sim
Análise de Monte Carlo	A simulação de Monte Carlo é utilizada para estabelecer a variação agregada em um sistema resultante das variações no sistema, para um número de entradas, onde cada entrada tem uma distribuição definida e as entradas são relativas aos relacionamentos definidos nos resultados. A análise pode ser utilizada para um modelo específico onde as interações de várias entradas podem ser definidas matematicamente. As entradas podem ser baseadas sob uma variedade de tipos de distribuição de acordo com a natureza da incerteza que são destinadas a representar. Para avaliação de riscos, distribuições triangular ou distribuições beta são comumente utilizadas	Alto	Baixo	Alta	Sim
Análise Bayesiana	Um procedimento estatístico que utiliza dados de distribuição anteriores para avaliar a probabilidade do resultado. A análise Bayesiana depende da exatidão da distribuição anterior para deduzir um resultado exato. As redes Bayesianas modelam a causa e efeito em uma variedade de domínios capturando relacionamentos probabilísticos de entradas variáveis para derivar um resultado	Alto	Baixo	Alta	Sim

[1] SWIFT - Structured What If Technique
[2] HRA - Human resource accounting
[3] HAZOP - Hazard and Operability Studies
[4] LOPA - Layer Protection Analysis

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Anexo B
(informativo)

Técnicas para o processo de avaliação de risco

B.1 *Brainstorming*

B.1.1 Visão geral

O *Brainstorming* envolve estimular e incentivar o livre fluxo de conversação entre um grupo de pessoas conhecedoras para identificar os modos de falha potenciais e os perigos e riscos associados, os critérios para decisões e/ou opções para tratamento. O termo "*brainstorming*" é frequentemente utilizado muito livremente para qualquer tipo de discussão em grupo. Entretanto, o verdadeiro *brainstorming* envolve técnicas específicas para tentar assegurar que a imaginação das pessoas é provocada pelos pensamentos e declarações de outras pessoas no grupo.

A facilitação eficaz é muito importante nesta técnica e inclui o estímulo da discussão desde o início, provocando periodicamente o grupo em outras áreas pertinentes e a captura das questões que emergem da discussão (que normalmente é bastante intensa).

B.1.2 Utilização

O *Brainstorming* pode ser utilizado em conjunto com outros métodos para o processo de avaliação de riscos descritos a seguir ou pode ser utilizado sozinho como uma técnica para incentivar o pensamento criativo em qualquer estágio do processo de gestão de riscos e qualquer estágio do ciclo de vida de um sistema. Ele pode ser utilizado para discussões de alto nível onde as questões são identificadas, para análise crítica mais detalhada ou num nível detalhado para problemas em particular.

O *Brainstorming* põe uma forte ênfase na imaginação. Portanto, ele é particularmente útil ao identificar os riscos de novas tecnologias, onde não existem dados ou onde soluções inovadoras para os problemas são necessárias.

B.1.3 Entradas

Uma equipe de pessoas com conhecimento da organização, sistema, processo ou aplicação a ser avaliado.

B.1.4 Processo

O *Brainstorming* pode ser formal ou informal. O *brainstorming* formal é mais estruturado com participantes preparados com antecedência e a sessão tem um objetivo definido e resultados com um recurso de avaliar as idéias apresentadas. O *brainstorming* informal é menos estruturado e muitas vezes mais *ad-hoc*.

Em um processo formal:

- o facilitador prepara instruções e estímulos para o pensamento apropriados ao contexto previamente à sessão;
- os objetivos da sessão são definidos e as regras explicadas;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- o facilitador começa uma linha de pensamento e qualquer um explora idéias identificando tantas questões quanto possível. Não há discussão neste momento sobre se as coisas devem ou não devem estar numa lista ou o que se entende por declarações particulares, porque isto tende a inibir o livre fluxo do pensamento. Todas as entradas são aceitas e nenhuma é criticada e o grupo prossegue rapidamente para permitir idéias que estimulem o pensamento lateral;

- o facilitador pode estabelecer que as pessoas se desviem para uma nova pista quando uma direção de pensamento é esgotada ou a discussão se desvia demasiado do assunto. A idéia, porém, é coletar o maior número possível de idéias para análise posterior.

B.1.5 Saídas

As saídas dependem do estágio do processo de gestão de riscos em que é aplicado, por exemplo, no estágio de identificação, as saídas podem ser uma lista de riscos e controles atuais.

B.1.6 Pontos fortes e limitações

Os pontos fortes do *brainstorming* incluem:

- o incentivo à imaginação que ajuda a identificar novos riscos e soluções inovadoras;

- o envolvimento das partes interessadas chave e, consequentemente, no auxílio à comunicação global;

- a relativamente rápida e fácil preparação.

As limitações incluem:

- os participantes podem não ter a habilidade e conhecimento para serem eficazes contribuidores;

- uma vez que é relativamente não-estruturado, é difícil demonstrar que o processo foi abrangente, por exemplo, que todos os riscos potenciais foram identificados;

- pode haver dinâmicas de grupo particulares onde algumas pessoas com idéias valiosas permanecem quietas enquanto outras dominam a discussão. Isso pode ser superado por *brainstorming* em computador utilizando um fórum de discussão ou técnica de grupo nominal. O *brainstorming* em computador pode ser configurado para ser anônimo, evitando assim que questões pessoais e políticas possam impedir o livre fluxo de idéias. Na técnica de grupo nominal, as idéias são submetidas anonimamente a um moderador e em seguida discutidas pelo grupo.

B.2 Entrevistas estruturadas ou semi-estruturadas

B.2.1 Visão geral

Em uma entrevista estruturada, os entrevistados são solicitados individualmente a responder a um conjunto de questões pré-elaboradas que constam de um roteiro de instruções e que incentivam o entrevistado a ver uma situação a partir de uma perspectiva diferente e, assim, identificar os riscos a partir desta perspectiva. Uma entrevista semi-estruturada é semelhante, porém permite mais liberdade para uma conversa que explore questões que surjam.

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.2.2 Utilização

As entrevistas estruturadas e semi-estruturadas são úteis quando for difícil reunir as pessoas para uma sessão de *brainstorming* ou quando o livre fluxo de discussão em um grupo não é apropriado para a situação ou pessoas envolvidas. São muitas vezes utilizadas para identificar os riscos ou avaliar a eficácia dos controles existentes como parte da análise de risco. Podem ser aplicadas em qualquer estágio de um projeto ou processo. São um meio de fornecer as entradas para o processo de avaliação de riscos pelas partes interessadas

B.2.3 Entradas

As entradas incluem:

- uma definição clara dos objetivos das entrevistas;
- uma lista de entrevistados selecionados dentre as partes interessadas pertinentes;
- um conjunto de perguntas pré-elaboradas.

B.2.4 Processo

Um conjunto pertinente de perguntas é criado para orientar o entrevistador. Convém que as perguntas sejam abertas sempre que possível, que sejam simples, em linguagem apropriada para o entrevistado e que abranjam somente uma questão de cada vez. Também são preparadas questões adicionais para buscar maior clareza.

As perguntas são então apresentadas à pessoa que está sendo entrevistada. Quando se pretender respostas elaboradas, convém que as perguntas sejam abertas. Cuidado deve ser tomado para não “conduzir” o entrevistado.

Convém que as respostas sejam consideradas com um certo grau de flexibilidade, a fim de dar a oportunidade ao entrevistado de explorar as áreas que desejar.

B.2.5 Saídas

As saídas são as visões das partes interessadas sobre as questões que são o objeto das entrevistas.

B.2.6 Pontos fortes e limitações

Os pontos fortes das entrevistas estruturadas são os seguintes:

- as entrevistas estruturadas permitem às pessoas tempo para refletir sobre uma questão;
- a comunicação pessoa-a-pessoa pode permitir considerações mais aprofundadas das questões;
- as entrevistas estruturadas permitem o envolvimento de um maior número de partes interessadas do que o *brainstorming*, o qual utiliza um grupo relativamente pequeno.

As limitações são as seguintes:

- é dispendioso em termos de tempo para o facilitador a obtenção de opiniões múltiplas desta forma;

Documento impresso em 03/04/2019 15:30:29, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- vieses são tolerados e não removidos por meio de discussão em grupo;
- o desencadeamento da imaginação que é uma característica do *brainstorming*, pode não ser atingido.

B.3 Técnica Delphi

B.3.1 Visão geral

A técnica Delphi é um procedimento para obter um consenso confiável de opiniões de um grupo de especialistas. Embora muitas vezes o termo seja agora amplamente utilizado para significar qualquer forma de *brainstorming*, uma característica essencial da técnica Delphi, como originalmente formulada, era a de que os especialistas expressavam suas opiniões individual e anonimamente e tinham acesso aos pontos de vista de outros especialistas à medida o processo evoluía.

B.3.2 Utilização

A técnica Delphi pode ser aplicada em qualquer estágio do processo de gestão de riscos ou em qualquer fase de um sistema de ciclo de vida, sempre que um consenso de visões de especialistas for necessário.

B.3.3 Entradas

Um conjunto de opções para as quais o consenso é necessário.

B.3.4 Processo

Um grupo de especialistas é questionado utilizando um questionário semi-estruturado. Os especialistas não se reúnem de maneira que as suas opiniões são independentes.

O procedimento é o seguinte:

- formação de uma equipe para realizar e monitorar o processo Delphi;
- seleção de um grupo de especialistas (pode ser um ou mais grupos específicos de especialistas);
- desenvolvimento do questionário da primeira rodada;
- teste do questionário;
- envio do questionário aos membros do grupo individualmente;
- as informações da primeira rodada de respostas são analisadas, combinadas e recirculadas aos membros do grupo;
- os membros do grupo respondem e o processo é repetido até que o consenso seja alcançado.

B.3.5 Saídas

Convergência em direção ao consenso sobre o assunto em questão.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.3.6 Pontos fortes e limitações

Os pontos fortes incluem:

- como as visões são anônimas, opiniões impopulares são mais prováveis de serem expressas;
- todas visões têm peso igual, o que evita o problema de personalidades dominantes;
- atinge a propriedade de resultados;
- as pessoas não precisam estar reunidas em um só local ao mesmo tempo.

As limitações incluem:

- consumo intensivo de trabalho e tempo;
- os participantes precisam ser capazes de expressar-se claramente por escrito.

B.4 Listas de verificação

B.4.1 Visão geral

As listas de verificação são listas de perigos, riscos ou falhas de controle que foram desenvolvidas normalmente a partir da experiência, como resultado de um processo de uma avaliação de riscos anterior ou como um resultado de falhas passadas.

B.4.2 Utilização

Uma lista de verificação pode ser utilizada para identificar perigos e riscos ou para avaliar a eficácia de controles. Elas podem ser utilizadas em qualquer estágio do ciclo de vida de um produto, processo ou sistema. Elas podem ser utilizadas como parte de outras técnicas do processo de avaliação de riscos, porém são mais úteis quando aplicadas para verificar que tudo foi coberto após a aplicação de uma técnica mais imaginativa que identifique novos problemas.

B.4.3 Entradas

Informações anteriores e conhecimento especializado sobre o assunto, de tal forma que uma lista de verificação pertinente e preferencialmente validada possa ser selecionada ou desenvolvida.

B.4.4 Processo

O procedimento é o seguinte:

- o escopo da atividade é definido;
- uma lista de verificação é selecionada de maneira a cobrir adequadamente o escopo. As listas de verificação precisam ser cuidadosamente selecionadas para esta finalidade. Por exemplo, uma lista de verificação de controles padronizados não pode ser utilizada para identificar novos perigos ou riscos;
- a pessoa ou a equipe que usa a lista de verificação percorre cada elemento do processo ou sistema e analisa criticamente se os itens da lista de verificação estão presentes.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.4.5 Saídas

As saídas dependem do estágio do processo de gestão de riscos em que elas são aplicadas. Por exemplo, a saída pode ser uma lista de controles que são inadequados ou uma lista de riscos.

B.4.6 Pontos fortes e limitações

Os pontos fortes das listas de verificação incluem:

- elas podem ser utilizadas por não especialistas;
- quando bem concebidas, elas combinam ampla gama de conhecimento especializado em um sistema de fácil utilização;
- elas podem auxiliar a assegurar que os problemas comuns não sejam esquecidos.

As limitações incluem:

- elas tendem a inibir a imaginação na identificação de riscos;
- elas tratam o “que sabemos que sabemos” , e não o “que sabemos que não sabemos “ ou os “que não sabemos que não sabemos”;
- elas incentivam o comportamento do tipo “marque a opção”;
- elas tendem a ser baseadas em observação, de maneira que ignoram problemas que não são prontamente vistos.

B.5 Análise preliminar de perigos (APP)

B.5.1 Visão geral

A APP é um método de análise simples e indutivo cujo objetivo é identificar os perigos e situações e eventos perigosos que podem causar danos em uma determinada atividade, instalação ou sistema.

B.5.2 Utilização

É mais comumente realizada no início do desenvolvimento de um projeto quando há pouca informação sobre detalhes do projeto ou procedimentos operacionais e pode muitas vezes ser uma precursora para estudos adicionais ou fornecer informações para a especificação do projeto de um sistema. Ela também pode ser útil ao analisar os sistemas existentes para priorizar os perigos e riscos para análise adicional ou quando as circunstâncias impedem a utilização de uma técnica mais extensiva.

B.5.3 Entradas

As entradas incluem:

- informações sobre o sistema a ser avaliado;
- os detalhes do projeto do sistema que estão disponíveis e são pertinentes.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.5.4 Processo

Uma lista de perigos, de situações genéricas perigosas e de riscos é formulada considerando características, tais como:

- os materiais utilizados ou produzidos e sua reatividade;
- equipamentos utilizados;
- ambiente operacional;
- leiaute;
- interfaces entre os componentes do sistema etc.

A análise qualitativa das consequências de um evento indesejável e suas probabilidades pode ser conduzida para identificar os riscos para uma avaliação adicional.

Convém que a APP seja atualizada durante as fases de projeto, construção e ensaio, a fim de detectar quaisquer novos riscos e efetuar correções, se necessário. Os resultados obtidos podem ser apresentados em diferentes formas, tais como tabelas e árvores.

B.5.5 Saídas

As saídas incluem:

- uma lista de perigos e riscos;
- recomendações sob a forma de aceitação, controles recomendados, especificação de projeto ou solicitações para uma avaliação mais detalhada.

B.5.6 Pontos fortes e limitações

Os pontos fortes incluem:

- que é capaz de ser utilizada quando houver pouca informação;
- ela permite que os riscos sejam considerados muito precocemente no ciclo de vida do sistema.

As limitações incluem:

- uma APP fornece somente informações preliminares, ela não é abrangente e também não fornece informações detalhadas sobre os riscos e como eles podem ser melhor evitados.

B.6 Estudo de perigos e operabilidade (HAZOP)

B.6.1 Visão geral

HAZOP é o acrônimo para “**HAZ**ard and **OP**erability Study” e é um exame estruturado e sistemático de um produto, processo, procedimento ou sistema existente ou planejado. É uma técnica para identificar os riscos para pessoas, equipamentos, ambiente e/ou objetivos organizacionais. Espera-se também que a equipe de estudo, sempre que possível, forneça uma solução para o tratamento do risco.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

O processo HAZOP é uma técnica qualitativa baseada no uso de palavras-guia as quais questionam como a intenção do projeto ou as condições de operação podem não ser atingidas a cada etapa do projeto, processo, procedimento ou sistema. É geralmente conduzido por uma equipe multidisciplinar ao longo de uma série de reuniões.

HAZOP é similar à FMEA enquanto se identificam os modos de falha de um processo, sistema ou procedimento bem como as suas causas e consequências. A diferença é que a equipe considera os resultados indesejáveis e os seus desvios e condições pretendidas e os trabalha de trás para a frente até chegar aos modos de falha e causas possíveis, enquanto que a FMEA começa por identificar os modos de falha.

B.6.2 Utilização

A técnica HAZOP foi inicialmente desenvolvida para analisar sistemas de processo químico, porém foi estendida para outros tipos de sistemas e operações complexas. Estes incluem sistemas mecânicos e eletrônicos, procedimentos e sistemas de *software*, e até mesmo alterações organizacionais e concepção e análise crítica de contratos legais.

O processo HAZOP pode tratar de todas as formas de desvio da intenção do projeto devido a deficiências no projeto, componente(s), procedimentos planejados e ações humanas.

Ele é amplamente utilizado para análise crítica de projeto de *software*. Quando aplicado ao controle de instrumentos críticos de segurança e a sistemas de computador, ele pode ser conhecido como CHAZOP (*Control Hazards and Operability Analysis* ou análise de perigo e operabilidade de computadores).

Um estudo HAZOP é geralmente realizado no estágio de detalhamento do projeto, quando um diagrama completo do processo pretendido está disponível, porém enquanto as alterações de projeto ainda sejam praticáveis. Ele pode, entretanto, ser conduzido em uma abordagem gradual com diferentes palavras-guia para cada estágio à medida em que os detalhes do projeto são desenvolvidos. Um estudo HAZOP também pode ser realizado durante a operação, porém alterações requeridas podem ser caras neste estágio.

B.6.3 Entradas

As entradas essenciais para um estudo HAZOP incluem informações atuais sobre o sistema, o processo ou procedimento a serem analisados criticamente e a intenção e as especificações de desempenho do projeto.

As entradas podem incluir: desenhos, folhas de especificação, diagramas de fluxo, diagramas de controle de processo e lógicos, desenhos de leiaute, procedimentos de operação e manutenção e procedimentos de resposta a emergência. Para HAZOP não relacionado a *hardware*, as entradas podem ser qualquer documento que descreva funções e elementos do sistema ou procedimento em estudo. Por exemplo, as entradas podem ser diagramas organizacionais e descrições de funções, uma minuta de contrato ou mesmo uma minuta de procedimento.

B.6.4 Processo

HAZOP considera o “projeto” e a especificação do processo, procedimento ou sistema a serem estudados e analisados criticamente cada parte dele para descobrir quais desvios do desempenho pretendido podem ocorrer, quais são as causas potenciais e quais são as consequências prováveis de um desvio. Isto é conseguido examinando sistematicamente como cada parte do sistema, processo ou procedimento responderá às alterações nos parâmetros-chave, utilizando palavras-guia adequadas.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

As palavras-guia podem ser personalizadas para um sistema, processo ou procedimento específico ou palavras genéricas podem ser utilizadas que englobem todos os tipos de desvio. A Tabela B.1 fornece exemplos de palavras-guia comumente utilizadas para sistemas técnicos. Palavras-guia similares tais como, 'muito cedo', 'muito tarde', 'muito', 'muito pouco', 'muito grande', 'muito curto', 'sentido errado', 'objeto errado' ou 'ação errada' podem ser utilizadas para identificar os modos de erro humano.

As etapas normais em um estudo HAZOP incluem:

- a nomeação de uma pessoa com a responsabilidade e a autoridade necessárias para conduzir o estudo HAZOP e assegurar que quaisquer ações decorrentes do estudo sejam concluídas;
- a definição dos objetivos e o escopo do estudo;
- o estabelecimento de um conjunto de chaves ou palavras-guia para o estudo;
- a definição de uma equipe de estudo HAZOP; esta equipe é geralmente multidisciplinar e convém que inclua pessoal de projeto e de operações com conhecimento técnico especializado apropriado para avaliar os efeitos de desvios do projeto pretendido ou em curso. É recomendado que a equipe inclua pessoas que não estejam diretamente envolvidas no projeto ou no sistema, processo ou procedimento em análise critica;
- a coleta da documentação requerida.

Dentro de uma oficina de trabalho com a equipe de estudo:

- dividir o sistema, processo ou procedimento em elementos menores ou subsistemas ou subprocessos ou sub-elementos para tornar a análise crítica tangível;
- acordar a intenção do projeto para cada subsistema, subprocesso ou sub-elemento e, em seguida, para cada item naquele subssistema ou elemento, aplicar as palavras-guia, uma após a outra, para postular possíveis desvios que teriam resultados indesejáveis;
- quando um resultado indesejável for identificado, concordar com a causa e a conseqüência, em cada caso, e sugerir como eles podem ser tratados para evitar que eles ocorram ou atenuar as consequências se ocorrerem;
- documentar a discussão e acordar ações específicas para tratar os riscos identificados.

Tabela B.1 – Exemplo de palavras-guia *HAZOP* possíveis

Termos	Definições
Nenhum(a) ou não	Nenhuma parte do resultado pretendido é atingida ou a condição pretendida está ausente
Mais (maior)	Aumento quantitativo na saída ou na condição operacional
Menos (menor)	Diminuição quantitativa
Bem como	Aumento quantitativo (por exemplo, material adicional)
Parte de	Diminuição quantitativa (por exemplo, somente um ou dois componentes em uma mistura)
Reverso/oposto	Oposto (por exemplo, retorno de fluxo)

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Tabela B.1 (continuação)

Termos	Definições
Exceto	Nenhuma parte da intenção é atingida, algo completamente diferente acontece (por exemplo, fluxo ou material errado)
Compatibilidade	Material; ambiente
As palavras-guia são aplicadas a parâmetros tais como	
	Propriedades físicas de um material ou processo
	Condições físicas tais como, temperatura, velocidade
	Uma intenção especificada de um componente de um sistema ou projeto (por exemplo, transferência de informações)
	Aspectos operacionais

B.6.5 Saídas

Ata(s) de reunião(ões) do *HAZOP* com itens para cada ponto de análise critica registrado. Convém que isto inclua: a palavra-guia utilizada, o(s) desvio(s), as possíveis causas, as ações para tratar dos problemas identificados e a pessoa responsável pela ação.

Para qualquer desvio que não possa ser corrigido, então convém que o risco para o desvio seja avaliado.

B.6.6 Pontos fortes e limitações

Uma análise HAZOP oferece as seguintes vantagens:

- fornece os meios para sistemática e totalmente analisar um sistema, processo ou procedimento;
- envolve uma equipe multidisciplinar, incluindo aquela com experiência operacional na vida real e aquela que pode ter que realizar ações de tratamento;
- gera soluções e ações de tratamento de riscos;
- é aplicável a uma ampla gama de sistemas, processos e procedimentos;
- permite a consideração explícita das causas e consequências de erro humano;
- cria um registro escrito do processo que pode ser utilizado para demonstrar devido zelo.

As limitações incluem:

- uma análise detalhada pode ser muito demorada e, portanto, cara;
- uma análise detalhada requer um alto nível de documentação ou especificação do sistema/processo e procedimento;
- pode focar em encontrar soluções detalhadas, ao invés de questionar premissas fundamentais (entretanto, isto pode ser atenuado por uma abordagem gradual);
- a discussão pode ser focada em questões de detalhe do projeto, e não em questões mais amplas ou externas ;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- é limitada pelo projeto (esboço) e o intuito do projeto, e o escopo e objetivos dados à equipe;
- o processo se baseia fortemente no conhecimento especializado dos projetistas que podem achar difícil ser suficientemente objetivos na procura de problemas em seus projetos.

B.6.7 Documento de referência

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

B.7 Análise de perigos e pontos críticos de controle (APPCC)

B.7.1 Visão geral

A análise de perigos e pontos críticos de controle (APPCC) fornece uma estrutura para a identificar perigos e pôr em prática controles em todas as partes pertinentes de um processo para proteger dos perigos e manter a confiabilidade da qualidade e segurança de um produto. A APPCC tem como objetivo assegurar que os riscos sejam minimizados por controles ao longo do processo ao invés de mediante a inspeção do produto final.

B.7.2 Utilização

A APPCC foi desenvolvida para assegurar a qualidade dos alimentos para o programa espacial da NASA. Agora é utilizada pelas organizações que operam em qualquer lugar dentro da cadeia de alimentos para controlar os riscos de contaminantes físicos, químicos ou biológicos dos alimentos. Também foi estendida para uso na fabricação de produtos farmacêuticos e dispositivos médicos. O princípio de identificação de coisas que podem ter influência na qualidade do produto e na definição de pontos em um processo onde parâmetros críticos podem ser monitorados e os perigos controlados, podem ser generalizados para outros sistemas técnicos.

B.7.3 Entradas

A APPCC começa a partir de um diagrama de fluxo básico ou diagrama de processo e informações sobre os perigos que possam afetar a qualidade, segurança ou confiabilidade do produto ou saída do processo. Informação sobre os perigos e seus riscos e as formas em que podem ser controlados é uma entrada da APPCC.

B.7.4 Processo

A APPCC consiste nos sete princípios seguintes:

- identifica os perigos e as medidas preventivas relacionadas a tais perigos;
- determina os pontos no processo onde os perigos podem ser controlados ou eliminados (os pontos críticos de controle ou PCC);
- estabelece limites críticos necessários para controlar os perigos, ou seja, convém que cada PCC opere dentro de parâmetros específicos para assegurar que o perigo está controlado;
- monitora os limites críticos para cada PCC a intervalos definidos;
- estabelece ações corretivas se o processo estiver fora dos limites estabelecidos;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- estabelece procedimentos de verificação;
- implementa a manutenção de registros e procedimentos de documentação para cada etapa.

B.7.5 Saídas

Registros documentados, incluindo uma planilha de análise de perigos e um plano APPCC.

A planilha de análise de perigos lista para cada etapa do processo:

- os perigos que poderiam ser introduzidos, controlados ou exacerbados nesta etapa;
- se os perigos apresentam um risco significativo (com base na consideração da consequência e probabilidade a partir da combinação da experiência, dados e literatura técnica);
- uma justificativa para a significância;
- possíveis medidas preventivas para cada perigo;
- se as medidas de monitoramento ou controle podem ser aplicadas nesta etapa (ou seja, é um PCC?).
- O plano APPCC delineia os procedimentos a serem seguidos para assegurar o controle de um projeto, produto, processo ou procedimento específicos. O plano inclui uma lista de todos os PCC e para cada PCC:
- os limites críticos para as medidas preventivas;
- as atividades de monitoramento e controle contínuos (incluindo o que, como e quando o monitoramento será realizado e por quem);
- as ações corretivas requeridas se desvios dos limites críticos forem detectados;
- as atividades de verificação e manutenção de registros.

B.7.6 Pontos fortes e limitações

Os pontos fortes incluem:

- um processo estruturado que fornece evidência documentada de controle da qualidade, bem como a identificação e a redução de riscos;
- um foco sobre os aspectos práticos de como e onde, em um processo, os perigos podem ser prevenidos e os riscos controlados;
- um melhor controle de risco em todo o processo ao invés de depender da inspeção do produto final;
- uma capacidade para identificar perigos introduzidos por meio de ações humanas e como estes podem ser controlados no momento da introdução ou subsequentemente.

As limitações incluem:

- a APPCC requer que os perigos sejam identificados, os riscos que eles representam definidos e sua significância entendida como entradas no processo. Controles apropriados também precisam ser definidos. Estes são requeridos a fim de especificar os pontos críticos de controle e os parâmetros de controle durante a APPCC e pode ser necessário que sejam combinados com outras ferramentas para atingir estes controles apropriados;

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- tomar ações quando os parâmetros de controle excedem limites definidos pode levar a perda de alterações graduais nos parâmetros de controle as quais são estatisticamente significativas e que, portanto, conviria que fossem acionadas.

B.7.7 Documento de referência

ABNT NBR ISO 22000, *Sistemas de gestão da segurança de alimentos – Requisitos para qualquer organização na cadeia produtiva de alimentos*

B.8 Avaliação da toxicidade

B.8.1 Visão geral

O processo de avaliação de riscos ambientais é utilizado aqui para abranger o processo seguido no processo de avaliação de riscos em vegetais, animais e seres humanos como um resultado da exposição a uma série de perigos ambientais. A gestão de riscos refere-se às etapas do processo decisório, incluindo a avaliação de riscos e o tratamento de riscos.

O método envolve a análise do perigo ou da fonte de dano e como ela afeta a população-alvo e os caminhos pelos quais o perigo pode alcançar uma população-alvo susceptível. Esta informação é então combinada para dar uma estimativa da provável extensão e a natureza do dano.

B.8.2 Utilização

O processo é utilizado para o processo de avaliar riscos em vegetais, animais e seres humanos como um resultado da exposição a perigos, tais como produtos químicos, microrganismos ou outras espécies.

Os aspectos da metodologia, tais como a análise do caminho que explora as diferentes rotas pelas quais um alvo pode ser exposto a uma fonte de risco, podem ser adaptados e utilizados em uma gama muito ampla de diferentes áreas de risco, fora da saúde humana e do meio ambiente e é útil na identificação de tratamentos para reduzir o risco.

B.8.3 Entradas

O método requer bons dados sobre a natureza e as propriedades dos perigos, as susceptibilidades da população-alvo (ou populações) e a maneira em que os dois interagem. Estes dados são normalmente baseados em pesquisas que podem ser laboratoriais ou epidemiológicas.

B.8.4 Processo

O procedimento é o seguinte:

a) Formulação do problema – isto inclui a definição do escopo da avaliação, definindo a gama de populações-alvo e os tipos de perigo de interesse;

b) Identificação do perigo – isto envolve a identificação de todas as fontes possíveis de dano à população-alvo oriundos dos perigos dentro do escopo do estudo. A identificação do perigo normalmente depende de conhecimentos de especialistas e uma revisão da literatura;

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

c) Análise de perigos – isto envolve o entendimento da natureza do perigo e como ele interage com o alvo. Por exemplo, ao considerar a exposição humana aos efeitos de produtos químicos, o perigo poderá incluir a toxicidade aguda e crônica, o potencial de danos ao DNA ou o potencial de causar câncer ou defeitos congênitos. Para cada efeito perigoso, a magnitude do efeito (a resposta) é comparada com a quantidade de perigo em que o alvo é exposto (a dose) e, sempre que possível, o mecanismo pelo qual o efeito produzido é determinado. Os níveis em que Não Há Nenhum Efeito Observável (NOEL) e Nenhum Efeito Adverso Observável (NOAEL) são observados. Estes são algumas vezes utilizados como critérios para aceitabilidade do risco.

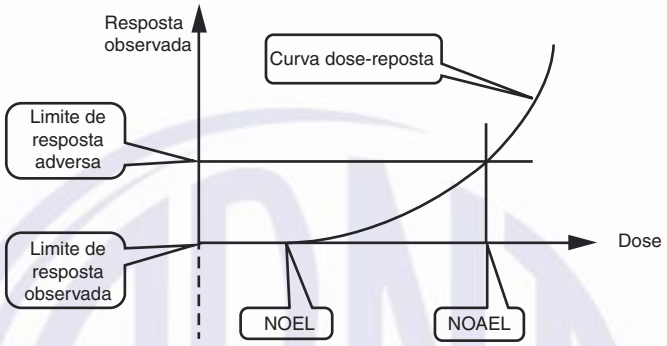

Figura B.1 – Curva dose-resposta

Para exposição a substâncias químicas, os resultados do ensaio são utilizados para derivar as curvas de dose-resposta tais como as mostradas esquematicamente na Figura B.1. Estas são geralmente derivadas a partir de ensaios em animais ou a partir de sistemas experimentais, tais como cultura de tecidos ou células.

Os efeitos de outros perigos, tais como os micro-organismos ou espécies introduzidas, podem ser determinados a partir de dados de campo e estudos epidemiológicos. A natureza da interação de doenças ou pragas com o alvo é determinada e é estimada a probabilidade de ocorrência de um nível específico de danos em resposta a uma exposição específica ao perigo.

a) Análise da exposição – esta etapa examina como uma substância perigosa ou seus resíduos pode alcançar uma população-alvo susceptível e em que quantidade. Esta etapa geralmente envolve uma análise do caminho que considera as diferentes rotas que o perigo pode tomar, as barreiras que podem evitar que atinja o alvo e os fatores que podem influenciar o nível de exposição. Por exemplo, ao considerar o risco de pulverização química, a análise da exposição consideraria quanto do produto químico foi pulverizado, de que forma e em que condições, se houve qualquer exposição direta de seres humanos ou animais, o quanto de resíduos foi deixado na vida vegetal, o destino ambiental de pesticidas ao atingir o solo: se eles podem ser acumulados em animais ou se eles atingem águas subterrâneas. Em biossegurança, a análise do caminho pode considerar como quaisquer pragas que entram no país e podem entrar no meio ambiente, tornam-se estabelecidas e se espalham.

b) Caracterização do risco – nesta etapa, as informações a partir da análise de perigos e a análise da exposição, são reunidas para estimar as probabilidades de consequências específicas quando os efeitos de todos os caminhos forem combinados. Quando houver um grande número de perigos ou caminhos, uma seleção inicial pode ser realizada e o perigo detalhado e a análise da exposição e a caracterização do risco realizadas nos cenários de maior risco.

B.8.5 Saídas

A saída é normalmente uma indicação do nível de risco a partir da exposição de um alvo particular a um perigo particular no contexto em questão. O risco pode ser expresso quantitativamente, semi-

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

quantitativamente ou qualitativamente. Por exemplo, o risco de câncer é muitas vezes expresso quantitativamente como a probabilidade de que uma pessoa irá desenvolver câncer durante um período especificado dada uma exposição especificada a um contaminante. A análise semi-quantitativa pode ser utilizada para derivar um índice de risco para um contaminante ou praga específico e a saída qualitativa pode ser um nível de risco (por exemplo, alto, médio, baixo) ou uma descrição com dados práticos sobre os prováveis efeitos.

B.8.6 Pontos fortes e limitações

Os pontos fortes desta análise é que ela fornece um entendimento muito detalhado da natureza do problema e os fatores que aumentam o risco.

A análise do caminho é uma ferramenta útil, geralmente, para todas as áreas de risco e permite a identificação de como e onde pode ser possível melhorar os controles ou introduzir novos.

Entretanto, são necessários bons dados que muitas vezes não estão disponíveis ou têm um alto nível de incerteza associada a eles. Por exemplo, convém que as curvas de dose-resposta derivadas da exposição de animais a altos níveis de um perigo sejam extrapoladas para estimar os efeitos de níveis muito baixos de contaminantes a seres humanos e existem múltiplos modelos pelos quais isto é alcançado. Quando o alvo for o meio ambiente ao invés de seres humanos e o perigo não for químico, os dados que são diretamente pertinentes para as condições específicas do estudo podem ser limitados.

B.9 *Técnica estruturada "E se"* (SWIFT)

B.9.1 Visão geral

A técnica SWIFT foi originalmente desenvolvida como uma alternativa mais simples para o HAZOP. É um estudo sistemático, baseado em trabalho em equipe, que utiliza um conjunto de palavras ou frases de 'comando' que é usado pelo facilitador dentro de uma oficina de trabalho para estimular os participantes a identificar riscos. O facilitador e a equipe utilizam frases padrão do tipo "e se" em combinação com os comandos para investigar como um sistema, item de instalações, organização ou procedimento será afetado por desvios de comportamento e operações normais. A técnica SWIFT é normalmente aplicada mais em nível de sistemas com um nível menor de detalhes do que o HAZOP.

B.9.2 Utilização

Enquanto a técnica SWIFT foi originalmente concebida para o estudo de perigos de instalações químicas e petroquímicas, a técnica é hoje amplamente aplicada a sistemas, itens de instalações, procedimentos e organizações em geral. Particularmente, é utilizada para examinar as consequências de mudanças e os riscos assim alterados ou criados.

B.9.3 Entradas

O sistema, procedimento, item de instalação e/ou mudança têm que ser cuidadosamente definidos antes do início do estudo. Ambos os contextos externo e interno são estabelecidos pelo facilitador por meio de entrevistas e mediante o estudo de documentos, planos e desenhos. Normalmente, o item, situação ou sistema para estudo é dividido em nós ou elementos-chave para facilitar o processo de análise, porém isso raramente ocorre ao nível de definição requerido para o HAZOP.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Outra entrada-chave é o conhecimento especializado e a experiência presentes na equipe de estudo que convém ser cuidadosamente selecionada. Convém que todas as partes interessadas sejam representadas, se possível juntamente com aqueles com experiência de itens, sistemas, mudanças ou situações similares.

B.9.4 Processo

O processo geral é o seguinte:

a) Antes do início dos estudos, o facilitador prepara uma lista de instruções adequada de palavras ou frases que podem ser baseadas em um conjunto padrão ou serem criadas para possibilitar uma análise crítica abrangente dos perigos ou riscos.

b) Na oficina de trabalho, os contextos externo e interno do item, sistema, mudança ou situação e o escopo do estudo são discutidos e acordados.

c) O facilitador pede aos participantes para levantar e discutir:

   — riscos e perigos conhecidos;

   — experiência e incidentes anteriores;

   — os controles conhecidos e existentes e as salvaguardas;

   — os requisitos regulatórios e restrições.

d) A discussão é facilitada pela criação de uma pergunta utilizando uma frase ‘e se’ e uma palavra de instrução ou assunto. As frases ‘e se’ a serem utilizadas são “e se ...”, “o que aconteceria se ...” “alguém ou alguma coisa poderia ...”, “há alguém ou alguma coisa que nunca ...”. A intenção é estimular a equipe de estudo a explorar cenários potenciais, suas causas e consequências e impactos.

e) Os riscos são resumidos e a equipe considera controles existentes.

f) A descrição do risco, suas causas, consequências e controles esperados são confirmados com a equipe e registrados.

g) A equipe considera se os controles são adequados e eficazes e acorda uma declaração da eficácia do controle de risco. Se isto for menos do que satisfatório, a equipe também considera tarefas de tratamento de risco e controles potenciais definidos.

h) Durante esta discussão, questões adicionais ‘e se’ são colocadas para identificar riscos adicionais.

i) O facilitador utiliza a lista de instruçõespara monitorar a discussão e sugerir questões e cenários adicionais para a equipe discutir.

j) É normal utilizar um método de processo de avaliação de riscos qualitativo ou semi-quantitativo para classificar as ações criadas em termos de prioridade. Este processo de avaliação de riscos é normalmente conduzido levando em consideração os controles existentes e a sua eficácia.

B.9.5 Saídas

As saídas incluem um registro do risco com as ações ou tarefas classificadas por risco. Estas tarefas podem então tornar-se a base para um plano de tratamento.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.9.6 Pontos fortes e limitações

Pontos fortes da técnica SWIFT:

- é amplamente aplicável a todas as formas de instalação física, sistema, situação ou circunstância, organização ou atividade;
- necessita preparo mínimo pela equipe;
- é relativamente rápida e os principais perigos e riscos rapidamente tornam-se evidentes na sessão da oficina de trabalho;
- o estudo é “orientado a sistemas” e permite que os participantes vejam a resposta do sistema a desvios ao invés de apenas examinar as consequências de falhas de componentes;
- pode ser utilizada para identificar oportunidades de melhoria de processos e sistemas e geralmente pode ser utilizada para identificar as ações que conduzam e melhorem suas probabilidades de sucesso;
- o envolvimento na oficina de trabalho por aqueles que são responsáveis pelos controles existentes e pelas ações de tratamento de riscos adicionais, reforçam a sua responsabilidade;
- cria um registro de riscos e plano de tratamento de riscos com um pouco mais de esforço;
- embora muitas vezes uma classificação de riscos qualitativa ou semi-quantitativa é utilizada para o processo de avaliação de riscos e para priorizar a atenção sobre as ações resultantes, a técnica SWIFT pode ser utilizada para identificar os riscos e perigos que podem ser levados adiante em um estudo quantitativo.
- Limitações da técnica SWIFT:
- é necessário um facilitador experiente e capaz para que seja eficiente;
- preparação cuidadosa é necessária para que o tempo da equipe da oficina de trabalho não seja desperdiçado;
- se a equipe da oficina de trabalho não tiver uma base suficientemente ampla de experiência ou se o sistema de instruções não for abrangente, alguns riscos ou perigos podem não ser identificados;
- a aplicação da técnica em alto nível pode não revelar causas complexas, detalhadas ou correlacionadas.

B.10 Análise de cenários

B.10.1 Visão geral

A análise de cenários é um nome dado para o desenvolvimento de modelos descritivos de como o futuro poderá ser. Pode ser utilizada para identificar os riscos, considerando possíveis desenvolvimentos futuros e explorando suas implicações. Os conjuntos de cenários (por exemplo) ‘melhor caso’, ‘pior caso’ e ‘caso esperado’, podem ser utilizados para analisar consequências potenciais e suas probabilidades para cada cenário como uma forma de análise da sensibilidade ao analisar o risco.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

O poder da análise de cenários é ilustrado considerando as grandes mudanças ao longo dos últimos 50 anos em tecnologia, as preferências do consumidor, atitudes sociais etc. A análise de cenários não pode prever as probabilidades de tais mudanças, mas pode considerar as consequências e auxiliar as organizações a desenvolverem forças e resiliência necessárias para se adaptar às mudanças previsíveis.

B.10.2 Utilização

A análise de cenários pode ser utilizada para auxiliar na tomada de decisões políticas e no planejamento de futuras estratégias, bem como considerar as atividades existentes. Pode desempenhar um papel em todos os três componentes do processo de avaliação de riscos. Para a identificação e análise, conjuntos de cenários refletindo (por exemplo) melhor caso, pior caso e caso 'esperado', podem ser utilizados para identificar o que poderia acontecer sob circunstâncias específicas e analisar as consequências potenciais e suas probabilidades para cada cenário.

A análise de cenários pode ser utilizada para antecipar como tanto ameaças quanto oportunidades podem se desenvolver e pode ser utilizada para todos os tipos de risco com ambas escalas de tempo, de curto e longo prazo. Com escalas de tempo de curto prazo e bons dados, os cenários prováveis podem ser extrapolados a partir do presente. Para escalas de tempo de longo prazo ou com dados menos confiáveis, a análise de cenários se torna mais imaginativa e pode ser referida como análise futura.

A análise de cenários pode ser útil quando houver grandes diferenças de distribuição entre resultados positivos e resultados negativos no espaço, tempo e grupos na comunidade ou numa organização.

B.10.3 Entradas

O pré-requisito para uma análise de cenários é uma equipe de pessoas que entre elas exista um entendimento da natureza das mudanças pertinentes (por exemplo, possíveis avanços em tecnologia) e a imaginação para pensar no futuro sem necessariamente extrapolar o passado. O acesso a literatura e dados sobre as mudanças que já estão ocorrendo também é útil.

B.10.4 Processo

A estrutura para a análise de cenários pode ser informal ou formal.

Tendo estabelecido uma equipe e canais pertinentes de comunicação, e definido o contexto do problema e questões a serem consideradas, a próxima etapa é identificar a natureza das mudanças que possam ocorrer. Isto necessitará de pesquisa sobre as principais tendências e o provável momento de mudanças nas tendências, bem como o pensamento imaginativo sobre o futuro.

As alterações a serem consideradas podem incluir:

- mudanças externas (tais como mudanças tecnológicas);
- decisões que precisam ser tomadas num futuro próximo, porém que podem ter uma variedade de resultados;
- necessidades das partes interessadas e como elas podem mudar;
- mudanças no macroambiente (regulatório, demográfico etc.). Algumas serão inevitáveis e algumas serão incertas.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Algumas vezes, uma mudança pode ser devida às consequências de outro risco. Por exemplo, o risco das alterações climáticas está resultando em mudanças na demanda do consumidor relacionadas à distância percorrida no transporte de alimentos. Isto influenciará quais os alimentos podem ser lucrativamente exportados, assim como quais alimentos podem ser produzidos localmente.

Os fatores macro e locais ou tendências podem agora ser listados e classificados por (1) importância (2) incerteza. Atenção especial é dada aos fatores que são mais importantes e mais incertos. Os fatores-chave ou tendências são mapeados uns contra os outros para mostrar áreas onde os cenários podem ser desenvolvidos.

Uma série de cenários é proposta com cada um focando em uma mudança plausível em parâmetros.

Uma “história” é, então, escrita para cada cenário que explica como você pode mover-se daqui em direção ao cenário específico. As histórias podem incluir detalhes plausíveis que agregam valor aos cenários.

Os cenários podem então ser utilizados para testar ou avaliar a questão original. O teste leva em consideração quaisquer fatores significativos, porém previsíveis (por exemplo, padrões de uso) e em seguida, explora como a política (atividade) seria ‘bem sucedida’ neste novo cenário, e os resultados de ‘pré-testes’ utilizando as perguntas “e se” baseadas em premissas do modelo.

Quando a pergunta ou proposta foi avaliada em relação a cada cenário, pode ser óbvio que seja necessário modificá-lo para torná-lo mais robusto ou menos arriscado. Também convém que seja possível identificar alguns indicadores principais que mostrem quando a mudança estiver ocorrendo. O monitoramento e a resposta aos indicadores principais podem fornecer oportunidade para mudanças nas estratégias planejadas.

Uma vez que os cenários são apenas “fatias” definidas de futuros possíveis, é importante ter certeza de que é levada em consideração a probabilidade da ocorrência de um resultado específico (cenário), ou seja, adotar uma estrutura de riscos. Por exemplo, quando os cenários de melhor caso, pior caso e caso esperado forem utilizados, convém que uma tentativa seja efetuada para qualificar ou expressar a probabilidade da ocorrência de cada cenário.

B.10.5 Saídas

Pode não haver cenário que melhor se ajuste, porém, convém que se termine com uma percepção mais clara da gama de opções e de como modificar o curso de ação escolhido conforme os indicadores se movem.

B.10.6 Pontos fortes e limitações

A análise de cenários leva em consideração uma gama de futuros possíveis que pode ser preferível à abordagem tradicional de se basear em projeções do tipo alta-média-baixa que assumem, por meio do uso de dados históricos, que acontecimentos futuros provavelmente continuarão a seguir tendências passadas. Isto é importante para situações onde há pouco conhecimento atual sobre no que basear as previsões ou quando os riscos estão sendo considerados no futuro a longo prazo.

Este ponto forte, entretanto, tem uma fraqueza associada que é aquela em que onde há alta incerteza, alguns cenários podem ser irreais.

As principais dificuldades na utilização da análise de cenários estão associadas com a disponibilidade de dados e a capacidade dos analistas e tomadores de decisão de serem capazes de desenvolver cenários realistas propícios a explorar os resultados possíveis.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Os perigos do uso da análise de cenários como uma ferramenta para tomada de decisões é que os cenários utilizados podem não ter um fundamento adequado; os dados podem ser especulativos; e resultados irreais podem não ser reconhecidos como tal.

B.11 Análise de impactos nos negócios (BIA)

B.11.1 Visão geral

A análise de impactos nos negócios, também conhecida como avaliação de impacto nos negócios, analisa como os principais riscos de ruptura poderiam afetar as operações da organização, e identifica e quantifica as capacidades que seriam necessárias para gerenciá-los. Especificamente, a BIA prevê um entendimento acordado de:

- identificação e criticidade dos principais processos de
- negócios, funções e recursos associados e as principais interdependências que existem para uma organização;
- como os eventos de ruptura afetarão a capacidade e a capabilidade de alcançar os objetivos críticos do negócio;
- capacidade e capabilidade necessárias para gerenciar o impacto de uma ruptura e recuperar a organização para níveis acordados de operação.

B.11.2 Utilização

A BIA é utilizada para determinar a criticidade e as escalas de tempo de recuperação de processos e recursos associados (pessoas, equipamentos, tecnologia da informação), para assegurar o atendimento continuado de objetivos. Além disso, a BIA auxilia na determinação das interdependências e inter-relações entre os processos, partes internas e externas e toda a ligação da cadeia de fornecimento.

B.11.3 Entradas

As entradas incluem:

- uma equipe para realizar a análise e desenvolver um plano;
- informações sobre os objetivos, o ambiente, as operações e as interdependências da organização;
- detalhes sobre as atividades e operações da organização, incluindo processos, recursos de suporte, relacionamento com outras organizações, arranjos de subcontratação, partes interessadas;
- consequências financeiras e operacionais de perdas em processos críticos;
- questionário preparado;
- lista de entrevistados de áreas pertinentes da organização e/ou partes interessadas que serão contactadas.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.11.4 Processo

A BIA pode ser realizada por meio de questionários, entrevistas, oficinas de trabalho estruturadas ou combinações de todos os três, para obter um entendimento dos processos críticos, os efeitos das perdas daqueles processos e escalas de tempo de recuperação requeridas e recursos de suporte.

As etapas chave incluem:

- baseada na avaliação de riscos e vulnerabilidade, confirmação dos processos chave e saídas da organização para determinar a criticidade dos processos;
- determinação das consequências de uma ruptura nos processos críticos identificados em termos financeiros e/ou operacionais, em períodos definidos;
- identificação das interdependências com as partes interessadas chave internas e externas. Isto pode incluir o mapeamento da natureza das interdependências ao longo da cadeia de fornecimento;
- determinação dos recursos atualmente disponíveis e o nível essencial de recursos necessários para continuar a operar em um nível mínimo aceitável após a ruptura;
- identificação de soluções e processos alternativos atualmente em uso ou planejados para serem desenvolvidos. Soluções e processos alternativos podem necessitar que sejam desenvolvidos onde os recursos ou a capabilidade forem inacessíveis ou insuficientes durante a ruptura;
- determinação do tempo de interrupção máxima aceitável (IMA) para cada processo com base nas consequências identificadas e os fatores críticos de sucesso para a função. A IMA representa o período de tempo máximo em que a organização pode tolerar a perda de capabilidade;
- determinação do(s) objetivo(s) do tempo de recuperação (OTR) para quaisquer equipamentos especializados ou tecnologia da informação. O OTR representa o tempo durante o qual a organização pretende recuperar a capabilidade dos equipamentos especializados ou a tecnologia da informação;
- confirmação do atual nível de preparação dos processos críticos para gerenciar uma ruptura. Isto pode incluir avaliar o nível de redundância dentro do processo (por exemplo, equipamentos sobressalentes) ou a existência de fornecedores alternativos.

B.11.5 Saídas

As saídas são as seguintes:

- uma lista de prioridades de processos críticos e interdependências associadas;
- impactos financeiros e operacionais documentados originados de uma perda dos processos críticos;
- recursos de suporte necessários para os processos críticos identificados;
- escalas de tempo de interrupção do processo crítico e as escalas de tempo de recuperação associadas à tecnologia da informação.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.11.6 Pontos fortes e limitações

Os pontos fortes da BIA incluem:

- uma compreensão dos processos críticos que fornece à organização a capacidade de continuar a atingir seus objetivos declarados;
- uma compreensão dos recursos requeridos;
- uma oportunidade para redefinir o processo operacional de uma organização para auxiliar na resiliência da organização.

As limitações incluem:

- falta de conhecimento dos participantes envolvidos no preenchimento de questionários, na realização de entrevistas ou em oficinas de trabalho;
- as dinâmicas de grupo podem afetar a análise completa de um processo crítico;
- expectativas simplistas ou super-otimistas dos requisitos de recuperação;
- dificuldade em obter um nível adequado de compreensão das operações e atividades da organização.

B.12 Análise de causa-raiz (RCA)

B.12.1 Visão geral

A análise de uma grande perda para evitar a sua recorrência é comumente referida como Análise de Causa-Raiz (RCA), Análise de Falhas de Causa-Raiz (RCFA) ou análise da perda. A RCA é focada nas perdas dos ativos devidas a vários tipos de falhas enquanto a análise da perda está relacionada principalmente às perdas financeiras ou econômicas devido a fatores externos ou catástrofes. Esta análise tenta identificar a raiz ou causas originais ao invés de lidar somente com os sintomas imediatamente óbvios. É reconhecido que a ação corretiva nem sempre pode ser totalmente eficaz e que a melhoria contínua pode ser requerida. A RCA é mais frequentemente aplicada para a avaliação de uma grande perda, mas também pode ser utilizada para analisar as perdas de uma forma mais global a fim de determinar onde as melhorias podem ser efetuadas.

B.12.2 Utilização

A RCA é aplicada em vários contextos, com as seguintes grandes áreas de uso:

- a RCA baseada na segurança é utilizada para investigações de acidentes e de saúde e segurança ocupacional;
- a análise de falhas é utilizada em sistemas tecnológicos relacionados à confiabilidade e manutenção;
- a RCA baseada na produção é aplicada no campo do controle da qualidade para a fabricação industrial;
- a RCA baseada no processo é focada em processos de negócio;

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- a RCA baseada em sistemas foi desenvolvida como uma combinação das áreas anteriores para lidar com sistemas complexos, com aplicação em gestão de mudanças, gestão de riscos e análise de sistemas.

B.12.3 Entradas

A entrada básica para uma RCA é toda a evidência coletada da falha ou perda. Dados da outras falhas similares também podem ser considerados na análise. Outras entradas podem ser resultados que são utilizados para testar hipóteses específicas.

B.12.4 Processo

Quando a necessidade de uma RCA for identificada, um grupo de especialistas é apontado para realizar a análise e fazer recomendações. O tipo de especialista será em muitas vezes dependente do conhecimento específico necessário para analisar a falha.

Embora diferentes métodos possam ser utilizados para realizar a análise, as etapas básicas na execução de uma RCA são similares e incluem:

- formação da equipe;
- estabelecer o escopo e os objetivos da RCA;
- coletar dados e evidências da falha ou perda;
- realizar uma análise estruturada para determinar a causa-raiz;
- desenvolver soluções e fazer recomendações;
- implementar as recomendações;
- verificar o sucesso das recomendações implementadas.

As técnicas de análise estruturada podem consistir em um dos seguintes procedimentos:

- a técnica dos “5 porquês”, ou seja, repetidamente perguntar ‘por quê?’ para remover camadas da causa e sub-causa;
- análise do modo e efeito de falhas;
- análise de árvore de falhas;
- diagramas de espinha de peixe ou Ishikawa;
- análise de Pareto;
- mapeamento da causa raiz.

A avaliação das causas muitas vezes progride de causas físicas inicialmente evidentes para causas humanas e finalmente para causas de gestão ou fundamentais subjacentes. Os fatores causais devem poder ser controlados ou eliminados pelas partes envolvidas a fim de que a ação corretiva seja eficaz e útil.

Documento impresso em 03/04/2019 15:34:12, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.12.5 Saídas

As saídas de uma RCA incluem:

- documentação de dados e evidências coletados;
- hipóteses consideradas;
- conclusão sobre as causas raízes mais prováveis para a falha ou perda;
- recomendações para ação corretiva.

B.12.6 Pontos fortes e limitações

Os pontos fortes incluem:

- envolvimento de especialistas aplicáveis trabalhando num ambiente de equipe;
- análise estruturada;
- consideração de todas as hipóteses prováveis;
- documentação dos resultados;
- necessidade de produzir recomendações finais.

Limitações de uma RCA:

- especialistas necessários podem não estar disponíveis;
- evidências críticas podem ser destruídas na falha ou removidas durante a limpeza;
- a equipe pode não ter à disposição tempo ou recursos suficientes para uma avaliação completa da situação;
- pode não ser possível implementar adequadamente as recomendações.

B.13 Análise de modo e efeito de falha (FMEA) e análise de modo, efeito e criticidade de falha (FMECA)

B.13.1 Visão geral

A análise de modo e efeito de falha (FMEA) é uma técnica utilizada para identificar as formas em que componentes, sistemas ou processos podem falhar em atender o intuito de seu projeto.

A FMEA identifica:

- todos os modos de falha potenciais das várias partes de um sistema (um modo de falha é aquilo que é observado ao falhar ou ao desempenhar incorretamente);
- os efeitos que estas falhas podem ter no sistema;

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- os mecanismos de falha;
- como evitar as falhas e/ou mitigar os efeitos das falhas no sistema.

A análise de modo, efeito e criticidade de falha FMECA estende uma FMEA de modo que cada modo de falha identificado seja classificado de acordo com a sua importância ou criticidade.

Esta análise de criticidade é normalmente qualitativa ou semiquantitativa, porém pode ser quantificada utilizando taxas reais de falha.

B.13.2 Utilização

Existem diversas aplicações da FMEA: FMEA de Projeto (ou produto), que é utilizada para componentes e produtos; FMEA de sistema que é utilizada para sistemas; FMEA de Processo, que é utilizada para processos de manufatura e montagem; FMEA de Serviço; e FMEA de *Software*.

A FMEA/FMECA pode ser aplicada durante o projeto, manufatura ou operação de um sistema físico.

Para melhorar a garantia de funcionamento, entretanto, as mudanças são normalmente mais facilmente implementadas no estágio de projeto. A FMEA e FMECA também podem ser aplicadas a processos e procedimentos. Por exemplo, é utilizada para identificar o potencial para erros médicos nos sistemas de saúde e falhas nos procedimentos de manutenção.

A FMEA/FMECA pode ser utilizada para

- auxiliar na seleção de alternativas de projeto com elevada garantia de funcionamento,
- assegurar que todos os modos de falha de sistemas e processos e seus efeitos no sucesso operacional foram considerados,
- identificar os modos e efeitos de erros humanos,
- fornecer uma base para o planejamento de testes e manutenção de sistemas físicos,
- melhorar o projeto de procedimentos e processos,
- fornecer informações qualitativas ou quantitativas para técnicas de análise, como análise de árvore de falhas.

A FMEA/FMECA pode fornecer entradas para outras técnicas de análises, como análise de árvore de falhas em um nível qualitativo ou quantitativo.

B.13.3 Entradas

A FMEA e a FMECA necessitam de informações sobre os elementos do sistema em detalhes suficientes para análise do significado das formas em que cada elemento pode falhar. Para uma FMEA de Projeto detalhada, o elemento pode estar no nível de componente individual detalhado, enquanto que, para FMEA de Sistemas de alto nível, os elementos podem ser definidos em um nível superior.

As informações podem incluir:

- desenhos ou um fluxograma do sistema que está sendo analisado e seus componentes, ou as etapas de um processo;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- uma compreensão da função de cada etapa de um processo ou componente de um sistema;
- detalhes dos parâmetros ambientais e outros parâmetros que podem afetar a operação;
- uma compreensão dos resultados de falhas específicas;
- informações históricas sobre falhas, incluindo dados da taxa de falha, quando disponíveis.

B.13.4 Processo

O processo de FMEA é o seguinte:

a) definir o escopo e objetivos do estudo;

b) montar a equipe;

c) entender o sistema/processo a ser submetido ao FMECA;

d) desdobrar o sistema em seus componentes ou etapas;

e) definir a função de cada etapa ou componente;

f) para cada componente ou etapa listado, identificar:

- como pode ser concebível cada parte falhar?
- quais mecanismos podem produzir estes modos de falha?
- quais podem ser os efeitos se as falhas ocorrerem?
- a falha é inofensiva ou prejudicial?
- como a falha é detectada?

g) identificar as medidas inerentes ao projeto para compensar a falha.

Para a FMECA, a equipe de estudo prossegue na classificação de cada um dos modos de falha identificados, de acordo com a sua criticidade.

Existem diversas maneiras de como isto pode ser feito. Os métodos comuns incluem

- o índice de criticidade de modo,
- o nível de risco,
- o número de prioridade de risco.

O modelo de criticidade é uma medida da probabilidade de que o modo a ser considerado resultará em falha do sistema como um todo; é definido como:

Probabilidade do efeito de falha * Taxa do modo de falha * Tempo de operação do sistema

É mais frequentemente aplicado a falhas em equipamentos onde cada um desses termos pode ser definido quantitativamente e todos os modos de falha têm a mesma consequência.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

O nível de risco é obtido pela combinação das consequências da ocorrência de um modo de falha com a probabilidade de falha. É utilizado quando as consequências de diferentes modos de falha diferem e pode ser aplicado a sistemas de equipamentos ou processos. O nível de risco pode ser expresso qualitativa, semiquantitativa ou quantitativamente.

O número de prioridade de risco (NPR) é uma medida semiquantitativa da criticidade, obtido pela multiplicação de números em escalas de classificação (normalmente entre 1 e 10) para consequência de falha, probabilidade de falha e capacidade de detectar o problema. (À falha é dada uma maior prioridade, se ela for difícil de detectar). Este método é utilizado frequentemente em aplicações de garantia da qualidade.

Uma vez que os modos e os mecanismos de falha são identificados, ações corretivas podem ser definidas e implementadas para os modos de falha mais significativos.

A FMEA é documentada em um relatório que contém:

- detalhes do sistema que foi analisado;
- a forma como o exercício foi conduzido;
- premissas feitas na análise;
- fontes de dados;
- os resultados, incluindo as planilhas preenchidas;
- a criticidade (se finalizada) e a metodologia utilizada para defini-la;
- quaisquer recomendações para análises adicionais, alterações de projeto ou características a serem incorporadas em planos de teste, etc.

O sistema pode ser reavaliado por um outro ciclo de FMEA após as ações terem sido completadas.

B.13.5 Saídas

A saída principal da FMEA é uma lista de modos de falha, os mecanismos de falha e os efeitos para cada componente ou etapa de um sistema ou processo (que podem incluir informações sobre a probabilidade de falha). Também são dadas informações sobre as causas da falha e as consequências ao sistema como um todo. A saída da FMECA inclui uma classificação de importância com base na probabilidade de que o sistema irá falhar, o nível de risco resultante do modo de falha ou uma combinação do nível de risco e a 'detectabilidade' do modo de falha.

A FMECA pode dar uma saída quantitativa se dados adequados da taxa de falha e consequências quantitativas forem utilizados.

B.13.6 Pontos fortes e limitações

Os pontos fortes da FMEA/FMECA são os seguintes:

- amplamente aplicável a modos de falha humana, de equipamentos, e de sistemas, e para *hardware*, *software* e procedimentos;
- identificar modos de falha de componentes, suas causas e seus efeitos sobre o sistema, e apresentá-los em um formato facilmente legível;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- evitar a necessidade de modificações muito dispendiosas no equipamento em serviço por meio da identificação antecipada de problemas no processo de projeto;
- identificar os modos de falha pontuais e requisitos para sistemas redundantes ou de segurança;
- fornecer entrada para o desenvolvimento de programas de monitoramento, destacando as características chave a serem monitoradas.

As limitações incluem:

- só poder ser utilizada para identificar modos de falha singulares e não as combinações de modos de falha;
- a menos que sejam adequadamente controlados e focados, os estudos podem ser demorados e onerosos;
- pode ser difícil e tediosa para sistemas multi-camadas complexos.

B.13.7 Documento de referência

IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)*

B.14 Análise de árvore de falhas (FTA)

B.14.1 Visão geral

A FTA é uma técnica para identificar e analisar os fatores que podem contribuir para um evento específico indesejado (chamado “evento de topo”). Fatores causais são identificados por dedução e organizados de uma maneira lógica e representados pictograficamente em um diagrama de árvore que descreve os fatores causais e sua relação lógica com o evento de topo.

Os fatores identificados na árvore podem ser eventos que estão associados a falhas de componente de equipamentos, erros humanos ou quaisquer outros eventos pertinentes que levem ao evento indesejado.

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

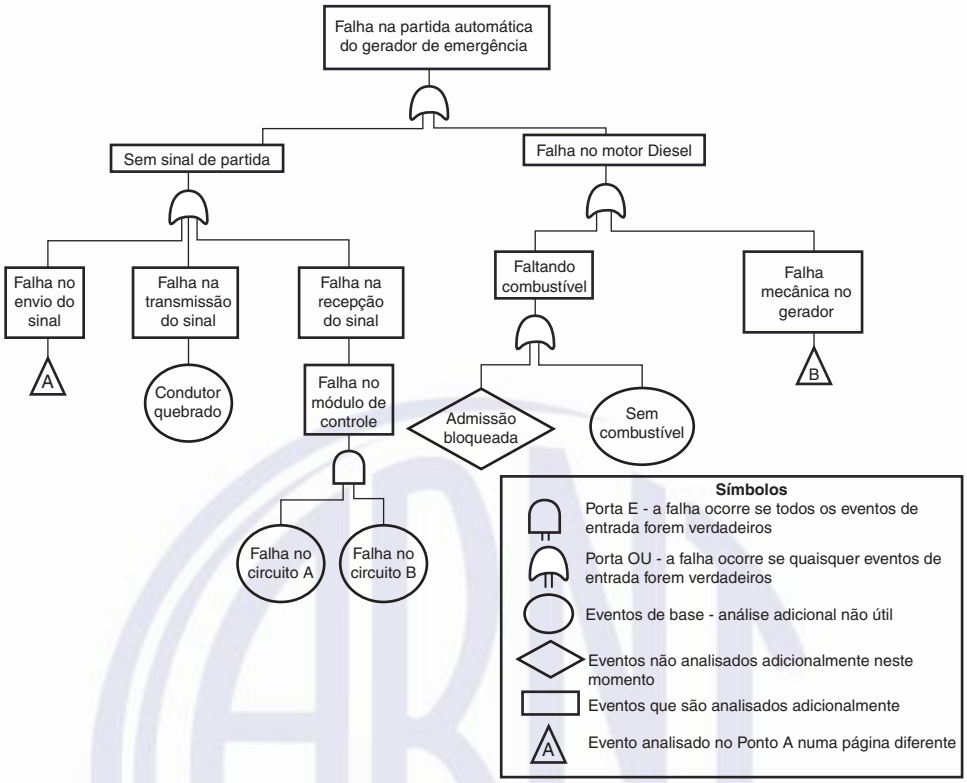

Figura B.2 – Exemplo de uma análise de árvore de falhas (FTA) da IEC 60300-3-9

B.14.2 Utilização

Uma árvore de falhas pode ser utilizada qualitativamente para identificar potenciais causas e os caminhos para uma falha (o evento de topo) ou quantitativamente para calcular a probabilidade do evento de topo, dado o conhecimento das probabilidades de eventos causais.

Pode ser utilizada no estágio de projeto de um sistema para identificar potenciais causas de falha e consequentemente selecionar entre diferentes opções de projeto. Ela pode ser utilizada na fase de operação para identificar como as principais falhas podem ocorrer e a importância relativa dos diferentes caminhos para o evento principal. Uma árvore de falhas também pode ser utilizada para analisar uma falha que ocorreu, mostrando esquematicamente como eventos diferentes se uniram para causar a falha.

B.14.3 Entradas

Para a análise qualitativa, uma compreensão do sistema e das causas da falha são requeridas, bem como uma compreensão técnica de como o sistema pode falhar. Diagramas detalhados são úteis para auxiliar a análise.

Para a análise quantitativa, dados sobre as taxas de falha ou probabilidade de ser um estado de falha para todos os eventos básicos na árvore de falhas são requeridos.

B.14.4 Processo

As etapas para o desenvolvimento de uma árvore de falhas são as seguintes:

- O evento de topo a ser analisado é definido. Este pode ser uma falha ou pode ser um resultado mais abrangente dessa falha. Quando o resultado é analisado, a árvore pode conter uma seção relacionada à mitigação da falha concreta.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- Iniciando com o evento de topo, os possíveis modos de falha e causas imediatos que conduzem ao evento de topo são identificados.

- Cada um destes modos causas/falhas é analisado para identificar como sua falha poderia ter sido causada.

- A identificação passo a passo da operação indesejada do sistema é acompanhada até níveis sucessivamente inferiores do sistema até que uma análise adicional se torne improdutiva. Em um sistema de equipamento isto pode ser o nível de falha do componente. Eventos e fatores causais no nível mais baixo do sistema analisado são conhecidos como eventos de base.

- Quando probabilidades podem ser atribuídas a eventos de base, a probabilidade do evento de topo pode ser calculada. Para que a quantificação seja válida, deve ser possível demonstrar que, para cada porta, todas as entradas são tanto necessárias quanto suficientes para produzir o evento de saída. Se este não for o caso, a árvore de falhas não é válida para a análise de probabilidade, mas pode ser uma ferramenta útil para mostrar relações causais.

Como parte da quantificação, a árvore de falhas pode necessitar ser simplificada utilizando álgebra Booleana para levar em conta os modos de falha duplicados.

Assim como fornece uma estimativa da probabilidade do evento principal, conjuntos mínimos de corte, os quais formam caminhos individuais separados para o evento principal, podem ser identificados e sua influência no evento de topo calculada.

Exceto para árvore de falhas simples, um pacote de *software* é necessário para manipular apropriadamente os cálculos quando eventos repetidos estiverem presentes em diversos locais na árvore de falhas e para calcular os conjuntos mínimos de corte. As ferramentas de *software* ajudam a assegurar a consistência, correção e verificabilidade.

B.14.5 Saídas

As saídas da análise de árvore de falhas são as seguintes:

- uma representação pictográfica de como o evento de topo pode ocorrer mostrando os caminhos de interação onde dois ou mais eventos simultâneos devem ocorrer;

- uma lista de cortes mínimos (caminhos individuais para a falha) com (onde dados forem disponíveis) a probabilidade com que cada um ocorrerá;

- a probabilidade do evento de topo.

B.14.6 Pontos fortes e limitações

Os pontos fortes da FTA são:

- Ela proporciona uma abordagem disciplinada que é altamente sistemática, porém, ao mesmo tempo suficientemente flexível, para permitir a análise de uma variedade de fatores, incluindo interações humanas e fenômenos físicos.

- A aplicação da abordagem "*top-down*", implícita na técnica, foca a atenção nos efeitos da falha que estão diretamente relacionados com o evento de topo.

- A AAF é especialmente útil para a análise de sistemas com muitas interfaces e interações.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- A representação pictográfica conduz a um fácil entendimento do comportamento do sistema e dos fatores incluídos, porém, como as árvores são muitas vezes grandes, o processamento das árvores de falhas pode requerer sistemas computacionais. Esta característica permite a inclusão de relações lógicas mais complexas (por exemplo, NAND e NOR), mas também dificulta a verificação das árvores de falhas.

- A análise lógica das árvores de falhas e a identificação de conjuntos de corte é útil na identificação de caminhos de falha simples em um sistema muito complexo, onde combinações específicas de eventos que levam ao evento de topo podem ser negligenciadas.

As limitações incluem:

- Incertezas nas probabilidades dos eventos de base são incluídas nos cálculos da probabilidade do evento de topo. Isto pode resultar em altos níveis de incerteza quando as probabilidades de falha no evento de base não são conhecidas com exatidão; entretanto, um alto grau de confiança é possível em um sistema bem entendido.

- Em algumas situações, os eventos causais não estão reunidos e pode ser difícil assegurar se todos os caminhos importantes para o evento de topo estão incluídos. Por exemplo, incluir todas as fontes de ignição em uma análise de um incêndio como um evento de topo. Nesta situação, a análise da probabilidade não é possível.

- A árvore de falhas é um modelo estático; interdependências de tempo não são tratadas.

- As árvores de falhas podem lidar apenas com estados binários (falhou/não falhou).

- Enquanto os modos de erro humano podem ser incluídos em uma árvore de falhas qualitativa, geralmente falhas de grau ou qualidade, que muitas vezes caracterizam o erro humano, não podem ser facilmente incluídas.

- Uma árvore de falhas não permite que efeitos dominó ou falhas condicionais sejam facilmente incluídos.

B.14.7 Documento de referência

IEC 61025, *Fault tree analysis (FTA)*

IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

B.15 Análise de árvore de eventos (ETA)

B.15.1 Visão geral

A ETA é uma técnica gráfica para representar as sequências mutuamente excludentes de eventos após um evento iniciador de acordo com o funcionamento/não funcionamento dos vários sistemas projetados para mitigar as suas consequências (ver Figura B.3). Pode ser aplicada qualitativa e quantitativamente.

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

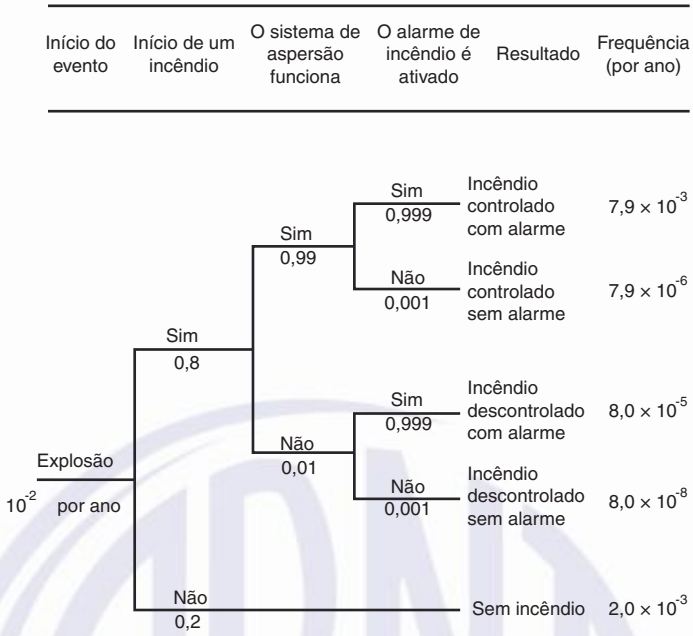

Figura B.3 – Exemplo de uma árvore de eventos

A Figura B.3 mostra cálculos simples para uma amostra de árvore de eventos, quando as ramificações são totalmente independentes.

Desdobrando-se como uma árvore, a ETA é capaz de representar os eventos agravantes ou atenuantes em resposta ao evento iniciador, levando em consideração sistemas, funções ou barreiras adicionais.

B.15.2 Utilização

A ETA pode ser utilizada para modelagem, cálculo e classificação (do ponto de vista de um risco) de diferentes cenários de acidentes após o evento iniciador.

A ETA pode ser utilizada em qualquer estágio do ciclo de vida de um produto ou processo. Pode ser utilizada qualitativamente para auxiliar o *brainstorm* de cenários potenciais e sequências de eventos após um evento iniciador e também como os resultados são afetados por vários tratamentos, barreiras ou controles destinados a atenuar resultados indesejados.

A análise quantitativa presta-se a considerar a aceitabilidade dos controles. É mais frequentemente utilizada para modelar falhas onde existem múltiplas proteções.

A ETA pode ser utilizada para modelar os eventos iniciadores que possam trazer perda ou ganho. Entretanto, as circunstâncias onde os caminhos para otimizar o ganho são procuradas, são mais frequentemente modeladas utilizando uma árvore de decisões.

B.15.3 Entradas

As entradas incluem:

- uma lista de eventos iniciadores apropriados;
- informações sobre tratamentos, barreiras e controles, e suas probabilidades de falha (para análises quantitativas);
- o entendimento dos processos pelos quais uma falha inicial se intensifica.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.15.4 Processo

Uma árvore de eventos começa selecionando-se um evento iniciador. Isto pode ser um incidente tal como uma explosão de pó ou um evento causal, tal como uma falha de energia. As funções ou sistemas que estão em prática para atenuar os resultados são então listados em sequência. Para cada função ou sistema, uma linha é desenhada para representar seu sucesso ou falha. Uma probabilidade específica de falha pode ser atribuída a cada linha, com esta probabilidade condicional estimada, por exemplo, por julgamento de especialistas ou uma análise da árvore de falhas. Desta forma, diferentes caminhos a partir do evento iniciador são modelados.

Note-se que as probabilidades na árvore de eventos são probabilidades condicionais, por exemplo, a probabilidade de funcionamento de um chuveiro automático para extinção de incêndio não é a probabilidade obtida a partir de ensaios sob condições normais, mas a probabilidade de funcionamento sob condições de incêndio causadas por uma explosão.

Cada caminho através da árvore representa a probabilidade de que todos os eventos naquele caminho ocorrerão. Portanto, a frequência do resultado é representada pelo produto das probabilidades condicionais individuais e a frequência do evento iniciador, uma vez que os vários eventos são independentes.

B.15.5 Saídas

As saídas da ETA incluem o seguinte:

- descrições qualitativas de potenciais problemas como combinações de eventos que produzem vários tipos de problemas (faixa de resultados) a partir dos eventos iniciadores;
- estimativas quantitativas das frequências ou probabilidades do evento e a importância relativa de várias sequências de falha e eventos contribuintes;
- listas de recomendações para reduzir os riscos;
- avaliações quantitativas da eficácia da recomendação.

B.15.6 Pontos fortes e limitações

Os pontos fortes da ETA são os seguintes:

- a ETA apresenta de uma forma gráfica clara os cenários potenciais analisados que sucedem um evento iniciador e o impacto do sucesso ou da falha dos sistemas ou funções de atenuação;
- representa o tempo , a dependência e os efeitos dominó que são difíceis de modelar em árvores de falhas;
- representa graficamente sequências de eventos que não são possíveis de representar ao utilizar árvores de falhas.

As limitações incluem:

- a fim de utilizar a ETA como parte de uma avaliação abrangente, todos os eventos iniciadores potenciais precisam ser identificados. Isto pode ser efetuado utilizando outro método de análise (por exemplo, HAZOP, APP), entretanto, existe sempre um potencial para a perda de alguns eventos iniciadores importantes;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- com as árvores de eventos, somente os estados de sucesso e falha de um sistema são tratados, e é difícil incorporar sucessos atrasados ou eventos de recuperação;

qualquer caminho é condicional em relação aos eventos que ocorrem em pontos anteriores ao longo do caminho. Muitas dependências ao longo dos caminhos possíveis são, portanto, tratadas. Entretanto, algumas dependências (componentes comuns, sistemas de consumo (*utility*) e operadores, por exemplo) podem ser ignoradas dando lugar a estimativas otimistas do risco se não forem cuidadosamente tratadas.

B.16 Análise de causa e consequência

B.16.1 Generalidades

A análise de causa e consequência é uma combinação da análise da árvore de falhas e árvore de eventos. Ela começa a partir de um evento crítico e analisa as consequências por meio de uma combinação de portas lógicas SIM/NÃO que representam condições que podem ocorrer ou falhas de sistemas projetados para atenuar as consequências do evento iniciador. As causas das condições ou falhas são analisadas por meio de árvores de falhas (ver Seção B.15).

B.16.2 Utilização

A análise de causa e consequência foi originalmente desenvolvida como uma ferramenta de confiabilidade para sistemas críticos de segurança para fornecer um entendimento mais completo das falhas no sistema. Semelhante à análise de árvore de falhas, a análise de causa e consequência é utilizada para representar a lógica da falha que leva a um evento crítico, porém ela se acrescenta à funcionalidade de uma árvore de falha, permitindo que as falhas sequenciais de tempo sejam analisadas. O método também permite retardos de tempo a serem incorporados à análise da consequência o que não é possível com a árvore de eventos.

O método é utilizado para analisar os vários caminhos que um sistema tomaria após um evento crítico em função do comportamento dos subsistemas específicos (tais como sistemas de resposta de emergência). Se forem quantificados, eles darão uma estimativa da probabilidade de diferentes consequências possíveis após um evento crítico.

Como cada sequência em um diagrama de causa e consequência é uma combinação de árvores de subfalhas, a análise de causa e consequência pode ser utilizada como uma ferramenta para construir grandes árvores de falhas.

Diagramas são complexos de produzir e utilizar, e tendem a ser usados quando a magnitude da consequência potencial de falha justifica esforços intensivos.

B.16.3 Entradas

Um entendimento do sistema e seus modos de falha e cenários de falha é requerido.

B.16.4 Processo

A Figura B.4 mostra um diagrama conceitual de uma análise de causa e consequência típica.

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

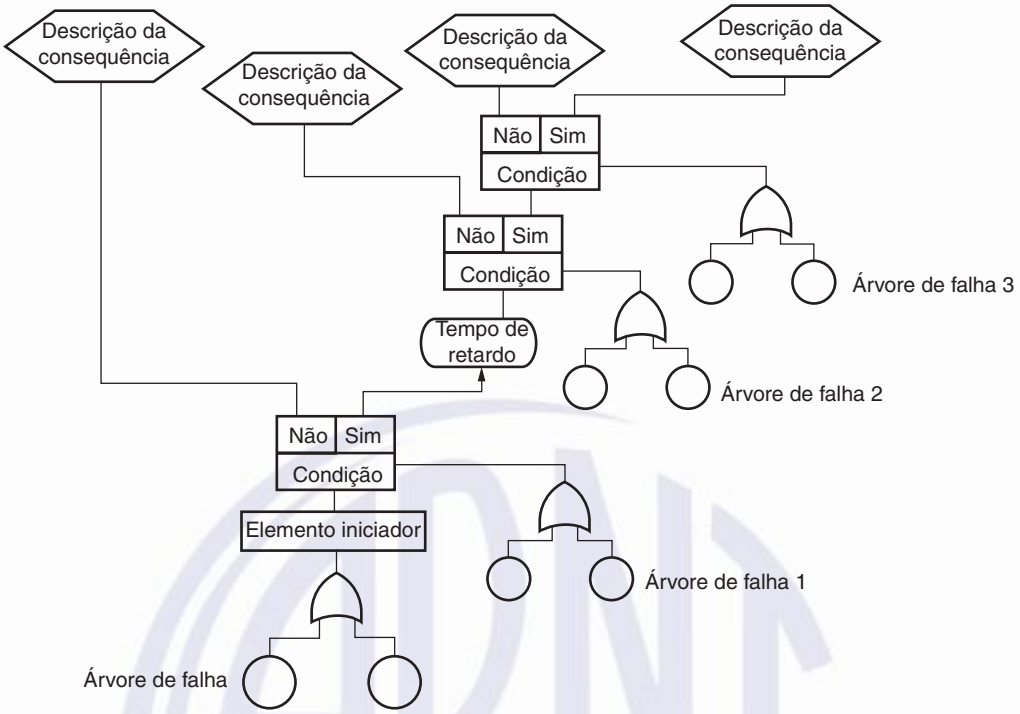

Figura B.4 – Exemplo de análise causa e conseqüência

O procedimento é o seguinte:

a) Identificar o evento crítico (ou iniciador) (equivalente ao evento de topo de uma árvore de falha e o evento iniciador de uma árvore de evento).

b) Desenvolver e validar a árvore de falha quanto às causas do evento iniciador, conforme descrito na Seção B.14. Os mesmos símbolos são utilizados como na análise da árvore de falha convencional.

c) Decidir a ordem em que as condições devem ser consideradas. Convém que isto seja uma sequência lógica, como a sequência de tempo em que elas ocorrem.

d) Construir os caminhos para as consequências, em função das diferentes condições. Isto é similar a uma árvore de evento, porém a separação em caminhos da árvore de evento é mostrada como uma caixa rotulada com a condição específica aplicável.

e) Uma vez que as falhas para cada caixa de condição são independentes, a probabilidade de cada consequência pode ser calculada. Isto é conseguido em primeiro lugar atribuindo-se probabilidades para cada saída da caixa de condição (utilizando as árvores de falhas pertinentes, como apropriado). A probabilidade de qualquer uma das sequências que conduz a uma consequência específica é obtida multiplicando as probabilidades de cada sequência de condições que termina nessa consequência específica. Se mais de uma sequência terminar com a mesma consequência, as probabilidades de cada sequência são somadas. Se houver dependências entre falhas de condições em uma sequência (por exemplo, uma falha de energia pode causar diversas condições para falha), então convém que as dependências sejam tratadas antes do cálculo.

B.16.5 Saída

A saída da análise de causa e consequência é uma representação esquemática de como um sistema pode falhar mostrando tanto as causas como as conseqüências, além de uma estimativa da

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

probabilidade de ocorrência de cada consequência potencial com base na análise das probabilidades de ocorrência de condições específicas após o evento crítico.

B.16.6 Pontos fortes e limitações

As vantagens da análise de causa e consequência são as mesmas das árvores de evento e árvores de falhas combinadas. Além disso, ela supera algumas das limitações dessas técnicas ao ser capaz de analisar eventos que se desenvolvam ao longo do tempo. A análise de causa e consequência fornece uma visão abrangente do sistema.

A limitação é que é mais complexa do que a análise da árvore de falha e árvore de evento, tanto para construir quanto na maneira em que as dependências são tratadas durante a quantificação.

B.17 Análise de causa e efeito

B.17.1 Visão geral

A análise de causa e efeito é um método estruturado para identificar as possíveis causas de um evento ou problema indesejado. Ele organiza os possíveis fatores contributivos em categorias amplas de modo que todas as hipóteses possíveis possam ser consideradas. Entretanto, por si só não aponta para as causas reais, já que estas somente podem ser determinadas por evidência real e testes empíricos de hipóteses. A informação é organizada em diagramas de espinha de peixe (também chamados de Ishikawa) ou por vezes em diagramas de árvore (ver B.17.4).

B.17.2 Utilização

A análise de causa e efeito fornece uma visualização gráfica estruturada de uma lista de causas para um efeito específico. O efeito pode ser positivo (um objetivo) ou negativo (um problema), dependendo do contexto.

É utilizada para permitir a consideração de todos os cenários e causas possíveis gerados por uma equipe de especialistas e permite que o consenso seja estabelecido quanto às causas mais prováveis que podem ser testadas empiricamente ou pela avaliação de dados disponíveis. É mais vantajosa no início de uma análise para ampliar a reflexão sobre as possíveis causas e, em seguida, para estabelecer as potenciais hipóteses que podem ser consideradas mais formalmente.

A construção de um diagrama de causa e efeito pode ser realizada quando houver necessidade de:

- identificar as possíveis causas-raiz, as razões básicas, para um efeito, problema ou condição específicos;
- classificar e correlacionar algumas das interações entre os fatores que afetam um processo específico;
- analisar os problemas existentes de modo que ações corretivas possam ser tomadas.

Os benefícios de construir um diagrama de causa e efeito incluem:

- concentrar a atenção dos membros da equipe de analistas sobre um problema específico;
- ajudar a determinar as causas-raiz de um problema utilizando uma abordagem estruturada;

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- incentivar a participação do grupo e utilizar o conhecimento do grupo para o produto ou processo;
- utilizar um formato ordenado de fácil leitura para diagramar as relações de causa e efeito;
- indicar as possíveis causas de variação em um processo;
- identificar áreas onde convém que dados sejam coletados para um estudo adicional.

A análise de causa e efeito pode ser utilizada como um método na realização da análise de causa-raiz (ver Seção B.12).

B.17.3 Entradas

A entrada para uma análise de causa e efeito pode ser proveniente de conhecimentos e experiência dos participantes ou de um modelo previamente desenvolvido que tenha sido utilizado no passado.

B.17.4 Processo

Convém que a análise de causa e efeito seja realizada por uma equipe de especialistas com conhecimento no problema que requer solução.

As etapas básicas na realização de uma análise de causa e efeito são as seguintes:

- estabelecer o efeito a ser analisado e colocá-lo em uma caixa. O efeito pode ser positivo (um objetivo) ou negativo (um problema), dependendo das circunstâncias;
- determinar as principais categorias de causas representadas por caixas no diagrama de espinha de peixe. Normalmente, para um problema de sistema, as categorias podem ser pessoas, equipamentos, ambiente, processos etc. Entretanto, estas são escolhidas para se adequarem ao contexto específico;
- preencher as possíveis causas para cada categoria principal com ramificações e sub-ramificações para descrever a relação entre elas;
- continuar perguntando “por quê?” ou “o que causou isto?” para conectar as causas;
- analisar criticamente todas as ramificações para verificar a consistência e a completeza e para assegurar que as causas aplicam-se ao efeito principal;
- identificar as causas mais prováveis com base na opinião da equipe e evidência disponíveis.

Os resultados são normalmente exibidos como um diagrama de espinha de peixe, ou Ishikawa, ou diagrama de árvore. O diagrama de espinha de peixe é estruturado separando as causas em categorias principais (representadas pelas linhas que saem da espinha dorsal do peixe) com ramificações e sub-ramificações que descrevem as causas mais específicas nestas categorias.

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

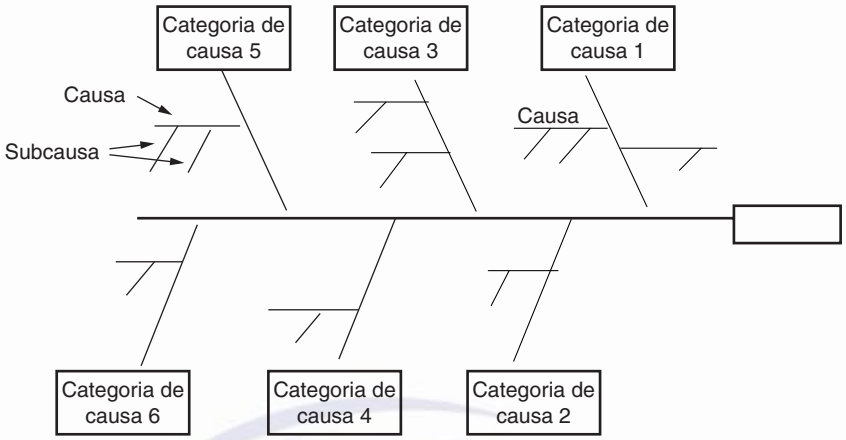

Figura B.5 – Exemplo de diagrama de Ishikawa ou espinha de peixe

A representação em árvore é similar a uma árvore de falha na aparência, embora muitas vezes ela seja exibida com a árvore desenvolvendo da esquerda para a direita em vez de cima para baixo ao longo da página. Entretanto, ela não pode ser quantificada para produzir a probabilidade do evento principal uma vez que as causas são possíveis fatores contributivos mais do que falhas com uma probabilidade de ocorrência conhecida.

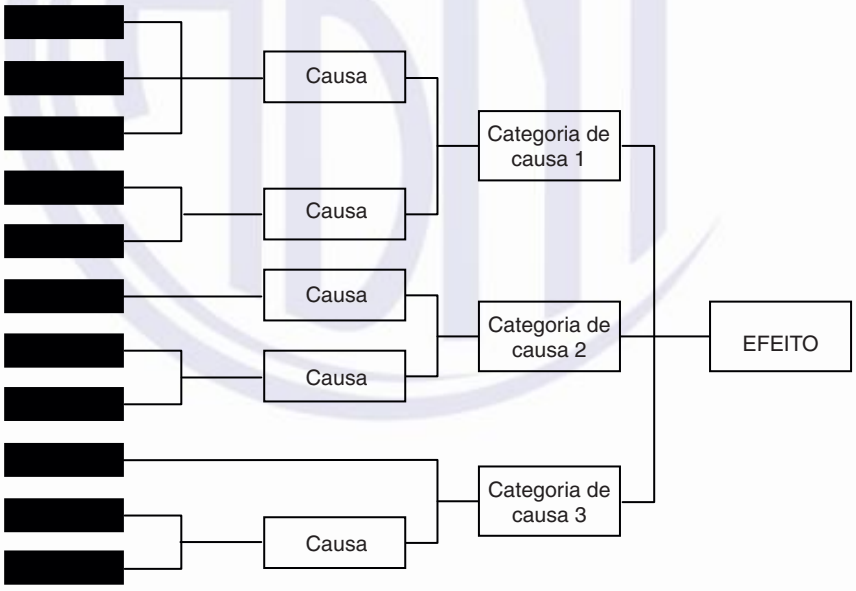

Figura B.6 – Exemplo de formulação de árvore de análise de causa e efeito

Os diagramas de causa e efeito são geralmente utilizados qualitativamente. É possível assumir que a probabilidade do problema é 1 e atribuir probabilidades a causas genéricas e, subsequentemente, para as subseções, com base no grau de convicção sobre sua pertinência. Entretanto, os fatores contributivos muitas vezes interagem e contribuem para o efeito de maneiras complexas, que tornam a quantificação inválida.

B.17.5 Saída

A saída de uma análise de causa e efeito é um diagrama de espinha de peixe ou diagrama de árvore que mostra as causas possíveis e prováveis. Este então deve ser verificado e testado empiricamente antes que recomendações possam ser feitas.

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.17.6 Pontos fortes e limitações

Os pontos fortes incluem:

- envolvimento de especialistas trabalhando em um ambiente de equipe;
- análise estruturada;
- consideração de todas as hipóteses prováveis;
- ilustração gráfica de fácil leitura dos resultados;
- identificação de áreas onde dados adicionais são necessários;
- pode ser utilizada para identificar os fatores contributivos para os efeitos pretendidos bem como os não pretendidos. Adotar um enfoque positivo sobre um tema pode encorajar uma maior apropriação e participação.

As limitações incluem:

- a equipe pode não ter a especialização necessária;
- não ser um processo completo por si só e precisar ser parte de uma análise de causa-raiz para produzir recomendações;
- é uma técnica de exibição das causas para *brainstorming* mais do que uma técnica de análise em separado;
- a separação de fatores causais em categorias principais no início da análise significa que as interações entre as categorias podem não ser consideradas de forma adequada, por exemplo, quando a falha do equipamento for causada por erro humano ou problemas humanos forem causados por projeto deficiente.

B.18 Análise de camadas de proteção (LOPA)

B.18.1 Visão geral

A LOPA é um método semiquantitativo para estimar os riscos associados a um evento ou cenário indesejado. Analisa se há medidas suficientes para controlar ou mitigar os riscos.

Um par de causa e consequência é selecionado e as camadas de proteção que evitam que a causa leve à consequência indesejada são identificadas. Um cálculo da ordem de grandeza é realizado para determinar se a proteção é adequada para reduzir o risco a um nível tolerável.

B.18.2 Utilização

A LOPA pode ser utilizada qualitativamente simplesmente para analisar criticamente as camadas de proteção entre um perigo ou evento causal e um resultado. Normalmente, uma abordagem semiquantitativa seria aplicada para acrescentar mais rigor aos processos de seleção, como, por exemplo, após o HAZOP ou APP.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

A LOPA fornece uma base para a especificação de camadas de proteção independentes (IPL) e os níveis de integridade de segurança (SIL) para sistemas instrumentados, conforme descrito na série IEC 61508 e na IEC 61511, na determinação dos requisitos do nível de integridade de segurança (SIL) para sistemas de segurança instrumentados. A LOPA pode ser utilizada para auxiliar na alocação eficaz de recursos de redução de riscos, analisando a redução do risco produzida por cada camada de proteção.

B.18.3 Entradas

As entradas da LOPA incluem

- informações básicas sobre riscos, incluindo os perigos, causas e conseqüências, como os proporcionados por uma APP;
- informações sobre controles em uso ou propostos;
- frequências de eventos causais e probabilidades de falha de camada de proteção, medidas de consequência e uma definição do risco tolerável;
- frequências de causas iniciadoras, probabilidades de falha de camada de proteção, medidas de consequência e uma definição do risco tolerável.

B.18.4 Processo

A LOPA é realizada utilizando uma equipe de especialistas que aplicam o seguinte procedimento:

- identificar causas iniciadoras para um resultado indesejado e buscar dados sobre suas frequências e consequências;
- selecionar um único par de causa e consequência;
- camadas de proteção que evitam que a causa prossiga para a consequência indesejada são identificadas e analisadas quanto à sua eficácia;
- identificar camadas de proteção independentes (IPL) (nem todas as camadas de proteção são IPL);
- estimar a probabilidade de falha de cada IPL;
- a frequência da causa iniciadora é combinada com as probabilidades de falha de cada IPL e as probabilidades de quaisquer modificadores condicionais (um modificador condicional é, por exemplo, se uma pessoa estará presente para ser impactada) para determinar a frequência de ocorrência da consequência indesejada. Ordens de grandeza são utilizadas para frequências e probabilidades;
- o nível de risco calculado é comparado com níveis de tolerância de risco para determinar se proteção adicional é requerida.

Uma IPL é um sistema de dispositivos ou ação capaz de evitar que um cenário progrida para sua consequência indesejada, qualquer que seja o evento causal ou camada de proteção associada com o cenário.

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

As IPL incluem:

- características de projeto;
- dispositivos de proteção física;
- sistemas de travamento e desligamento;
- alarmes críticos e de intervenção manual;
- proteção física pós-evento;
- sistemas de resposta a emergência (procedimentos e inspeções não são IPL).

B.18.5 Saída

Recomendações devem ser dadas para quaisquer controles adicionais e a eficácia destes controles na redução do risco.

A LOPA é uma das técnicas utilizadas para a avaliação do SIL ao tratar de sistemas relativos à segurança/instrumentados.

B.18.6 Pontos fortes e limitações

Os pontos fortes incluem:

- requer menos tempo e menos recursos do que uma análise de árvore de falhas ou processo de avaliação de risco integralmente quantitativo, porém é mais rigorosa do que julgamentos subjetivos qualitativos;
- ajuda a identificar e concentrar recursos nas camadas de proteção mais críticas;
- identifica operações, sistemas e processos para os quais existem salvaguardas insuficientes;
- concentra-se nas consequências mais sérias.

As limitações incluem:

- a LOPA focaliza em um par de causa e consequência e um cenário por vez. Interações complexas entre riscos ou entre controles não são cobertas;
- os riscos quantificados podem não levar em conta falhas de modo comum;
- a LOPA não se aplica a cenários muito complexos onde há muitos pares de causa e consequência ou quando há uma variedade de consequências que afetam diferentes partes interessadas.

B.18.7 Documentos de referência

IEC 61508 (todas as partes), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.19 Análise de árvore de decisões

B.19.1 Visão geral

Uma árvore de decisões representa alternativas de decisão e resultados de maneira seqüencial, que leva em consideração resultados incertos. É similar a uma árvore de eventos na medida em que ela começa a partir de um evento iniciador ou uma decisão inicial e modela diferentes caminhos e resultados como um resultado de eventos que podem ocorrer e decisões diferentes que podem ser tomadas.

B.19.2 Utilização

Uma árvore de decisões é utilizada na gestão de riscos de projeto e em outras circunstâncias para auxiliar a selecionar o melhor curso de ação onde houver incerteza. Uma ilustração gráfica também pode auxiliar a comunicar as razões para decisões.

B.19.3 Entradas

Um plano de projeto, com pontos de decisão. Informações sobre possíveis resultados de decisões e sobre eventos ao acaso que podem afetar as decisões.

B.19.4 Processo

Uma árvore de decisões começa com uma decisão inicial, por exemplo, prosseguir com o projeto A em vez do projeto B. À medida em que os dois projetos hipotéticos prosseguem, diferentes eventos ocorrerão e diferentes decisões previsíveis precisarão ser tomadas. Estes são representados em formato de árvore, similar a uma árvore de eventos. A probabilidade dos eventos pode ser estimada juntamente com o custo ou utilidade do resultado final do caminho.

Informações concernentes ao melhor caminho de decisão são, logicamente, aquelas que produzem o maior valor esperado calculado como o produto de todas as probabilidades condicionais ao longo do caminho e o valor do resultado.

B.19.5 Saídas

As saídas incluem:

- uma análise lógica do risco, mostrando diferentes opções que podem ser tomadas;
- um cálculo do valor esperado para cada caminho possível.

B.19.6 Pontos fortes e limitações

Os pontos fortes incluem:

- fornecer uma representação gráfica clara dos detalhes de um problema de decisão;
- permitir um cálculo do melhor caminho através de uma situação.

As limitações incluem:

- grandes árvores de decisão podem tornar-se muito complexas para uma comunicação fácil com outros;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- uma tendência de simplificar demasiadamente a situação, de modo a permitir sua representação como um diagrama de árvore.

B.20 Avaliação da confiabilidade humana (ACH)

B.20.1 Visão geral

A avaliação da confiabilidade humana (ACH) trata do impacto de pessoas sobre o desempenho do sistema e pode ser utilizada para avaliar as influências de erro humano no sistema.

Muitos processos contêm potencial para erro humano, especialmente quando o tempo disponível para o operador tomar decisões for curto. A probabilidade de que problemas irão se desenvolver suficientemente para tornarem-se graves pode ser pequena. Algumas vezes, porém, a ação humana será a única defesa para evitar que uma falha inicial progrida para um acidente.

A importância da ACH foi ilustrada por vários acidentes em que os erros humanos críticos contribuíram para uma sequência de eventos catastróficos. Tais acidentes são advertências contra os processos de avaliações de riscos que se concentram exclusivamente no *hardware* e *software* em um sistema. Eles ilustram os perigos de ignorar a possibilidade de contribuição do erro humano. Além disso, as ACH são úteis em destacar os erros que podem impedir a produtividade e em revelar as maneiras pelas quais esses erros e outras falhas (*hardware* e *software*) podem ser "recuperados" pelos operadores humanos e pelo pessoal de manutenção.

B.20.2 Utilização

A ACH pode ser utilizada qualitativamente ou quantitativamente. Qualitativamente, ela é utilizada para identificar o potencial de erro humano e suas causas de forma que a probabilidade de erro possa ser reduzida. A ACH quantitativa é utilizada para fornecer dados sobre falhas humanas em AAF ou outras técnicas.

B.20.3 Entradas

As entradas para a ACH incluem:

- informações para definir tarefas que as pessoas devem realizar;
- experiência dos tipos de erro que ocorrem na prática e o potencial para erro;
- especialidade em erro humano e sua quantificação.

B.20.4 Processo

O processo de ACH é o seguinte:

- **Definição do problema**, quais tipos de envolvimentos humanos devem ser investigados/avaliados?
- **Análise da tarefa**, como a tarefa será realizada e que tipo de auxílio será necessário para apoiar a realização?
- **Análise do erro humano**, como a realização da tarefa pode falhar: quais erros podem ocorrer e como eles podem ser recuperados?

Documento impresso em 03/04/2019 15:35:43, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- **Representação**, como estes erros ou falhas no desempenho da tarefa podem ser integrados com outro *hardware*, *software* e eventos ambientais para permitir que as probabilidades de falha no sistema total sejam calculadas?
- **Seleção**, existem erros ou tarefas que não requerem quantificação detalhada?
- **Quantificação**, quão prováveis são erros individuais e falhas nas tarefas?
- **Avaliação do impacto**, quais erros ou tarefas são mais importantes, ou seja, quais têm a maior contribuição para a confiabilidade ou risco?
- **Redução do erro**, como uma maior confiabilidade humana pode ser atingida?
- **Documentação**, quais detalhes da ACH precisam ser documentados?

Na prática, o processo de ACH desenvolve-se em etapas sequenciais, embora às vezes com partes prosseguindo em paralelo uma com outra (por exemplo, análise de tarefas e identificação de erros).

B.20.5 Saídas

As saídas incluem:

- uma lista de erros que podem ocorrer e os métodos pelos quais eles podem ser reduzidos – preferivelmente por meio de redesenho do sistema;
- modos de erro, causas e consequências dos tipos de erro;
- uma avaliação qualitativa ou quantitativa do risco representado pelos erros.

B.20.6 Pontos fortes e limitações

Os pontos fortes da ACH incluem:

- a ACH fornece um mecanismo formal para incluir o erro humano na consideração de riscos associados a sistemas onde a intervenção humana muitas vezes desempenha um papel importante;
- a consideração formal dos mecanismos e modos de erro humano pode auxiliar a reduzir a probabilidade de falha devido a um erro.

As limitações incluem:

- a complexidade e a variabilidade humanas, que tornam difícil a definição de modos e probabilidades de falha simples;
- muitas atividades humanas não têm um modo passa/não passa simples. A ACH dificilmente trata de falhas parciais ou falhas na qualidade ou na tomada de decisões deficiente.

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

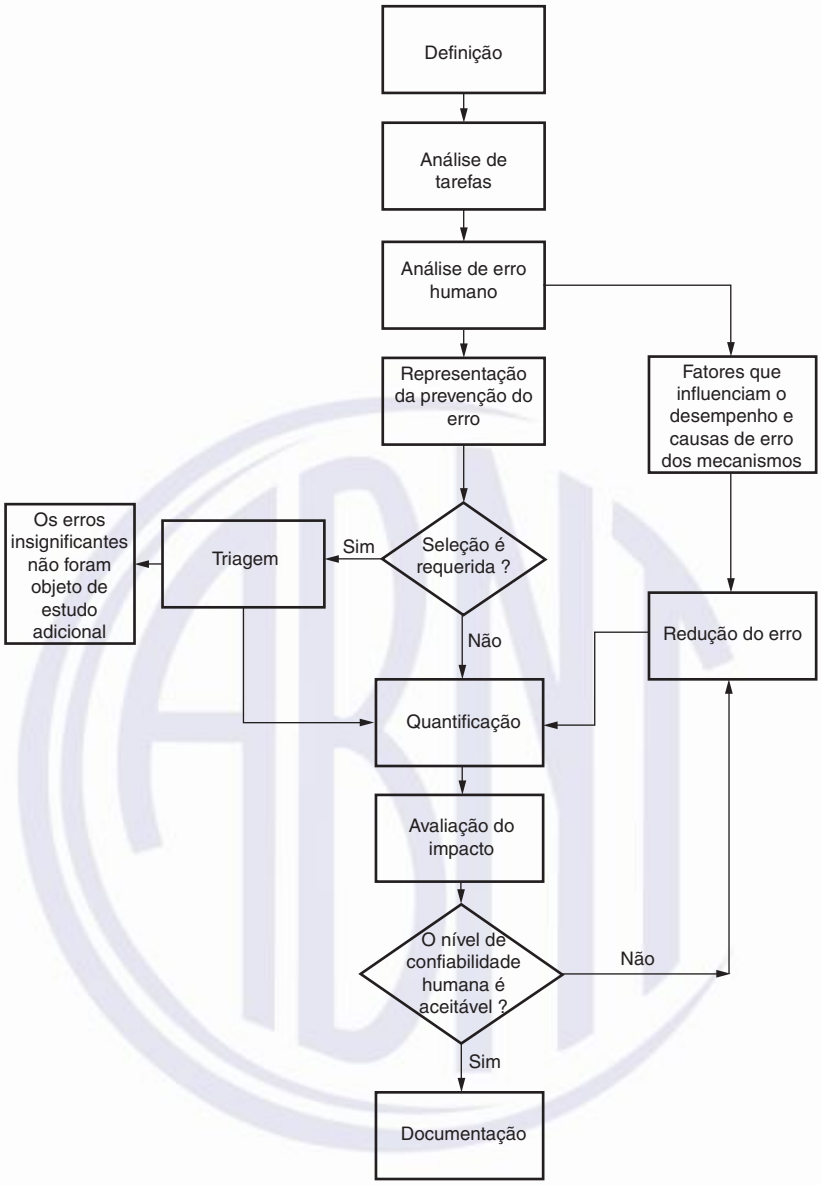

Figura B.7 – Exemplo de avaliação da confiabilidade humana

B.21 Análise *bow tie*

B.21.1 Visão geral

A análise *bow tie* é uma maneira esquemática simples de descrever e analisar os caminhos de um risco desde as causas até as consequências. Pode ser considerada uma combinação do raciocínio de árvore de falhas, que analisa a causa de um evento (representada pelo nó de uma *bow tie*), com árvore de eventos, que analisa as consequências. Entretanto, o foco *bow tie* está nas barreiras entre as causas e o risco, e o risco e as consequências. Diagramas de *bow tie* podem ser construídos a partir das árvores de falhas e eventos, porém são mais frequentemente desenhados diretamente a partir de uma sessão de *brainstorming*.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.21.2 Utilização

A análise *bow tie* é utilizada para representar um risco que possui uma gama de possíveis causas e consequências. É utilizada quando a situação não justificar a complexidade de uma análise de árvore de falhas completa ou quando o foco estiver mais em assegurar que existe uma barreira ou controle para cada caminho de falha. É útil quando há caminhos claros independentes levando à falha.

A análise *bow tie* é muitas vezes mais fácil de entender do que árvores de falhas e de eventos e, portanto, pode ser uma ferramenta de comunicação útil quando a análise for conseguida utilizando técnicas mais complexas.

B.21.3 Entradas

É necessária uma compreensão das causas e consequências de um risco e das barreiras e controles que podem evitá-lo, atenuá-lo ou estimulá-lo.

B.21.4 Processo

A *bow tie* é desenhada conforme descrito a seguir:

a) Um risco específico é identificado para análise e representado como o nó central de uma *bow tie*.

b) As causas do evento são listadas considerando as fontes de risco (ou perigos em um contexto de segurança).

c) O mecanismo pelo qual a fonte de risco leva ao evento crítico é identificado.

d) Linhas são traçadas entre cada causa e o evento formando o lado esquerdo da *bow tie*. Os fatores que podem levar a uma intensificação podem ser identificados e incluídos no diagrama.

e) As barreiras que evitariam que cada causa leve a consequências não desejadas podem ser mostradas como barras verticais cruzando a linha. Onde havia fatores que poderiam causar intensificação, as barreiras para a intensificação também podem ser representadas. A abordagem pode ser utilizada para consequências positivas, onde as barras refletem os “controles” que estimulam a geração do evento.

f) No lado direito da *bow tie* diferentes consequências potenciais do risco são identificadas e linhas são desenhadas para irradiar do evento de risco para cada consequência potencial.

g) As barreiras para a consequência são representadas como barras que cruzam as linhas radiais. A abordagem pode ser utilizada para efeitos positivos onde as barras refletem os “controles” que suportam a geração das consequências.

h) As funções de gestão que suportam os controles (como treinamento e inspeção) podem ser mostradas sob a *Bow tie* e vinculadas ao respectivo controle.

Algum nível de quantificação de um diagrama de *bow tie* pode ser possível quando os caminhos forem independentes, a probabilidade de uma consequência ou resultado específicos é conhecida e um valor pode ser estimado para a eficácia de um controle. Entretanto, em muitas situações, os caminhos e as barreiras não são independentes, os controles podem ser procedimentais e, consequentemente, a eficácia pouco clara. A quantificação é muitas vezes realizada mais apropriadamente utilizando AAF) e AAE.

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.21.5 Saída

A saída é um diagrama simples mostrando os principais caminhos de risco e as barreiras existentes para evitar ou atenuar as consequências indesejadas ou estimular e promover as consequências desejadas.

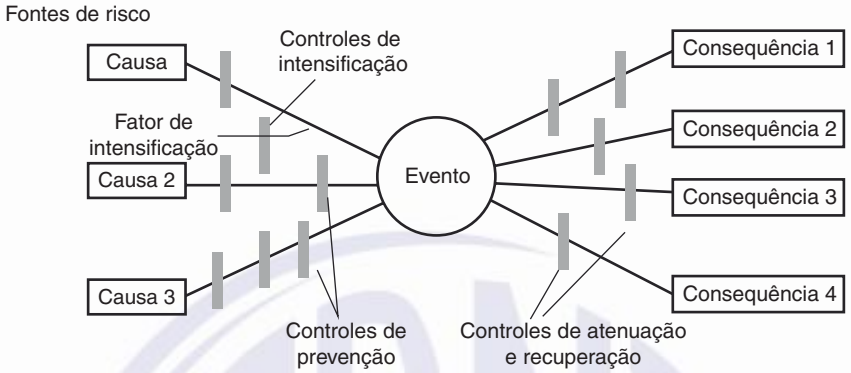

Figura B.8 – Exemplo de diagrama de "*bow tie*" para consequências indesejadas

B.21.6 Pontos fortes e limitações

Pontos fortes da análise de *bow tie*:

- é simples de entender e fornece uma representação gráfica clara do problema;
- foca a atenção nos controles supostamente existentes para prevenção e atenuação e sua eficácia;
- pode ser utilizada para consequências desejáveis;
- não necessita de um alto nível de especialização para utilizar.

As limitações incluem:

- não pode ser representada onde múltiplas causas ocorrem simultaneamente para resultar nas consequências (ou seja, onde houver portas "AND" em uma árvore de falhas representando o lado esquerdo do diagrama de *bow tie*);
- pode simplificar demasiadamente situações complexas, particularmente quando se pretende a quantificação.

B.22 Manutenção centrada em confiabilidade

B.22.1 Visão geral

A manutenção centrada em confiabilidade (RCM) é um método para identificar as políticas que é conveniente que sejam implementadas para gerenciar falhas, a fim de alcançar a segurança, disponibilidade e economia de operação requeridas, de maneira eficiente e eficaz, para todos os tipos de equipamento.

A RCM é atualmente uma metodologia comprovada e aceita, utilizada em uma ampla gama de indústrias.

A RCM fornece um processo de decisão para identificar requisitos de manutenção preventiva eficazes e aplicáveis para equipamentos de acordo com as consequências de segurança, operacionais e econômicas das falhas identificáveis, e o mecanismo de degradação responsável por essas falhas.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

O resultado final do processo é um julgamento quanto à necessidade de realizar uma tarefa de manutenção ou outras ações, como mudanças operacionais. Os detalhes sobre o uso e aplicação da RCM são fornecidos na IEC 60300-3-11.

B.22.2 Utilização

Todas as tarefas são baseadas na segurança no que diz respeito ao pessoal e ao meio ambiente, e nos interesses operacionais ou econômicos. Entretanto, convém que seja observado que os critérios considerados dependerão da natureza do produto e sua aplicação. Por exemplo, um processo de produção precisará ser economicamente viável e pode ser sensível a considerações ambientais rigorosas, enquanto que um item de equipamento de defesa deve ser operacionalmente bem-sucedido, porém pode ter critérios de segurança, econômicos e ambientais menos rigorosos. Maior benefício pode ser conseguido concentrando-se na análise de onde as falhas teriam graves efeitos, ambientais, econômicos, operacionais ou de segurança.

A RCM é utilizada para assegurar que se faz uma manutenção aplicável e eficaz, e é geralmente utilizada durante a fase de projeto e desenvolvimento e, em seguida, implementada durante a operação e manutenção.

B.22.3 Entradas

A aplicação bem-sucedida da RCM precisa de um bom entendimento do equipamento e da estrutura, do ambiente operacional e dos sistemas, subsistemas e itens do equipamento associados, juntamente com as possíveis falhas e as consequências dessas falhas.

B.22.4 Processo

As etapas básicas de um programa de RCM são as seguintes:

- início e planejamento;
- análise funcional de falhas;
- seleção de tarefas;
- implementação;
- melhoria contínua.

A RCM é baseada no risco, uma vez que ela segue as etapas básicas do processo de avaliação de riscos. O tipo de processo de avaliação de riscos é uma análise de modos de falha, efeitos e criticidade (FMECA) , porém requer uma abordagem específica para análise quando utilizado neste contexto.

A identificação de riscos foca nas situações onde as falhas potenciais podem ser eliminadas ou reduzidas em frequência e/ou consequência, realizando tarefas de manutenção. É realizada identificando as funções requeridas e os padrões de desempenho, assim como as falhas dos equipamentos e componentes que podem interromper essas funções.

A análise de riscos consiste em estimar a frequência de cada falha sem a manutenção ser realizada. As consequências são estabelecidas definindo os efeitos da falha. Uma matriz de risco que combina a frequência e as consequências da falha permite que categorias para os níveis de risco sejam estabelecidas.

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Avaliação de riscos é então realizada, selecionando a política de gestão de falha apropriada para cada modo de falha.

O processo de RCM completo é extensivamente documentado para referência e análise crítica futuras. A coleta de dados de falha e manutenção permite o monitoramento dos resultados e a implementação de melhorias.

B.22.5 Saída

A RCM fornece uma definição das tarefas de manutenção, como monitoramento da condição, restauração programada, substituição programada, pesquisa da falha ou manutenção não preventiva. Outras ações possíveis que podem resultar da análise podem incluir redesenho, alterações nos procedimentos de operação ou manutenção ou treinamento adicional. Os intervalos das tarefas e os recursos requeridos são então identificados.

B.22.6 Documentos de referência

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.23 *Sneak analysis (SA) e sneak circuit analysis* (SCA)

B.23.1 Visão geral

A *sneak analysis* (SA) é uma metodologia para a identificação de erros de projeto. Uma condição *sneak* é um *hardware*, *software* ou condição integrada latente que pode causar a ocorrência de um evento indesejado ou inibir um evento desejado, não sendo causado por falha do componente. Estas condições são caracterizadas pela sua natureza aleatória e capacidade de escapar à detecção durante os ensaios normalizados mais rigorosos do sistema. As condições *sneak* podem causar operação imprópria, perda da disponibilidade do sistema, atrasos no programa ou mesmo morte ou ferimento de pessoas.

B.23.2 Utilização

A *sneak circuit analysis* (SCA) foi desenvolvida no final dos anos 60 para a NASA, a fim de verificar a integridade e a funcionalidade de seus projetos. Ela serviu como uma ferramenta útil para a descoberta de caminhos de circuito elétrico involuntários e auxiliou na elaboração de soluções para isolar cada função. Entretanto, como a tecnologia avançou, as ferramentas para a *sneak circuit analysis* também teve de avançar. A *sneak analysis* inclui e excede a cobertura da *sneak circuit analysis*. Ela pode localizar problemas em *hardware* e *software* utilizando qualquer tecnologia. As ferramentas de *sneak analysis* podem integrar diversas análises, como árvores de falhas, *failure mode and effect analysis* (FMEA), estimativas de confiabilidade etc. em uma única análise, economizando tempo e despesas de projeto.

B.23.3 Entradas

A *sneak analysis* é uma ferramenta única do processo de projeto na medida em que ela utiliza diferentes ferramentas (rede de árvores, florestas e índices ou questões para auxiliar o analista a identificar as condições *sneak*) para encontrar um tipo específico de problema. As redes de árvores e florestas são agrupamentos topológicos do sistema real. Cada rede de árvores representa uma subfunção e mostra

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

todas as entradas que podem afetar a saída da subfunção. As florestas são construídas combinando as redes de árvores que contribuem para uma saída do sistema específico. Uma floresta apropriada mostra uma saída do sistema em termos de todas as suas entradas relacionadas. Estas, juntamente com outros, tornam-se a entrada para a análise.

B.23.4 Processo

As etapas básicas na realização de uma *sneak analysis* consistem em:

- preparação dos dados;
- construção da rede de árvores;
- avaliação dos caminhos da rede;
- recomendações finais e relatório.

B.23.5 Saída

Um *sneak circuit* é um caminho inesperado ou fluxo lógico dentro de um sistema que, sob certas condições, pode iniciar uma função indesejada ou inibir uma função desejada. O caminho pode consistir de *hardware*, *software*, ações do operador ou combinações destes elementos. Os *sneak circuits* não são o resultado de uma falha de *hardware*, porém são condições latentes, inadvertidamente projetadas no sistema, codificadas no programa de *software* ou provocadas por erro humano. Há quatro categorias de *sneak circuits*:

a) caminhos *sneak*: caminhos inesperados ao longo dos quais a corrente, energia ou sequência lógica flui em uma direção não pretendida;

b) sincronismo *sneak*: eventos que ocorrem em uma sequência inesperada ou conflitante;

c) indicações *sneak*: exibições ambíguas ou falsas das condições operacionais do sistema que podem fazer com que o sistema ou um operador tomem uma ação indesejada;

d) rótulos *sneak*: rotulagem incorreta ou imprecisa das funções do sistema, por exemplo, entradas do sistema, controles, barramentos que podem levar a que um operador aplique um estímulo incorreto ao sistema.

B.23.6 Pontos fortes e limitações

Os pontos fortes incluem:

- a *sneak analysis* é boa para a identificação de erros de projeto;
- funciona melhor quando aplicada em conjunto com o *HAZOP*;
- é muito boa para tratar de sistemas que tenham estados múltiplos, como plantas em lote e semilote.

As limitações podem incluir:

- o processo é um pouco diferente, dependendo se é aplicado a circuitos elétricos, plantas de processamento, equipamentos mecânicos ou *software*;
- o método é dependente do estabelecimento correto da rede de árvores.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.24 Análise de Markov

B.24.1 Visão geral

A análise de Markov é utilizada quando o estado futuro de um sistema depende somente de seu estado atual. Ela é comumente utilizada para a análise de sistemas reparáveis que podem existir em múltiplos estados e a utilização de uma análise de bloco de confiabilidade seria inapropriada para analisar adequadamente o sistema. O método pode ser estendido para sistemas mais complexos, empregando processos de Markov de ordem mais elevada, e é somente restrito pelo modelo, cálculos matemáticos e as premissas.

O processo da análise de Markov é uma técnica quantitativa e pode ser discreto (utilizando probabilidades de mudança entre os estados) ou contínuo (utilizando taxas de mudança através dos estados).

Apesar de uma análise de Markov poder ser realizada manualmente, a natureza das técnicas se presta ao uso de programas de computador, estando muitos deles disponíveis no mercado.

B.24.2 Utilização

A técnica de análise de Markov pode ser utilizada em várias estruturas de sistema, com ou sem reparo, incluindo:

- componentes independentes em paralelo;
- componentes independentes em série;
- sistema de compartilhamento de carga;
- sistema de espera (*stand-by*), incluindo o caso onde falha na comutação pode ocorrer;
- sistemas degradados.

A técnica de análise de Markov também pode ser utilizada para o cálculo da disponibilidade, inclusive levando em consideração os componentes sobressalentes para reparos.

B.24.3 Entradas

As entradas essenciais para uma análise de Markov são as seguintes:

- lista dos vários estados em que o sistema, subsistema ou componente pode estar (por exemplo, totalmente operacional, parcialmente em operação (ou seja, um estado degradado), estado de falha etc.);
- um entendimento claro das transições possíveis que é necessário que sejam modeladas. Por exemplo, a falha de um pneu de automóvel precisa considerar o estado da roda sobressalente e, portanto, a frequência de inspeção;
- taxa de mudança de um estado para outro, tipicamente representada por uma probabilidade de mudança entre os estados para eventos discretos, ou taxa de falha (λ) e/ou a taxa de reparo (μ) para eventos contínuos.

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.24.4 Processo

A técnica de análise de Markov é centrada em torno do conceito de “estados”, por exemplo, “disponível” e “falho”, e a transição entre estes dois estados ao longo do tempo com base em uma probabilidade constante de mudança. Uma matriz de probabilidade de transição estocástica é utilizada para descrever a transição entre cada um dos estados para permitir o cálculo das várias saídas.

Para ilustrar a técnica de análise de Markov, considerar um sistema complexo que pode estar somente em três estados; funcionando, degradado e falho, definidos como estados S1, S2, S3, respectivamente. Cada dia o sistema existe em um destes três estados. A Tabela B.2 mostra a probabilidade de que amanhã, o sistema esteja em estado S*i* onde *i* pode ser 1, 2 ou 3.

Tabela B.2 – Matriz de Markov

		Estado hoje		
		S1	S2	S3
Estado amanhã	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Esta matriz de probabilidades é chamada de matriz de Markov ou matriz de transição. Observar que a soma para cada uma das colunas é 1, já que é a soma de todos os resultados possíveis em cada caso. O sistema também pode ser representado por um diagrama de Markov, onde os círculos representam os estados e as setas representam a transição, juntamente com a probabilidade que as acompanham.

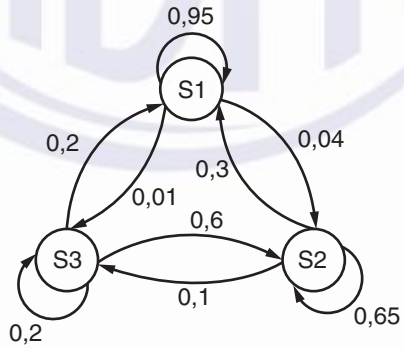

Figura B.9 – Exemplo de diagrama de Markov do sistema

As setas de um estado para si mesmo não são geralmente mostradas, porém são mostradas dentro destes exemplos para completeza.

Seja P*i* a probabilidade de encontrar o sistema no estado *i* para *i* = 1, 2, 3, então as equações simultâneas a serem resolvidas são:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \quad \text{(B.1)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \quad \text{(B.2)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \quad \text{(B.3)}$$

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Estas três equações não são independentes e não resolverão as três incógnitas. Convém que a seguinte equação seja utilizada e uma das equações acima descartada.

$$1 = P1 + P2 + P3 \quad \text{(B.4)}$$

A solução é 0,85, 0,13 e 0,02 para os respectivos estados 1, 2, 3. O sistema está funcionando plenamente em 85 % do tempo, no estado degradado em 13 % do tempo e no estado de falha em 2 % do tempo.

Considerar dois itens operando em paralelo com o requisito de um ou outro estar operacional para o sistema funcionar. Os itens podem tanto ser operacionais quanto falhos, e a disponibilidade do sistema depende do estado dos itens.

Os estados podem ser considerados como:

Estado 1 Ambos os itens estão funcionando corretamente;

Estado 2 Um item falhou e está passando por reparos, o outro está funcionando;

Estado 3 Ambos os itens falharam e um está passando por reparos.

Se a taxa de falha contínua para cada item for assumida como sendo λ e a taxa de reparo como sendo μ, então o diagrama de transição de estado é:

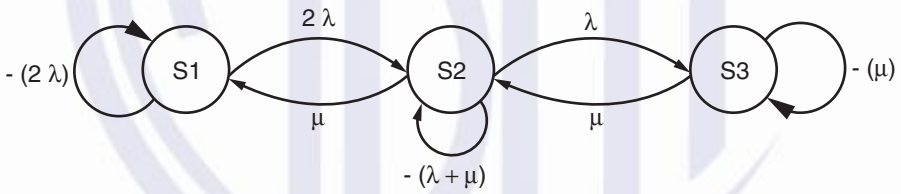

Figura B.10 – Exemplo de diagrama de transição de estado

Observar que a transição do estado 1 para o estado 2 é 2λ, já que a falha de qualquer um dos dois itens levará o sistema para o estado 2.

Seja P*i* (*t*) a probabilidade de estar em um estado inicial *i* no tempo *t*; e

Seja P*i* ($t + \delta t$) a probabilidade de estar em um estado final no tempo $t + \delta t$

A matriz de probabilidade de transição torna-se:

Tabela B.3 – Matriz de Markov final

		Estado inicial		
		P1(*t*)	P2(*t*)	P3(*t*)
Estado final	P1($t + \delta t$)	-2λ	μ	0
	P2($t + \delta t$)	2λ	$-(\lambda + \mu)$	μ
	P3($t + \delta t$)	0	λ	$-\mu$

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

É interessante notar que os valores zero ocorrem, já que não é possível passar do estado 1 para o estado 3 ou do estado 3 para o estado 1. Além disso, a soma das colunas é zero, quando se especificam as taxas.

As equações simultâneas tornam-se:

$$dP1/dt = -2\lambda\, P1(t) + \mu\, P2(t) \quad \text{(B.5)}$$

$$dP2/dt = 2\lambda\, P1(t) + -(\lambda + \mu)\, P2(t) + \mu\, P3(t) \quad \text{(B.6)}$$

$$dP3/dt = \lambda\, P2(t) + -\mu\, P3(t) \quad \text{(B.7)}$$

Por simplicidade, será assumido que a disponibilidade requerida é a disponibilidade em regime permanente.

Quando δt tende ao infinito, DPi/dt tenderá a zero e as equações se tornam mais fáceis de resolver. A equação adicional, conforme mostrado na Equação (B.4) acima, também deve ser utilizada:

Agora, a equação $A(t) = P1(t) + P2(t)$ pode ser expressa como:

$A = P1 + P2$

Portanto, $A = (\mu^2 + 2\,\lambda\,\mu)/(\mu^2 + 2\,\lambda\,\mu + \lambda^2)$

B.24.5 Saídas

As saídas de uma análise de Markov são as várias probabilidades de estar nos vários estados e, portanto, uma estimativa das probabilidades de falha e/ou disponibilidade, um dos componentes essenciais de um sistema.

B.24.6 Pontos fortes e limitações

Os pontos fortes de uma análise de Markov incluem:

- capacidade de calcular as probabilidades para sistemas com uma capacidade de reparo e múltiplos estados degradados.

As limitações de uma análise de Markov incluem:

- a premissa de probabilidades constantes de mudança de estado, seja de falha ou reparos;
- todos os eventos são estatisticamente independentes, uma vez que os estados futuros são independentes de todos os estados passados, exceto para o estado imediatamente anterior;
- necessidade de conhecimento de todas as probabilidades de mudança de estado;
- conhecimento de operações com matrizes;
- os resultados são difíceis de comunicar para pessoal não técnico.

B.24.7 Comparações

A análise de Markov é similar a uma análise de Rede de Petri por ser capaz de monitorar e observar os estados do sistema, embora diferente uma vez que a Rede de Petri pode existir em vários estados ao mesmo tempo.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.24.8 Documentos de referência

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (todas as partes), *Software and systems engineering – High-level Petri nets*

B.25 Simulação de Monte Carlo

B.25.1 Visão geral

Muitos sistemas são muito complexos quanto aos efeitos da incerteza sobre eles para serem modelados utilizando técnicas analíticas, porém eles podem ser avaliados considerando as entradas como variáveis aleatórias e executando-se um número N de cálculos (as chamadas simulações), por meio de amostragens da entrada, a fim de obter N saídas possíveis do resultado desejado.

Este método pode tratar de situações complexas que seriam muito difíceis de entender e resolver por um método analítico. Sistemas podem ser desenvolvidos utilizando planilhas e outras ferramentas convencionais, porém ferramentas mais sofisticadas estão prontamente disponíveis para auxiliar com requisitos mais complexos, muitas das quais são relativamente baratas. Quando a técnica foi desenvolvida pela primeira vez, o número de iterações requerido para as simulações de Monte Carlo resultou em um processo lento e demorado, porém os avanços nos desenvolvimentos de computadores e teóricos, como amostragem por Hipercubo Latino, tornaram o tempo de processamento quase insignificante para muitas aplicações.

B.25.2 Utilização

A simulação de Monte Carlo fornece um meio de avaliar o efeito da incerteza em sistemas em uma ampla gama de situações. É tipicamente utilizado para avaliar a faixa de possíveis resultados e a frequência relativa de valores naquela faixa para medidas quantitativas de um sistema, como custo, duração, intensidade, demanda e medidas similares. A simulação de Monte Carlo pode ser utilizada para duas finalidades diferentes:

- propagação da incerteza em modelos analíticos convencionais;
- cálculos probabilísticos quando as técnicas analíticas não funcionam.

B.25.3 Entradas

As entradas para uma simulação de Monte Carlo são um bom modelo do sistema e informações sobre os tipos de entradas, as fontes de incerteza que devem ser representadas e as saídas requeridas. Os dados de entrada, juntamente com as suas incertezas, são representados como variáveis aleatórias cujas distribuições são mais ou menos dispersas de acordo com o nível das incertezas. Distribuições uniformes, triangulares, normais e log normais são frequentemente utilizadas para esse fim.

B.25.4 Processo

O processo é o seguinte:

a) Um modelo ou algoritmo é definido, o qual representa, tanto quanto possível, o comportamento do sistema que está sendo estudado.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

b) O modelo é executado várias vezes, utilizando números aleatórios para produzir saídas do modelo (simulações do sistema). Quando a aplicação é para modelar os efeitos da incerteza, o modelo está sob a forma de uma equação fornecendo a relação entre os parâmetros de entrada e uma saída. Os valores selecionados para as entradas são tomados a partir de distribuições de probabilidade apropriadas que representam a natureza da incerteza nestes parâmetros.

c) Em ambos os casos um computador executa o modelo várias vezes (frequentemente até 10 000 vezes) com diferentes entradas e produz saídas múltiplas. Estes dados podem ser processados utilizando estatísticas convencionais para fornecer informações, como valores médios, desvio padrão e intervalos de confiança.

Um exemplo de uma simulação é dado abaixo.

Considerar o caso de dois itens que operam em paralelo e somente um é requerido para que o sistema funcione. O primeiro item tem uma confiabilidade de 0,9 e o outro de 0,8.

É possível construir uma planilha com as seguintes colunas.

Tabela B.4 – Exemplo de simulação de Monte Carlo

	Item 1		Item 2		
Número de simulação	**Número aleatório**	**Funções?**	**Número aleatório**	**Funções?**	**Sistema**
1	0,577 243	SIM	0,059 355	SIM	1
2	0,746 909	SIM	0,311 324	SIM	1
3	0,541 728	SIM	0,919 765	NÃO	1
4	0,423 274	SIM	0,643 514	SIM	1
5	0,917 776	NÃO	0,539 349	SIM	1
6	0,994 043	NÃO	0,972 506	NÃO	0
7	0,082 574	SIM	0,950 241	NÃO	1
8	0,661 418	SIM	0,919 868	NÃO	1
9	0,213 376	SIM	0,367 555	SIM	1
10	0,565 657	SIM	0,119 215	SIM	1

O gerador aleatório cria um número entre 0 e 1 que é utilizado para comparar com a probabilidade de cada item para determinar se o sistema está operacional. Com apenas 10 execuções, não convém esperar que o resultado de 0,9 seja um resultado exato. A abordagem usual é construir um dispositivo de cálculo para comparar o resultado total enquanto a simulação prossegue para atingir o nível de exatidão requerido. Neste exemplo, um resultado de 0,979 9 foi atingido após 20 000 iterações.

O modelo acima pode ser estendido em inúmeras maneiras. Por exemplo:

- estendendo o próprio modelo (como considerar o segundo item tornando-se imediatamente operacional somente quando o primeiro item falhar);

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

- alterando a probabilidade fixada a uma variável (um bom exemplo é a distribuição triangular), quando a probabilidade não pode ser definida com exatidão;
- utilizando taxas de falha combinadas com o gerador aleatório para deduzir um tempo de falha (exponencial, *Weibull* ou outra distribuição apropriada) e introduzindo tempos de reparo.

As aplicações incluem, entre outras coisas, a avaliação da incerteza em previsões financeiras, desempenho de investimentos, custo de projetos e previsões de programação, interrupções no processo de negócios e requisitos de pessoal.

As técnicas analíticas não são capazes de fornecer resultados pertinentes quando existem incertezas nos dados de entrada e consequentemente nas saídas.

B.25.5 Saídas

A saída pode ser um valor único, conforme determinado no exemplo acima, pode ser um resultado expresso como a probabilidade ou distribuição da frequência ou pode ser a identificação das funções principais dentro do modelo que tem o maior impacto na saída.

Em geral, uma simulação de Monte Carlo será utilizada para avaliar tanto a distribuição global dos resultados que poderiam surgir quanto as medidas-chave de uma distribuição, como:

- a probabilidade de um resultado decorrente definido;
- o valor de um resultado em que os donos do problema têm um certo nível de confiança que não será ultrapassado ou superado, um custo que tenha uma chance de 10 % de ser ultrapassado ou uma duração que tenha 80 % de certeza de ser ultrapassada.

Uma análise das relações entre as entradas e as saídas pode lançar luz sobre a significância relativa dos fatores em ação e identificar alvos úteis para os esforços em influenciar a incerteza no resultado.

B.25.6 Pontos fortes e limitações

Os pontos fortes da análise de Monte Carlo incluem os seguintes:

- o método pode, em princípio, acomodar qualquer distribuição de uma variável de entrada, incluindo distribuições empíricas derivadas das observações de sistemas relacionados;
- os modelos são relativamente simples de desenvolver e podem ser estendidos em caso de necessidade;
- quaisquer influências ou relações que surgirem na realidade podem ser representadas, incluindo efeitos sutis como dependências condicionais;
- análise de sensibilidade pode ser aplicada para identificar influências fortes e fracas;
- os modelos podem ser facilmente entendidos, uma vez que a relação entre entradas e saídas é transparente;
- modelos comportamentais eficientes, como Redes de Petri (futura IEC 62551), estão disponíveis e demonstraram ser muito eficientes para fins da simulação de Monte Carlo;
- fornece uma medida da exatidão de um resultado;
- o *software* está disponível e é relativamente barato.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

As limitações são as seguintes:

- a exatidão das soluções depende do número de simulações que podem ser realizadas (esta limitação está se tornando menos importante com o aumento da velocidade dos computadores);
- ela se baseia em ser capaz de representar as incertezas nos parâmetros por meio de uma distribuição válida;
- modelos grandes e complexos podem ser um desafio para o modelador e tornar difícil o engajamento das partes interessadas no processo;
- a técnica pode não ponderar adequadamente eventos de alta consequência/baixa probabilidade e, portanto, não permite refletir o apetite ao risco da organização na análise.

B.25.7 Documentos de referência

IEC 61649, *Weibull analysis*

IEC 62551, *Analysis techniques for dependability – Petri net technique* [1]

ISO/IEC Guide 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement* (GUM:1995)

B.26 Estatística Bayesiana e Redes de Bayes

B.26.1 Visão geral

As estatísticas Bayesianas são atribuídas ao Reverendo Thomas Bayes. Sua premissa é que quaisquer informações já conhecidas (*a priori*) podem ser combinadas com medições subsequentes (*a posteriori*) para estabelecer uma probabilidade global. A expressão geral do Teorema de Bayes pode ser expressa como:

$$\mathrm{P}(A \mid B) = \left\{\mathrm{P}(A)\,\mathrm{P}(B \mid A)\right\} \Big/ \sum_i \mathrm{P}(B \mid \mathrm{E}_i)\,P(\mathrm{E}_i)$$

onde

a probabilidade de X é indicada por P(X);

a probabilidade de X com a condição de que tenha ocorrido Y é indicada por P (X|Y); e

Ei é o enésimo evento.

Na sua forma mais simples, esta expressão reduz-se a P(A|B) = {P(A)P(B|A)}/P(B).

A estatística Bayesiana difere da estatística clássica ao não assumir que todos os parâmetros da distribuição sejam fixos, mas sim variáveis aleatórias. Uma probabilidade Bayesiana pode ser mais facilmente entendida se ela for considerada como o grau em que uma pessoa acredita em um determinado evento, oposto à teoria clássica, que é baseada em evidências físicas. Como a abordagem Bayesiana é baseada na interpretação subjetiva de probabilidade, ela fornece uma base direta para o pensamento decisório e o desenvolvimento de redes de Bayes (ou redes de crença ou redes Bayesianas).

[1] Atualmente em estudo.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

As redes de Bayes utilizam um modelo gráfico para representar um conjunto de variáveis e suas relações probabilísticas. A rede é composta de nós que representam uma variável aleatória e setas que conectam um nó pai a um nó filho, (onde um nó pai é uma variável que influencia diretamente a outra variável filho).

B.26.2 Utilização

Nos últimos anos, o uso da teoria e das redes de Bayes tornou-se generalizado, em parte devido ao seu apelo intuitivo e também por causa da disponibilidade de ferramentas computacionais de *software*. As redes de Bayes têm sido utilizadas em uma ampla gama de tópicos: diagnósticos médicos, modelagem de imagens, genética, reconhecimento de voz, economia, exploração espacial e nas poderosas ferramentas de busca na *Web* utilizadas hoje em dia. Podem ser valiosas em qualquer área onde for requerida a pesquisa de variáveis desconhecidas por meio da utilização de dados e relações estruturais. As redes de Bayes podem ser utilizadas para conhecer relações causais de maneira a obter uma compreensão sobre um domínio de problemas e prever as consequências de intervenção.

B.26.3 Entradas

As entradas são similares às entradas para um modelo de Monte Carlo. Para uma rede de Bayes, os exemplos das etapas a serem seguidas incluem as seguintes:

- definir as variáveis do sistema;
- definir as ligações causais entre variáveis;
- especificar probabilidades condicionais e probabilidades *a priori*;
- adicionar evidência à rede;
- realizar atualização de crenças;
- extrair crenças *a posteriori*.

B.26.4 Processo

A teoria de Bayes pode ser aplicada em uma ampla variedade de maneiras. Este exemplo considerará a criação de uma tabela de Bayes, onde um ensaio médico é utilizado para determinar se o paciente tem uma doença. A crença antes de realizar o ensaio é que 99 % da população não tem essa doença e 1 % tem a doença, ou seja, a informação *a priori*. A exatidão do ensaio mostrou que, se a pessoa tiver a doença, o resultado do ensaio é positivo em 98 % das vezes. Existe também uma probabilidade de que, se você não tiver a doença, o resultado do ensaio seja positivo em 10 % das vezes. A tabela de Bayes fornece as seguintes informações:

Tabela B.5 – Dados da tabela de Bayes

	A priori	**PROBABILIDADE**	**PRODUTO**	***A posteriori***
Tem a doença	0,01	0,98	0,009 8	0,090 1
Não tem a doença	0,99	0,10	0,099 0	0,909 9
SOMATÓRIA	1		0,108 8	1

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Utilizando a regra de Bayes, o produto é determinado pela combinação do valor *a priori* e da probabilidade. O valor *a posteriori* é encontrado dividindo o valor do produto pela soma dos produtos (produto total). A saída mostra que um resultado de ensaio positivo indica que o valor *a priori* aumentou de 1 % para 9 %. Mais importante ainda, há uma forte probabilidade de que, mesmo com um ensaio positivo, ter a doença seja improvável. O exame da equação $(0{,}01 \times 0{,}98)/((0{,}01 \times 0{,}98) + (0{,}99 \times 0{,}1))$ mostra que o valor "resultado positivo sem doença" desempenha um papel mais importante nos valores *a posteriori*.

Considerar a seguinte rede de Bayes:

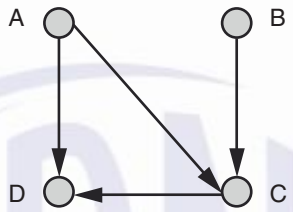

Figura B.11 – Exemplo de rede de Bayes

Com as probabilidades condicionais *a priori* definidas dentro das tabelas seguintes e utilizando a notação de que Y indica positivo e N indica negativo, o positivo poderia ser "tem doença" como acima, ou poderia ser Alto e N poderia ser Baixo.

Tabela B.6 – Probabilidades *a priori* para os nós A e B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Tabela B.7 – Probabilidades condicionais para o nó C com o nó A e o nó B definidos

A	*B*	P(*C* = *Y*)	P(*C* = *N*)
Y	Y	0,5	0,5
Y	N	0,9	0,1
N	Y	0,2	0,8
N	N	0,7	0,3

Tabela B.8 – Probabilidades condicionais para o nó D com o nó A e o nó C definidos

A	*C*	P(*D* = *Y*)	P(*D* = *N*)
Y	Y	0,6	0,4
Y	N	1,0	0,0
N	Y	0,2	0,8
N	N	0,6	0,4

Para determinar a probabilidade *a posteriori* P(A|D=N, C=Y), é necessário primeiro calcular P(A,B|D=N,C=Y).

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Utilizando a regra de Bayes, o valor P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*) é determinado conforme mostrado a seguir e a última coluna mostra as probabilidades normalizadas que somam 1, conforme deduzidas do exemplo anterior (resultado arredondado).

Tabela B.9 – Probabilidade *a posteriori* para os nós A e B com o nó D e o nó C definidos

A	B	P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*)	P(*A*,*B*|*D*=*N*,*C*=*Y*)
Y	Y	$0,4 \times 0,5 \times 0,9 \times 0,6 = 0,110$	0,4
Y	N	$0,4 \times 0,9 \times 0,9 \times 0,4 = 0,130$	0,48
N	Y	$0,8 \times 0,2 \times 0,1 \times 0,6 = 0,010$	0,04
N	N	$0,8 \times 0,7 \times 0,1 \times 0,4 = 0,022$	0,08

Para deduzir P(*A*|*D*=*N*,*C*=*Y*), todos os valores de *B* devem ser somados:

Tabela B.10 – Probabilidade *a posteriori* para o nó A, com o nó D e o nó C definidos

P(*A*=*Y*|*D*=*N*,*C*=*Y*)	P(*A*=*N*|*D*=*N*,*C*=*Y*)
0,88	0,12

Isto mostra que o valor *a priori* anterior para P(*A*=*N*) aumentou de 0,1 para *a posteriori* de 0,12, que é somente uma pequena alteração. Por outro lado, P(*B*=*N*|*D*=*N*,*C*=*Y*) foi alterado de 0,4 para 0,56, que é uma alteração mais significativa.

B.26.5 Saídas

A abordagem Bayesiana pode ser aplicada da mesma forma que a estatística clássica com uma ampla gama de saídas, por exemplo, análise de dados para deduzir estimativas de ponto e intervalos de confiança. Sua recente popularidade deve-se ao uso de redes de Bayes para deduzir distribuições *a posteriori.* A saída gráfica fornece um modelo de fácil compreensão e os dados podem ser facilmente modificados para considerar as correlações e a sensibilidade de parâmetros.

B.26.6 Pontos fortes e limitações

Pontos fortes:

- tudo que é necessário é o conhecimento sobre os *a priori*;
- as declarações inferenciais são fáceis de entender;
- a regra de Bayes é tudo o que é necessário;
- fornece um mecanismo para utilização de crenças subjetivas em um problema.

Limitações:

- a definição de todas as interações em redes de Bayes para sistemas complexos é problemática;
- a abordagem Bayesiana necessita do conhecimento de uma infinidade de probabilidades condicionais que são geralmente providas por julgamentos de especialistas. As ferramentas de *software* somente podem fornecer respostas com base nestas premissas.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.27 Curvas FN

B.27.1 Visão geral

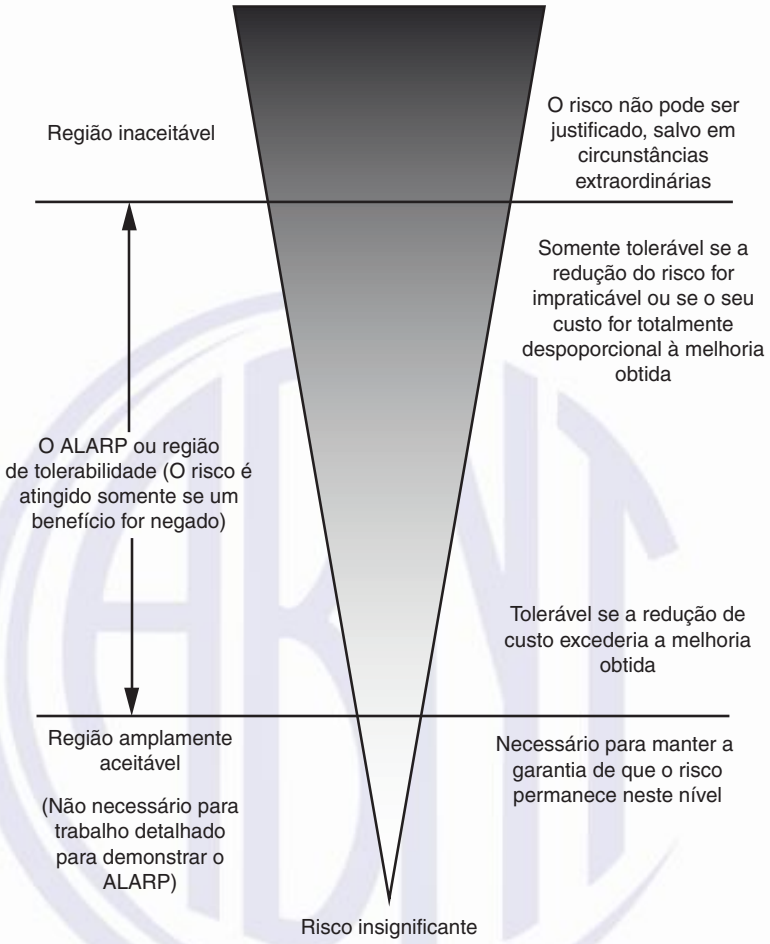

Figura B.12 – O conceito ALARP

As curvas FN são uma representação gráfica da probabilidade de eventos que causam um nível especificado de danos para uma população específica. Na maioria das vezes se referem à frequência de um determinado número de vítimas.

As curvas FN mostram a frequência acumulada (F) em que N ou mais membros da população serão afetados. Os altos valores de N que podem ocorrer com uma alta frequência F são de interesse significativo, pois eles podem ser social e politicamente inaceitáveis.

B.27.2 Utilização

As curvas FN são uma forma de representar as saídas da análise de riscos. Muitos eventos têm uma alta probabilidade de um resultado de consequência baixa e uma baixa probabilidade de um resultado de consequência alta. As curvas FN fornecem uma representação do nível de risco como uma linha que o descreve em vez de um único ponto representando um par probabilidade-consequência.

As curvas FN podem ser utilizadas para comparar riscos, por exemplo, comparar riscos previstos contra critérios definidos como uma curva FN, ou comparar riscos previstos com dados de incidentes históricos, ou com critérios de decisão (também expresso como uma curva F/N).

As curvas FN podem ser utilizadas tanto para o projeto de sistemas ou processos, ou para gestão de sistemas existentes.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

B.27.3 Entradas

As entradas são:

- conjuntos dos pares de consequência-probabilidade cobrindo um determinado período de tempo;
- dados de saída de uma análise de risco quantitativa fornecendo probabilidades estimadas para números especificados de vítimas;
- dados tanto de registros históricos quanto de uma análise de risco quantitativa.

B.27.4 Processo

Os dados disponíveis são traçados em um gráfico com o número de vítimas (para um nível especificado de dano, ou seja, morte) formando a abcissa, com a probabilidade de N ou mais vítimas formando as ordenadas. Devido à grande faixa de valores, ambos os eixos são normalmente em escalas logarítmicas.

As curvas FN podem ser construídas estatisticamente utilizando números “reais” de perdas no passado ou podem ser calculadas a partir de estimativas de modelos de simulação. Os dados utilizados e as premissas efetuadas podem significar que estes dois tipos de curva FN dão informações diferentes e convém que sejam utilizados separadamente e para diferentes finalidades. Em geral, as curvas FN teóricas são mais úteis para projeto de sistemas, e as curvas FN estatísticas são mais úteis para gestão de um sistema específico existente.

Ambas as abordagens de derivação podem ser muito demoradas e por isso não é incomum uma mistura de ambas. Os dados empíricos formarão então pontos fixos representando vítimas precisamente conhecidas que ocorreram em acidentes/incidentes conhecidos em um período de tempo especificado e a análise de risco quantitativa fornecendo outros pontos por extrapolação ou interpolação.

A necessidade de considerar acidentes de baixa frequência e alta consequência pode requerer a consideração de longos períodos de tempo para coletar dados suficientes para uma análise apropriada. Isto, por sua vez, pode tornar os dados disponíveis suspeitos, se alterações nos eventos iniciais acontecerem ao longo do tempo.

B.27.5 Saídas

Uma linha que representa o risco através de uma faixa de valores de consequência que pode ser comparada com critérios que são apropriados para a população que está sendo estudada e o nível especificado de danos.

B.27.6 Pontos fortes e limitações

As curvas FN são uma forma útil de apresentar informações sobre riscos que podem ser utilizadas por gestores e projetistas de sistemas para auxiliar na tomada de decisões sobre os níveis de risco e segurança. Elas são uma forma útil de apresentar informações de frequência e consequência em um formato acessível.

As curvas FN são apropriadas para a comparação de riscos de situações similares onde dados suficientes estão disponíveis. Convém que elas não sejam utilizadas para comparar riscos de diferentes tipos com características variáveis em circunstâncias onde a quantidade e a qualidade dos dados também variam.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:36:05, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Uma limitação das curvas FN é que elas não dizem nada sobre a faixa de efeitos ou resultados de incidentes, exceto o número de pessoas impactadas, e não há uma maneira de identificar as diferentes formas em que o nível de dano pode ter ocorrido. Elas mapeiam um tipo de consequência específica, geralmente dano às pessoas. As curvas FN não são um método de processo de avaliação de riscos, mas uma maneira de apresentar os resultados do processo de avaliação de riscos.

São um método bem estabelecido para a apresentação de resultados do processo de avaliação de riscos, porém requerem preparação por analistas especializados e são muitas vezes difíceis de serem interpretadas e avaliadas por não especialistas.

B.28 Índices de risco

B.28.1 Visão geral

Um índice de risco é uma medida semiquantitativa do risco. É uma estimativa derivada utilizando uma abordagem de pontuação mediante escalas ordinais. Os índices de risco podem ser utilizados para avaliar uma série de riscos com o uso de critérios similares, de modo a que possam ser comparados. Pontuações são aplicadas para cada componente de risco, por exemplo, características do contaminante (fontes), a faixa de possíveis vias de exposição e o impacto sobre os receptores.

Os índices de risco são essencialmente uma abordagem qualitativa para a classificação e a comparação de riscos. Embora números sejam utilizados, isto é feito simplesmente para permitir manipulação dos dados. Em muitos casos onde o modelo ou sistema subjacente não é bem conhecido ou não é capaz de ser representado, é melhor utilizar uma abordagem qualitativa mais aberta.

B.28.2 Utilização

Os índices podem ser utilizados para classificar diferentes riscos associados a uma atividade, se o sistema for bem entendido. Permitem a integração de uma faixa de fatores com impacto sobre o nível de risco em uma única pontuação numérica para um dado nível de risco.

Os índices são utilizados para tipos diferentes de risco geralmente como um dispositivo de pontuação para classificar os riscos de acordo com o nível de risco. Isto pode ser utilizado para determinar quais riscos necessitam de avaliação mais aprofundada e possivelmente quantitativa.

B.28.3 Entradas

As entradas são derivadas da análise do sistema ou de uma ampla descrição do contexto. Isto requer uma boa compreensão de todas as fontes de risco, os caminhos possíveis e o que pode ser afetado. Ferramentas como análise de árvore de falhas, análise de árvore de eventos e análise de decisão geral podem ser utilizadas para apoiar o desenvolvimento de índices de risco.

Uma vez que a escolha de escalas ordinais é, em certa medida, arbitrária, dados suficientes são necessários para validar o índice.

B.28.4 Processo

O primeiro passo é entender e descrever o sistema. Uma vez que o sistema tenha sido definido, pontuações são desenvolvidas para cada componente de tal forma que possam ser combinadas para fornecer um índice composto. Por exemplo, em um contexto ambiental, as fontes, caminho e receptor(es) serão pontuados, observando que em alguns casos pode haver múltiplos caminhos e

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

receptores para cada fonte. As pontuações individuais são combinadas de acordo com um esquema que leve em consideração as realidades físicas do sistema. É importante que as pontuações para cada parte do sistema (fontes, caminhos e receptores) sejam consistentes internamente e mantenham suas relações corretas. As pontuações podem ser dadas para componentes de risco (por exemplo, probabilidade, exposição, consequência) ou para fatores que aumentam o risco.

As pontuações podem ser adicionadas, subtraídas, multiplicadas e/ou divididas de acordo com este modelo de alto nível. Os efeitos acumulados podem ser levados em consideração, adicionando pontuações (por exemplo, adicionando pontuações para caminhos diferentes). Não é admitido de forma alguma aplicar fórmulas matemáticas para escalas ordinais. Portanto, uma vez que o sistema de pontuação tenha sido desenvolvido, convém que o modelo seja validado aplicando-o a um sistema conhecido. O desenvolvimento de um índice é uma abordagem iterativa, e vários sistemas diferentes para combinar as pontuações podem ser tentados antes que o analista esteja confortável com a validação.

A incerteza pode ser tratada por meio da análise de sensibilidade e variando as pontuações para descobrir quais parâmetros são os mais sensíveis.

B.28.5 Saídas

As saídas são uma série de números (índices compostos) que se relacionam com uma fonte específica e que podem ser comparados com índices desenvolvidos para outras fontes dentro do mesmo sistema ou que podem ser modelados da mesma maneira.

B.28.6 Pontos fortes e limitações

Pontos fortes:

- os índices podem fornecer uma boa ferramenta para classificar diferentes riscos;
- eles permitem que múltiplos fatores que afetam o nível de risco sejam incorporados em uma única pontuação numérica para o nível de risco.

Limitações:

- se o processo (modelo) e sua saída não forem bem validados, os resultados podem ser sem sentido. O fato de que a saída é um valor numérico para o risco pode ser mal interpretado e mal utilizado, por exemplo, em análise subsequente de custo/benefício;
- em muitas situações onde os índices são utilizados, não existe um modelo fundamental para definir se as escalas individuais para os fatores de risco são lineares, logarítmicas ou com alguma outra forma, e nenhum modelo para definir como fatores devem ser combinados. Nessas situações, a avaliação é inerentemente não confiável e a validação contra dados reais é particularmente importante.

B.29 Matriz de probabilidade/consequência

B.29.1 Visão geral

A matriz de probabilidade/consequência é um meio de combinar classificações qualitativas ou semi-quantitativas de consequências e probabilidades, a fim de produzir um nível de risco ou classificação de risco.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

O formato da matriz e as definições a ela aplicadas dependem do contexto em que é utilizada e é importante que um projeto apropriado seja utilizado para as circunstâncias.

B.29.2 Utilização

Uma matriz de probabilidade/consequência é utilizada para classificar os riscos, fontes de risco ou tratamentos de risco com base no nível de risco. É comumente utilizada como uma ferramenta de seleção, quando muitos riscos foram identificados, por exemplo, para definir quais riscos necessitam de análise adicional ou mais detalhada, quais riscos necessitam primeiro de tratamento, ou quais riscos necessitam ser referidos a um nível mais alto de gestão. Também pode ser utilizada para selecionar quais riscos não precisam de maior consideração neste momento. Este tipo de matriz de risco é também amplamente utilizado para determinar se um dado risco é de uma forma geral aceitável ou não aceitável (ver 5.4), de acordo com a sua localização na matriz.

A matriz de probabilidade/consequência também pode ser utilizada para auxiliar a comunicação de uma compreensão comum dos níveis qualitativos dos riscos em toda a organização. Convém que a maneira como os níveis de risco são estabelecidos e as regras de decisão a eles atribuídos sejam alinhados com o apetite pelo risco da organização.

Uma forma de matriz de probabilidade/consequência é utilizada para análise de criticidade em FMECA ou para estabelecer prioridades após o HAZOP. Também pode ser utilizada em situações onde há dados insuficientes para uma análise detalhada ou a situação não assegura o tempo e esforço para uma análise mais quantitativa.

B.29.3 Entradas

As entradas do processo são escalas personalizadas de consequência e probabilidade e uma matriz que combina as duas.

Convém que a escala (ou escalas) de consequência abranja(m) toda a faixa dos diferentes tipos de consequência a serem considerados (por exemplo, perda financeira, segurança, meio ambiente ou outros parâmetros, dependendo do contexto), bem como se estenda da consequência máxima credível até a consequência de menor grau de preocupação. Um exemplo parcial é mostrado na Figura B.13.

A escala pode ter qualquer número de pontos. As escalas de 3, 4 ou 5 pontos são as mais comuns.

A escala de probabilidade também pode ter qualquer número de pontos. As definições para probabilidade precisam ser selecionadas para serem o menos ambíguas possíveis. Se guias numéricos forem utilizados para definir diferentes probabilidades, então as unidades devem ser dadas. A escala de probabilidade precisa abranger a faixa pertinente ao estudo em mãos, lembrando que a probabilidade mais baixa deve ser aceitável para a consequência mais alta definida; caso contrário, todas as atividades com a consequência mais alta são definidas como intoleráveis. Um exemplo parcial é mostrado na Figura B.14.

Uma matriz é desenhada com a consequência em um eixo e a probabilidade no outro. A Figura B.15 mostra parte de uma matriz de exemplo com uma escala de consequência de 6 pontos e de probabilidade de 5 pontos.

Os níveis de risco atribuídos às células dependerão das definições para as escalas de probabilidade/consequência. A matriz pode ser estabelecida para dar ponderação extra às consequências (conforme mostrado) ou às probabilidades, ou pode ser simétrica, dependendo da aplicação. Os níveis de risco podem estar associados a regras decisórias, como o nível de atenção da gestão ou a escala do tempo pela qual uma resposta é necessária.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$300 + loss or gain	• Multiple fatalities, or • Significant irreversible effects to 10's of people	• Irreversible long term environmental harm. • Community outrage- potential large-scale class action.	• International press reporting over several days. • Total loss of shareholder support who act to dis-invest. • CEO departs and board is restructured.	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$30m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact. • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for gro	• Major litigation costing $10m+ • Investigation by regulator body resulting in lo Interruption to
4	$1m – $9m loss or gain	$3m – $29m loss or gain	• Extensive injuries or Irevers	• Major spi		
3	$100k – $900 loss or gain					
2	$10k lo					
1						

Figura B.13 – Exemplo de parte de uma tabela critérios de consequência

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distinct - could occur within "mor
Unlikely	- may occur but not c - could occur in "y
Rare	- occurrence re - exceptional - only occ
Remote	- theor - fr

Figura B.14 – Exemplo de parte de uma matriz de classificação de riscos

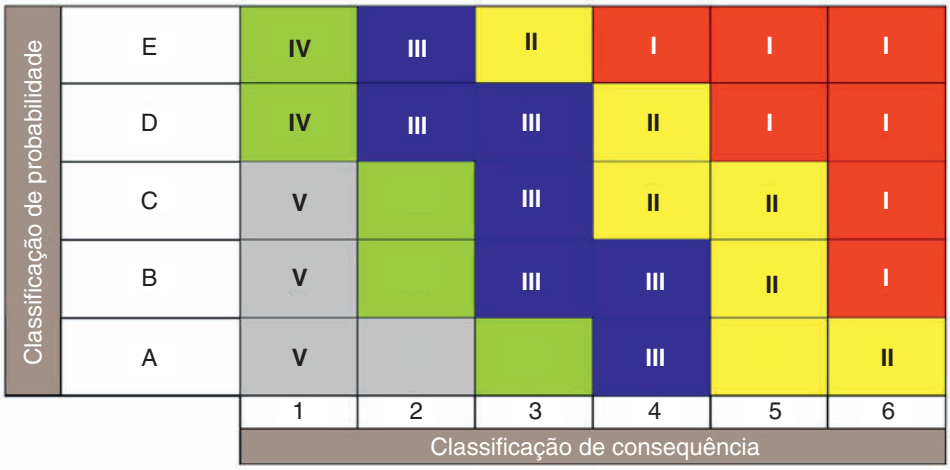

Figura B.15 – Exemplo de parte de uma matriz de critérios de probabilidade

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

As escalas de classificação e uma matriz podem ser estabelecidas com escalas quantitativas. Por exemplo, em um contexto de confiabilidade, a escala de probabilidade poderia representar taxas de falha indicativas e a escala de consequência, o custo monetário da falha.

A utilização da ferramenta necessita de pessoas (idealmente uma equipe) com especialização pertinente e dados disponíveis para auxiliar nos julgamentos de consequência e probabilidade.

B.29.4 Processo

Para classificar os riscos, o usuário primeiro encontra o descritor da consequência que melhor se adapta à situação e em seguida define a probabilidade com a qual essas consequências ocorrerão. O nível de risco é então estabelecido em função da matriz.

Muitos eventos de risco podem ter uma faixa de resultados com diferente probabilidade associada. Normalmente, os menores problemas são mais comuns do que as catástrofes. Portanto, há uma escolha em se classificar os resultados mais comuns, ou a combinação mais grave ou alguma outra combinação. Em muitos casos, é apropriado focar nos resultados confiáveis mais graves já que estes representam a maior ameaça e são muitas vezes os mais preocupantes. Em alguns casos pode ser apropriado classificar os problemas comuns e as catástrofes improváveis como riscos separados. É importante que a probabilidade pertinente para a consequência selecionada seja utilizada e não a probabilidade do evento como um todo.

O nível de risco definido pela matriz pode estar associado a uma regra de decisão, como tratar ou não tratar o risco.

B.29.5 Saídas

As saídas são uma classificação para cada risco ou uma lista classificada de riscos com níveis de significância definidos.

B.29.6 Pontos fortes e limitações

Pontos fortes:

- relativamente fácil de usar;
- fornece uma rápida classificação dos riscos em diferentes níveis de significância.

Limitações:

- uma matriz deve ser projetada para ser apropriada às circunstâncias de forma que pode ser difícil ter um sistema comum aplicável a uma faixa de circunstâncias pertinentes para uma organização;
- é difícil definir as escalas de forma não ambígua;
- a utilização é muito subjetiva e tende a haver uma variação significativa entre os classificadores;
- os riscos não podem ser agregados (ou seja, não se pode definir que um número específico de baixos riscos ou um baixo risco identificado um número específico de vezes seja equivalente a um risco médio);
- é difícil de combinar ou comparar o nível de risco para diferentes categorias de consequências.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Os resultados dependerão do nível de detalhes da análise, ou seja, quanto mais detalhada a análise, maior o número de cenários, cada um com probabilidade mais baixa. Isto subestimará o nível real de risco. A forma em que os cenários são agrupados na descrição do risco deve ser consistente e definida no início do estudo.

B.30 Análise de custo/benefício (ACB)

B.30.1 Visão geral

A análise de custo/benefício pode ser utilizada para avaliação de riscos quando os custos totais esperados são ponderados contra os benefícios totais esperados a fim de escolher a melhor ou a mais rentável opção. É uma parte implícita de muitos sistemas de avaliação de riscos. Ela pode ser qualitativa ou quantitativa, ou envolver uma combinação de elementos quantitativos e qualitativos. A ACB quantitativa agrega o valor monetário de todos os custos e todos os benefícios para todas as partes interessadas que estão incluídas no escopo e faz o ajuste para os diferentes períodos de tempo nos quais os custos e benefícios ocorrem. O valor presente líquido (VPL) calculado torna-se uma entrada nas decisões sobre o risco. Um VPL positivo associado a uma ação normalmente significaria que a ação deve ocorrer. Entretanto, para alguns riscos negativos, particularmente aqueles riscos que envolvem a vida humana ou danos ao meio ambiente, o princípio do ALARP pode ser aplicado. Isto divide os riscos em três regiões: um nível acima do qual os riscos negativos são intoleráveis e não devem ser aceitos, exceto em circunstâncias extraordinárias; um nível abaixo do qual os riscos são insignificantes e precisam somente ser monitorados para assegurar que eles permanecem baixos, e uma faixa central onde os riscos são mantidos tão baixos quanto razoavelmente praticável (ALARP). Em direção ao menor risco desta região, uma análise rigorosa de custo/benefício pode aplicar-se, porém quando os riscos estiverem próximos ao intolerável, a expectativa do princípio do ALARP é que o tratamento ocorrerá, a menos que os custos de tratamento sejam substancialmente desproporcionais em relação ao benefício obtido.

B.30.2 Utilização

A análise de custo/benefício pode ser utilizada para decidir entre opções que envolvam risco.

Por exemplo

- como entrada em uma decisão sobre se convém tratar um risco,
- para diferenciar e decidir entre a melhor forma de tratamento do risco,
- para decidir entre diferentes linhas de ação.

B.30.3 Entradas

As entradas incluem informações sobre custos e benefícios para as partes interessadas pertinentes e sobre incertezas nesses custos e benefícios. Convém que os custos e benefícios tangíveis e intangíveis sejam considerados. Os custos incluem recursos gastos e resultados negativos, os benefícios incluem resultados positivos, resultados negativos evitados e recursos economizados.

B.30.4 Processo

As partes interessadas que podem estar sujeitas aos custos ou receber benefícios são identificadas. Em uma análise completa de custo/benefício, todas as partes interessadas são incluídas.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Os benefícios e custos diretos e indiretos para todas as partes interessadas pertinentes das opções consideradas são identificados. Os benefícios diretos são aqueles que decorrem diretamente da ação tomada, enquanto os benefícios indiretos ou auxiliares são aqueles que são fortuitos, porém ainda podem contribuir significativamente para a decisão. Exemplos de benefícios indiretos incluem a melhoria de reputação, satisfação do pessoal e "paz de espírito". (Estes são muitas vezes fortemente considerados na tomada de decisões).

Os custos diretos são aqueles que estão diretamente associados com a ação. Os custos indiretos são aqueles custos adicionais, auxiliares e irrecuperáveis, como a perda de utilidade, desvio de atenção do tempo de gestão ou o desvio de capital em detrimento de outros investimentos potenciais. Ao aplicar uma análise de custo/benefício a uma decisão para se tratar de um risco, convém que sejam incluídos os custos e benefícios associados ao tratamento do risco e à assunção do risco.

Na análise quantitativa de custo/benefício, quando todos os custos e benefícios tangíveis e intangíveis forem identificados, um valor monetário é atribuído a todos os custos e benefícios (inclusive custos e benefícios intangíveis). Existem inúmeras formas padronizadas de fazer isto, incluindo a abordagem 'disposição a pagar' e utilizando substitutos. Se, como muitas vezes acontece, o custo incorrer durante um período curto de tempo (por exemplo, um ano) e o fluxo de benefícios por um longo período posteriormente, é normalmente necessário descontar os benefícios para trazê-los ao "dinheiro de hoje", de modo que uma comparação válida possa ser obtida. Todos os custos e benefícios são expressos como valor presente. O valor presente de todos os custos e benefícios para todas as partes interessadas pode ser combinado para produzir um valor presente líquido (VPL). Um VPL positivo significa que a ação é benéfica. Razões de custo/benefício são também utilizadas (ver B.30.5).

Se houver incerteza sobre o nível de custos ou benefícios, um ou ambos os termos podem ser ponderados de acordo com as suas probabilidades.

Na análise qualitativa de custo/benefício nenhuma tentativa é feita para encontrar um valor monetário para custos e benefícios intangíveis e, em vez de fornecer um único número que resuma os custos e benefícios, relações e concessões (*trade offs*) entre os diferentes custos e benefícios são consideradas qualitativamente.

Uma técnica relacionada é uma análise de custo-eficácia. Isso pressupõe que um certo benefício ou resultado é desejado, e que há diversas formas alternativas para atingi-lo. A análise olha somente os custos e qual é a forma mais barata de alcançar o benefício.

B.30.5 Saída

A saída de uma análise custo/benefício é a informação sobre os custos e benefícios de diferentes opções ou ações. Isto pode ser expresso quantitativamente como um valor presente líquido (VPL), um taxa interna de retorno (TIR) ou como a razão entre o valor presente dos benefícios e o valor presente dos custos. Qualitativamente as saídas são geralmente uma tabela que compara os custos e os benefícios dos diferentes tipos considerados, chamando a atenção para as concessões (*trade offs*).

B.30.6 Pontos fortes e limitações

Pontos fortes da análise de custo/benefício:

- permite que os custos e benefícios sejam comparados usando uma métrica única (monetária);
- fornece transparência na tomada de decisões;
- requer informações detalhadas a serem coletadas em todos os aspectos possíveis da decisão. Isto pode ser valioso para revelar a ignorância, bem como comunicar o conhecimento.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Limitações:

- A ACB quantitativa pode gerar números dramaticamente diferentes, dependendo dos métodos utilizados para atribuir valores econômicos a benefícios não econômicos;
- em algumas aplicações é difícil definir uma taxa de desconto válida para custos e benefícios futuros;
- os benefícios que alcançam uma grande população são difíceis de estimar, particularmente aqueles relativos ao bem público que não é transacionado em mercados;
- a prática do desconto (atualização dos valores com taxas de desconto) significa que os benefícios obtidos no futuro a longo prazo têm influência insignificante na decisão, dependendo da taxa de desconto escolhida. O método torna-se inadequado para consideração dos riscos que afetam as gerações futuras, a menos que taxas de desconto muito baixas ou nulas sejam estabelecidas.

B.31 Análise de decisão por multicritérios (MCDA)

B.31.1 Visão geral

O objetivo é utilizar uma faixa de critérios para avaliar de forma objetiva e transparente o valor global de um conjunto de opções. Em geral, o objetivo global é produzir uma ordem de preferência entre as opções disponíveis. A análise envolve o desenvolvimento de uma matriz de opções e critérios que são classificados e agregados para fornecer uma pontuação global para cada opção.

B.31.2 Utilização

A MCDA pode ser utilizada para

- comparar múltiplas opções para uma primeira análise para determinar opções preferenciais e potenciais e as inapropriadas,
- comparar opções onde existam critérios múltiplos e, algumas vezes, conflitantes,
- alcançar um consenso sobre uma decisão onde diferentes partes interessadas têm objetivos ou valores conflitantes.

B.31.3 Entradas

Um conjunto de opções para análise. Critérios baseados em objetivos que podem ser utilizados igualmente em todas as opções para diferenciá-las.

B.31.4 Processo

Em geral, um grupo de partes interessadas conhecedoras realizam o seguinte processo:

a) definem o(s) objetivo(s);

b) determinam os atributos (critérios ou medidas de desempenho) que se relacionam a cada objetivo;

c) estruturam os atributos dentro de uma hierarquia;

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

d) desenvolvem opções para serem avaliadas em relação aos critérios;

e) determinam a importância dos critérios e atribuem ponderações correspondentes a eles;

f) avaliam as alternativas com relação aos critérios. Isto pode ser representado como uma matriz de pontuações.

g) combinam múltiplas pontuações de atributo único em uma única pontuação multiatributo agregada;

h) avaliam os resultados.

Existem diferentes métodos pelos quais a ponderação para cada critério pode ser deduzida e diferentes formas de agregar as pontuações dos critérios para cada opção em uma pontuação única de multiatributos. Por exemplo, as pontuações podem ser agregadas como uma soma ponderada ou um produto ponderado, ou utilizando o método analítico hierárquico, uma técnica de dedução para as ponderações e pontuações baseada em comparações par a par – emparelhadas). Todos estes métodos assumem que a preferência por qualquer critério não depende dos valores dos outros critérios. Caso esta premissa não seja válida, diferentes modelos são utilizados.

Uma vez que as pontuações são subjetivas, a análise de sensibilidade é útil para examinar a extensão em que as ponderações e pontuações influenciam as preferências globais entre as opções.

B.31.5 Saída

A apresentação da ordem de classificação das opções vai da melhor para a menos preferida. Se o processo produzir uma matriz onde os eixos da matriz são os critérios ponderados e a pontuação dos critérios para cada opção, então as opções que falham nos critérios altamente ponderados também podem ser eliminadas.

B.31.6 Pontos fortes e limitações

Pontos fortes:

- fornece uma estrutura simples para uma tomada de decisão eficaz e apresentação de premissas e conclusões;
- pode tornar mais gerenciáveis os problemas de decisão complexos, que não são passíveis de análise de custo/benefício;
- pode auxiliar a considerar racionalmente os problemas onde concessões (*trade offs*) precisam ser efetuadas;
- pode auxiliar a atingir um acordo quando as partes interessadas têm objetivos e, consequentemente, critérios diferentes.

Limitações:

- pode ser afetada por viés e por má seleção dos critérios de decisão;
- a maioria dos problemas da MCDA não tem uma solução conclusiva ou única;
- algoritmos de agregação que calculam os critérios de ponderação a partir de preferências estabelecidas ou agregam diferentes pontos de vista podem obscurecer a verdadeira base da decisão.

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS

Bibliografia

[1] IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

[2] IEC 61508 (All parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[3] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

[4] ABNT NBR ISO 22000, *Sistemas de gestão da segurança de alimentos – Requisitos para qualquer organização na cadeia produtiva de alimentos*

[5] ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

[6] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

[7] IEC 61649, *Weibull analysis*

[8] IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[9] IEC 61165, *Application of Markov techniques*

[10] ISO/IEC 15909 (All parts), *Software and systems engineering – High-level Petri nets*

[11] IEC 62551, *Analysis techniques for dependability – Petri net techniques* [2]

[2] Atualmente em estudo.

© ISO/IEC 2009 - © ABNT 2012 - Todos os direitos reservados

Documento impresso em 03/04/2019 15:37:45, de uso exclusivo de UNIVERSIDADE FEDERAL DE PELOTAS