



Universidade Federal do Rio de Janeiro
Escola Politécnica & Escola de Química
Programa de Engenharia Ambiental

Marcela Mayo Pires

GESTÃO DA INTEGRIDADE DE BARREIRAS: FATOR CHAVE NA PREVENÇÃO DE
ACIDENTES

Rio de Janeiro
2012



UFRJ

Marcela Mayo Pires

GESTÃO DA INTEGRIDADE DE BARREIRAS: FATOR CHAVE NA PREVENÇÃO DE
ACIDENTES

Dissertação de Mestrado apresentada ao Programa de Engenharia Ambiental, Escola Politécnica & Escola de Química, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia Ambiental.

Orientador: Assed Naked Haddad, Prof. D.Sc.

Rio de Janeiro
2012

Pires, Marcela Mayo.

Gestão da Integridade de Barreiras: Fator Chave na
Prevenção de Acidentes / Marcela Mayo Pires. – 2012.
101 f.: il.

Dissertação (mestrado) – Universidade Federal do Rio de
Janeiro, Escola Politécnica e Escola de Química, Programa de
Engenharia Ambiental, Rio de Janeiro, 2012.

Orientador: Assed Naked Haddad

1. Segurança de Processo. 2. Gestão de Barreiras. 3.
Prevenção de acidentes. I. Haddad, Assed Naked. II.
Universidade Federal do Rio de Janeiro. Escola Politécnica e
Escola de Química. III. Mestrado.



UFRJ

GESTÃO DA INTEGRIDADE DE BARREIRAS: FATOR CHAVE NA PREVENÇÃO DE
ACIDENTES

Marcela Mayo Pires

Dissertação de Mestrado apresentada ao Programa de Engenharia Ambiental, Escola Politécnica & Escola de Química, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia Ambiental.

Orientador: Assed Naked Haddad, Prof. D.Sc.

Aprovada pela Banca:

Presidente, Prof. Assed Naked Haddad, D.Sc, UFRJ

Rio de Janeiro
2012

*Dedico essa dissertação à minha família que amo e
que com eles a vida faz todo sentido .*

AGRADECIMENTOS

Agradeço a Deus pelo amor incondicional e por estar sempre presente na minha vida;

Ao meu pai Nelson, minha mãe Neli e meus irmãos Juliana e Vinícius pelo amor, dedicação e o incentivo que recebo ao longo de minha vida;

Ao meu marido Vinícius Capillé, obrigada pelo seu amor, companheirismo e incentivo;

Aos meus amigos e irmãos de coração, Uara Sarmenghi e Marcello Tardelli, sem vocês meu mundo não seria tão completo;

Aos meus gerentes Mariana Bardy e Tobias Alvarenga, obrigada pela paciência, atenção e palavras de incentivo, sem vocês não teria conseguido;

À minha amiga Paula Dias, obrigada por nossas conversas e por sempre me orientar, tanto na vida pessoal quanto na profissional.

Aos meus amigos do PEA: Henri, Gustavo, Thomas, João e Manuel. Meus dias no Fundão se tornaram bem mais agradáveis e divertidas com a presença de vocês.

Ao meu orientador Assed, pelo incentivo na conclusão da dissertação.

"You get what you inspect, not what you expect."

Desconhecido

RESUMO

Pires, Marcela. Gestão da Integridade de Barreiras: Fator Chave na Prevenção de Acidentes. Rio de Janeiro, 2012. Dissertação (Mestrado) – Programa de Engenharia Ambiental, Escola Politécnica e Escola de Química, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2012.

Com os acidentes que ocorreram nos últimos anos, fica notório que a segurança de processo é ainda um assunto sério e preocupante e que ainda há muito a ser feito. Esses acidentes na indústria de processo demonstraram e intensificaram a importância das barreiras de segurança na prevenção de acidentes ou na redução dos seus efeitos.

Gerenciar as barreiras de segurança dos maiores cenários da planta é crucial e pode representar a diferença entre um dano e uma catástrofe, sendo assim um fator essencial para a prevenção de acidentes.

Esta dissertação visa apresentar um roteiro para identificação e verificação do status das barreiras de segurança de processo, uma vez que este elemento oferece contribuição significativa na prevenção de acidentes. Adicionalmente apresenta sugestões baseadas em boas práticas para a melhor condução e análise da integridade das barreiras de segurança. Itens como integridade de ativos, cultura de segurança, gerenciamento de riscos e de mudanças serão abordados a fim de evidenciá-los como grandes aliados à efetividade das barreiras de segurança para as instalações em operação. Alguns acidentes, como o DeepWater Horizon, apresentados no capítulo 3, ilustram e reforçam que o tema abordado e os itens expostos acima são importantes e essenciais na prevenção de acidentes.

Palavras-chave: 1. Segurança de Processo. 2. Gestão de Barreiras. 3. Prevenção de acidentes.

ABSTRACT

Pires, Marcela. Gestão da Integridade de Barreiras: Fator Chave na Prevenção de Acidentes. Rio de Janeiro, 2012. Dissertação (Mestrado) – Programa de Engenharia Ambiental, Escola Politécnica e Escola de Química, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2012.

With accidents that have occurred in recent years, it became clear that the security process is still a serious and concern issue and has much remains to be done. These accidents in process industry have been demonstrated the importance of safety barriers to prevent accidents or reduce their effects.

Manage the safety barriers of the plant major scenarios is crucial and may represent the difference between an injury and a catastrophe, and therefore is a key factor in accident prevention.

This thesis aims to present a guide for identification and verification of the process safety barriers status, since this element provides significant contribution to accident prevention. Additionally presents suggestions based on best practices for conducting and analyzing the integrity of the safety barriers. Items such as asset integrity, safety culture, risk management and managing change will be addressed in order to evidence them as great allies to the effectiveness of safety barriers for facilities in operation. Some accidents such as the Deepwater Horizon, presented in Chapter 3, illustrate and reinforce the theme and discussed the items above are important and essential in preventing accidents.

Kew-words: 1. Process Safety 2.Barriers Management. 3. Accident Prevention.

LISTA DE ILUSTRAÇÕES

Figura 2-1– Constituintes de um acidente (Fonte: adaptado Hollnagel, 2004).....	20
Figura 2-2– Falta da indicação da falha (Fonte: Hollnagel, 2004)	21
Figura 2-3– Modelo sequencial do acidente (Fonte: adaptado Hollnagel, 2002)	22
Figura 2-4– Teoria do dominó - depois de Heinrich, 1931 (Fonte: adaptado Hollnagel, 2002)	23
Figura 2-5– Modelo epidemiológico (Fonte: adaptado Hollnagel, 2002)	24
Figura 2-6– Teoria do queijo suíço, Reason 1990 (Fonte: Hollnagel, 2006)	25
Figura 2-7– Modelo sistêmico de acidente (Fonte: adaptado Hollnagel, 2002).....	26
Figura 2-8– Relações entre o blunt-end e o sharp-end que levam a falha (Fonte: adaptado Hollnagel, 2002)	26
Figura 2-9– Modelo de Reason, 1990 (Fonte: Oliveira, 2008).....	34
Figura 2-10– Níveis de controle das Ações (Fonte: Oliveira, 2008)	36
Figura 2-11– Níveis de controle das ações relacionados com modelo de Reason (Fonte: Oliveira, 2008).....	37
Figura 2-12– Prevenção e Proteção (Fonte: adaptado Hollnagel, 2002)	39
Figura 2-13– Método PDCA (Fonte: Falconi, 2002)	48
Figura 2-14– Exemplo de bow-tie.....	50
Figura 3-1– Relação das barreiras com os fatores críticos (Fonte: BP, 2010).	53
Figura 3-2– Acidente da Deepwater Horizon (Fonte: site BP, 2010).....	54
Figura 3-3–Plataforma P-36 (Fonte: ANP, 2001).	56
Figura 3-4– Esquemático do processo de drenagem de emergência da P-36 (Fonte: Aiche, 2008).	57
Figura 3-5– Acidente da Plataforma P-36 (Fonte: ANP, 2001).....	59

Figura 3-6– Acidente na Refinaria Tosco (Fonte: site CBS).....	60
Figura 3-7– Acidente de Flixborough (Fonte: AICHE, 2012).....	63
Figura 4-1– Planilha APP (Fonte: Adaptado AICHE, 2008)	68
Figura 4-2– Exemplo de itens a serem avaliados em sistemas instrumentados de segurança.....	76
Figura 4-3– Representação de Criticidade e Integridade no diagrama de bow-tie (Fonte: Bardy et al, 2012b).....	78
Figura 4-4– Bow-tie para o cenário de liberação de gás inflamável.....	79
Figura 5-1– Importância das funções instrumentadas de segurança (Fonte: IEC61511-3, 2003).....	87
Figura 5-2– Fatores fundamentais para obtenção de resultados (Fonte: Falconi, 2010).....	92

LISTA DE QUADROS

Quadro 2-1 – Cultura Fraca x Cultura Sólida (Fonte: AICHE, 2007)	32
Quadro 2-2 – Erro Humano (Oliveira, 2008)	34
Quadro 2-3 – Relação entre SIL, PFD e FRR (Fonte: IEC 61508, 2010)	44
Quadro 2-4 – Exemplos de IPLs Ativas (Fonte: AICHE, 2001)	46
Quadro 2-5 – Exemplos de IPLs Passivas (Fonte: AICHE, 2001)	46
Quadro 2-6 Salvaguardas que geralmente não são consideradas IPL (Fonte: AICHE, 2001)	46
Quadro 2-7 – Descrição dos campos do bow-tie	50
Quadro 4-1 – Descrição categoria de frequência (Fonte: Haddad e Morgado, 2002)	69
Quadro 4-2 – Descrição categoria de severidade (Fonte: Haddad e Morgado, 2002)	70
Quadro 4-3 – Matriz de Risco (Fonte: Haddad e Morgado, 2002)	71
Quadro 4-4 – Áreas responsáveis pela gestão das barreiras	74

SUMÁRIO

1	INTRODUÇÃO	15
1.1	APRESENTAÇÃO DO TEMA	15
1.2	OBJETIVO	15
1.3	APRESENTAÇÃO DO PROBLEMA	15
1.4	JUSTIFICATIVA DO TEMA	18
1.5	METODOLOGIA	19
1.6	LIMITAÇÕES DO TRABALHO.....	19
2	REFERENCIAL TEÓRICO.....	20
2.1	ACIDENTES E CAUSAS	20
2.2	MODELOS DE ACIDENTE	21
2.2.1	Modelo Sequencial	22
2.2.2	Modelo Epidemiológico.....	23
2.2.3	Modelo Sistêmico	25
2.3	PREVENÇÃO DE ACIDENTES.....	27
2.4	CULTURA DE SEGURANÇA	29
2.5	O FATOR HUMANO	33
2.6	BARREIRAS DE SEGURANÇA.....	38
2.6.1	Qualidade e Desempenho das Barreiras de Segurança.....	41
2.6.2	Nível de Confiabilidade das Barreiras de Segurança	43
2.7	SISTEMA DE GESTÃO	47
2.8	AUDITORIA	48
2.9	BOW-TIE	49
3	ACIDENTES QUE DEFINIRAM E DEFINEM A SEGURANÇA DE PROCESSO..	51
3.1	DEEPWATER HORIZON (ESTADOS UNIDOS, 2010)	51
3.1.1	Descrição do acidente	52
3.1.2	Principais fatores para a ocorrência do acidente	54
3.2	PLATAFORMA P-36 DA PETROBRAS (BRASIL, 2001)	56
3.2.1	Descrição do acidente	56
3.2.2	Principais fatores para a ocorrência do acidente	58
3.3	REFINARIA TOSCO (ESTADOS UNIDOS, 1999).....	59
3.3.1	Descrição do acidente	60
3.3.2	Principais fatores para a ocorrência do acidente	61

3.4 FLIXBOROUGH (REINO UNIDO, 1974).....	62
3.4.1 Descrição do acidente	62
3.4.2 Principais fatores para a ocorrência do acidente	63
4 ROTEIRO E CRITÉRIOS PARA UMA BOA GESTÃO DAS BARREIRAS EXISTENTES.....	65
4.1 IDENTIFICAÇÃO DOS CENÁRIOS.....	65
4.1.1 Análise Preliminar de Perigos.....	67
4.1.2 Seleção dos cenários	71
4.2 IDENTIFICAÇÃO DAS BARREIRAS DE SEGURANÇA PARA CADA CENÁRIO SELECIONADO	72
4.3 VERIFICAÇÃO DA INTEGRIDADE DAS BARREIRAS DE SEGURANÇA IDENTIFICADAS PELO PROCESSO DE AUDITORIA.....	72
4.3.1 Protocolos.....	75
4.3.2 Verificação da criticidade das barreiras de segurança identificadas	76
4.4 BOW-TIE	77
4.5 TRATAMENTO DE NÃO CONFORMIDADES.....	79
5 BOAS PRÁTICAS PARA GESTÃO DAS BARREIRAS DE SEGURANÇA	81
5.1 AUDITORIA	81
5.1.1 Pré-auditoria	82
5.1.2 Durante auditoria	82
5.1.3 Resultados da auditoria	82
5.2 INTEGRIDADE DOS ATIVOS.....	84
5.2.1 Manutenção Preventiva e Plano de Inspeção	84
5.2.2 Gerenciamento de Alarmes	85
5.2.3 Sistemas Instrumentados de Segurança	86
5.3 GERENCIAMENTO DOS RISCOS E DE MUDANÇAS	88
5.3.1 Plano de Ação de Emergência	89
5.3.2 Bow-tie.....	90
5.4 CULTURA DE SEGURANÇA	90
5.4.1 Treinamento	93
5.4.2 Procedimentos.....	93
6 CONCLUSÃO	95
7 REFERÊNCIAS BIBLIOGRÁFICAS.....	97

1 INTRODUÇÃO

1.1 APRESENTAÇÃO DO TEMA

Tema: Gestão da Integridade de Barreiras: Fator Chave na Prevenção de Acidentes.

Delimitação do Tema: Apresentar diretrizes para uma boa gestão das barreiras de segurança na indústria química e petroquímica para instalações em operação.

1.2 OBJETIVO

Esta dissertação tem como objetivo apresentar diretrizes para que a realidade de um empreendimento esteja mais próxima dos estudos de análise de riscos realizados para o mesmo em termos de suas barreiras de segurança. Esta foca em apresentar diretrizes para uma boa gestão das barreiras de segurança de processo a fim de prevenir e mitigar impactos de eventos indesejáveis.

1.3 APRESENTAÇÃO DO PROBLEMA

O avanço tecnológico conduz o crescimento industrial em todo mundo. Este crescimento é favorável para a economia local/mundial, porém o manuseio de produtos perigosos pode acarretar em significativos danos para os trabalhadores do local, população externa e para o meio ambiente.

Até a década de 70, a questão da segurança na indústria era somente tratada no âmbito da mesma, sem interferências do governo e da população. Poucas ações de segurança (de prevenção ou mitigação) eram implementadas para prevenir desvios de variáveis de processo, bem como mitigar possíveis efeitos de suas ocorrências.

Desde então, apesar da crescente intervenção do estado com a definição de regulações específicas e controles periódicos, os grandes acidentes ocorridos demonstraram que não somente os desvios de processo em uma indústria acontecem como também podem levar a sérios danos com relevantes perdas materiais e com expressivo número de feridos e vítimas fatais (Vieira, 2001).

Com isso, conforme exposto no site da Companhia Ambiental do Estado de São Paulo (CETESB), as técnicas e métodos já amplamente utilizados nas indústrias

bélica, aeronáutica e nuclear passaram a ser adaptados para a realização de estudos de análise e avaliação dos riscos associados a outras atividades industriais, em especial nas áreas de petróleo, química e petroquímica. A fim de evitar eventos que implicam em riscos graves para os trabalhadores e população no entorno do empreendimento, danos ambientais e perdas materiais, foram desenvolvidas/adaptadas diversas técnicas no sentido de conter ou minimizar os danos oriundos destas atividades. Visando avaliar e gerenciar os riscos das atividades na indústria química ou petroquímica se estabeleceu leis e regulamentos específicos para a operação das mesmas.

Com o objetivo de atender a legislação e fornecer uma maior segurança para seus funcionários, a indústria química iniciou a aplicação das técnicas de análise e gerenciamento de risco.

Segundo CETESB (2003), no Brasil, em particular em São Paulo, a preocupação com os acidentes de grande porte ganhou ênfase em 1984, após o rompimento de um duto de gasolina seguido de incêndio em Cubatão, causando cerca de 500 vítimas, das quais 93 fatais.

Além disto, com os acontecimentos dos últimos 10 anos, conforme exposto por Pitblado (2011), como a perda total da plataforma P-36 (2001) da Petrobras, a explosão de nitrato de amônia em Toulouse (2001), o desastre no duto da Bélgica (2004), Buncefield (2005), a explosão na refinaria de Texas City da BP (2005) entre outros, fica notório que a segurança de processo é ainda um assunto sério e preocupante e que ainda há muito a ser feito.

Pitblado (2011) aponta que estudos recentes realizados nos Estados Unidos e na Europa mostram que não há uma tendência de redução dos cenários acidentais, porém o banco de dados de grandes acidentes da União Européia apresentado pela MARS (*Major Accident Reporting System*) mostrou uma taxa estável no reporte dos eventos com uma taxa estável no nível de severidade.

Já nos Estados Unidos, analisando os dados dos últimos 10 anos do RMP-Star, a Escola de Negócios de Wharton, identificou pequenos avanços na segurança de processo.

Desta forma, há de se reconhecer que a segurança de processo já é um tema bem difundido junto aos trabalhadores e gestores da indústria em geral. A grande

questão é o quanto o conhecimento já adquirido pela indústria se materializa em redução significativa de incidentes e eventos catastróficos. O livro *Recognizing Catastrophic Incident Warning Signs in the Process Industries* do *Center for Chemical Process Safety* (AIChE, 2012), expõe que as organizações que compreendem a importância da segurança do processo refletirão essa consciência em suas ações. Para ser mais eficaz, segundo AIChE (2012), é necessário adotar a segurança de processo como um valor para toda a organização e mostrá-la em ações. Prioridades mudam com o ambiente de trabalho ou ambiente de negócios, já os valores não. Os valores são como algo que um grupo internaliza e caracteriza em seu comportamento para ajudar a definir suas ações.

Logo é de grande importância trabalhar em todos os elementos do sistema de gerenciamento de segurança de processo para a prevenção de acidentes.

Durante a fase de operação de um empreendimento, a avaliação de risco predominante é a qualitativa, que possui o foco voltado para identificação das barreiras críticas, além de definir responsáveis e verificar o nível de desempenho das barreiras de segurança.

E é exatamente neste quesito de segurança que este trabalho se concentrará. Na presente dissertação será abordada a gestão da integridade das barreiras de segurança como fator chave na prevenção de acidentes. Muitos sistemas que são apresentados como barreiras de segurança em estudos qualitativos e utilizados nos estudos quantitativos para a redução do risco nem sempre estão íntegros e quando demandados podem não desempenhar sua função ou desempenhá-la de forma ineficiente. Com isso, esse trabalho visa apresentar boas práticas para reduzir a distância entre o que está na teoria e o que é praticado no dia-a-dia de um empreendimento.

Devido ao fato citado anteriormente, o fator humano e conceitos sobre a cultura de segurança serão abordados a fim de reforçar que estes estão em plena sinergia com a efetividade das barreiras de segurança. Adicionalmente resultados da aplicação de programas de gestão de barreiras na indústria mostram o quanto ainda deve-se caminhar para alcançar a excelência na gestão de barreiras de segurança de processo.

A fim de suportar o tema proposto, no capítulo 2 serão apresentados fundamentos teóricos da gestão da segurança de processo envolvendo conceitos como o fator humano, a cultura de segurança, barreiras de segurança e de gestão.

Alguns acidentes que tiveram de suas causas relacionadas aos itens que serão abordados nesta dissertação, serão apresentados no capítulo 5.

No capítulo 4 será apresentada a gestão das barreiras de proteção como um fator para a prevenção de acidentes.

No capítulo 5, serão apresentados critérios para uma boa gestão das barreiras existentes.

Finalmente no capítulo 6 serão apresentadas as conclusões finais desta dissertação.

1.4 JUSTIFICATIVA DO TEMA

Os acidentes ocorridos nos últimos 10 anos alertam que segurança de processo é ainda um assunto sério e preocupante e que ainda há muito a ser feito.

Esses acidentes na indústria de processo demonstraram e intensificaram a importância das barreiras de segurança na prevenção de acidentes ou a redução dos seus efeitos (BARDY et al, 2012).

Segundo Pitblado (2011) enquanto na segurança ocupacional é observado um fator de 10 em avanços ao longo dos últimos 20 anos, na segurança de processo ainda a muito a se conquistar e um fator de 3 a 4 em avanços pode ser possível para os próximos 20 anos.

Aiche (2012) ressalta que sinais de alerta são um sutil indicador de um problema que pode levar a um acidente. Todo sinal fornece pistas que podem sinalizar preventivamente uma catástrofe. Essas pistas oferecem a oportunidade de se alterar a conduta, reduzindo assim o risco de um evento catastrófico.

De alguma maneira, operadores e supervisores desenvolveram a impressão que incidentes catastróficos somente acontecem em outras instalações e são resultados de uma má conduta ou colapso total do sistema. Uma organização ou instituição que durante anos se sustentou sem um acidente catastrófico, tem o sentimento que “nós devemos estar conduzindo as coisas de forma correta”. Porém, em muitos casos, esta percepção é equivocada.

Por esse motivo, a definição e o gerenciamento das barreiras de segurança de uma instalação é crucial e pode representar a diferença entre um dano e uma catástrofe.

1.5 METODOLOGIA

Com a análise da bibliografia aplicada, foram estudadas diferentes metodologias para a elaboração de roteiro para a realização da Gestão de Barreiras de Segurança existentes apresentado no capítulo 4.

As boas práticas apresentadas no capítulo 5 foram baseadas na experiência em campo durante a verificação da integridade das barreiras de segurança existentes em diversas instalações de empresas da área petroquímica e de óleo e gás e no livro do Aiche, *Recognizing Catastrophic Incident Warning Signs in the Process Industries*, 2012.

1.6 LIMITAÇÕES DO TRABALHO

Este trabalho não aborda a Gestão da Segurança de Processo como um todo, limitando-se em apresentar um subitem deste sistema, no caso, a gestão de barreiras de segurança.

Com relação à auditoria, o trabalho se limita a descrever as principais etapas da mesma, bem como chamar atenção para seus pontos críticos de sucesso. Não é detalhado o conteúdo dos protocolos ou mesmo apresentados documentos de apoio para sua realização.

O Sistema de Gestão de Barreiras de Segurança proposto busca abranger diferentes instituições, independente de seu tamanho ou atividade fim, entretanto sua aplicação conceitual é focada para indústrias petroquímicas e de óleo e gás, desta forma sua adequação a outra realidade carece de avaliação.

2 REFERENCIAL TEÓRICO

2.1 ACIDENTES E CAUSAS

Acidentes não são inevitáveis. Na prática é impossível prevenir todo acidente, porém é totalmente possível prevenir muitos e às vezes a sua maioria.

Quando algum acidente acontece, a primeira pergunta que se faz é o que aconteceu de errado e quais são as suas causas.

Segundo Hollnagel (2004), um acidente pode ser definido como um evento inesperado que resulta em um efeito indesejado.

Acidentes hoje em dia raramente acontecem somente devido a uma causa singular, mas sim por sucessivas falhas. Tais combinações são difíceis de prever e de prevenir, com isso, evidenciam a importância das proteções, ou seja, das suas barreiras de segurança. Uma barreira de segurança possui a função de prevenir ou minimizar as consequências de um evento. Logo, uma solução eficiente é desenvolver barreiras com ampla efetividade para diversas causas de potenciais acidentes. Conforme ilustrado na Figura 2-1, mesmo que não haja uma forma de impedir o evento de acontecer, ainda há a possibilidade de prevenir a ocorrência das consequências indesejadas. Prevenir um acidente de acontecer significa assegurar que o destinatário não sofrerá danos. O destinatário pode ser uma pessoa, a sociedade, um artefato tecnológico ou a combinação destes.

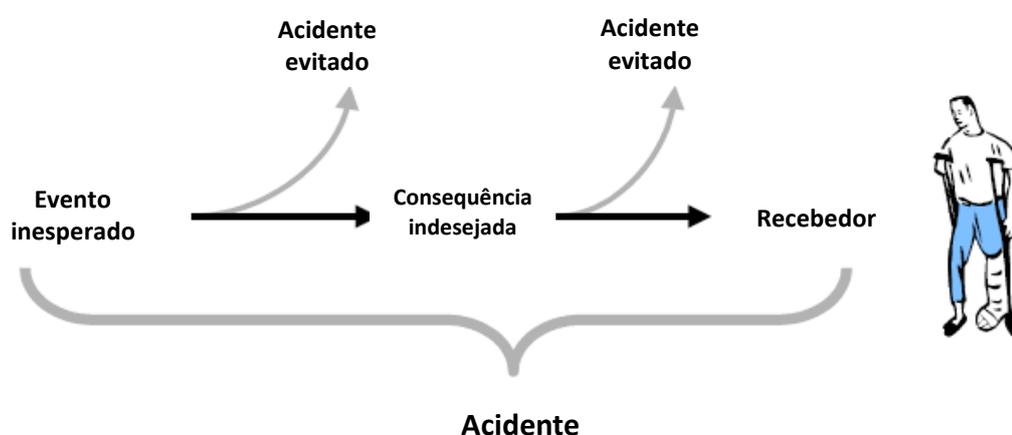


Figura 2-1– Constituintes de um acidente (Fonte: adaptado Hollnagel, 2004)

A ausência de um resultado indesejado, ou seja, a falta de indicação de uma falha pode ser tomada como indicação de que está tudo bem, o que nem sempre é verdade, conforme ilustrado na Figura 2-2. A falta de um resultado pode ser o resultado de várias condições ou fatores. Em muitos casos, a falta de uma indicação de uma falha pode ocorrer por uma condição encoberta, por vezes também referida como um estado latente (HOLLNAGEL, 2004). Esta questão será tratada em detalhes no próximo item, Modelos de Acidente.

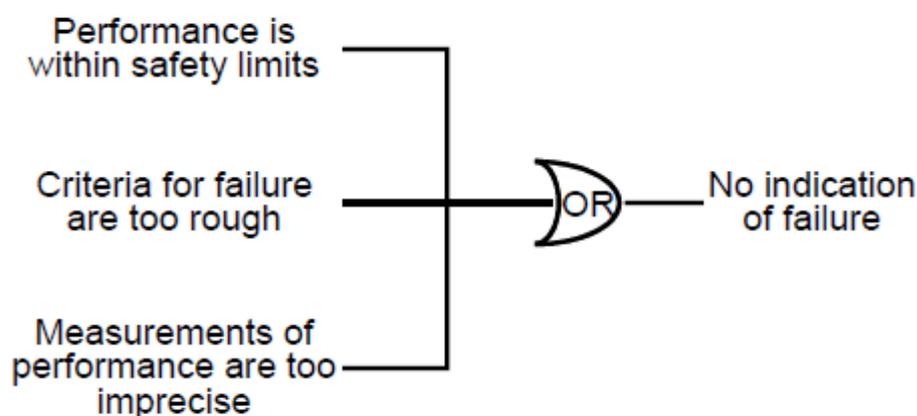


Figura 2-2– Falta da indicação da falha (Fonte: Hollnagel, 2004)

No capítulo 3, serão apresentados alguns acidentes que auxiliaram a definir a segurança de processo, como o acidente de Flixborough, e um dos acidentes mais recente de grandes proporções, o DeepWater Horizon, que representa o quanto ainda devemos aprender.

2.2 MODELOS DE ACIDENTE

A história da segurança é rica em teorias que tentam explicar a casualidade dos acidentes.

Hollnagel (2006) explicita que um sistema é seguro se este é impenetrável e resiliente a perturbações, adicionalmente, a identificação e avaliação dos possíveis riscos é um pré-requisito essencial para um sistema seguro. O autor reforça a teoria que acidentes e avaliação dos riscos são duas faces de uma mesma moeda, logo os dois estão limitados na mesma medida aos modelos e teorias, com isso é razoável assumir que desenvolvimentos no sistema de segurança são combinados com desenvolvimento na análise dos acidentes. Assim como é necessária a etiologia de acidentes, um estudo de possíveis causas ou origens dos acidentes, também o é

para a segurança – mais especificamente do que a segurança é e de como esta pode estar em perigo. No entanto, por razões que não são totalmente claras, tais desenvolvimentos tem faltado conforme já exposto por Pitblado (2011).

Algumas destas principais teorias serão expostas a seguir a fim de demonstrar a evolução do tema com o passar dos anos. Benner (1978) reconheceu o valor ou a necessidade de se obter um modelo de acidente quando observou que as dificuldades práticas surgem durante a investigação e na elaboração de relatórios da maioria dos acidentes. Estas dificuldades refletem diferenças na finalidade para as investigações, que por sua vez, refletem diferentes percepções do acidente.

As diferentes percepções de um acidente são o que hoje são chamados de modelos de acidentes segundo Hollnagel (2006).

Hollnagel (2004) explicita que três modelos de acidentes foram desenvolvidos: modelo sequencial, modelo epidemiológico e o modelo sistêmico.

2.2.1 Modelo Sequencial

De acordo com este modelo, um acidente pode acontecer quando um sistema está em seu estado normal e após um evento inesperado, como um ato inseguro, se inicia a sequência de consequências onde pelo menos uma é o acidente.

A Figura 2-3 a seguir apresenta o modelo sequencial de acidente.

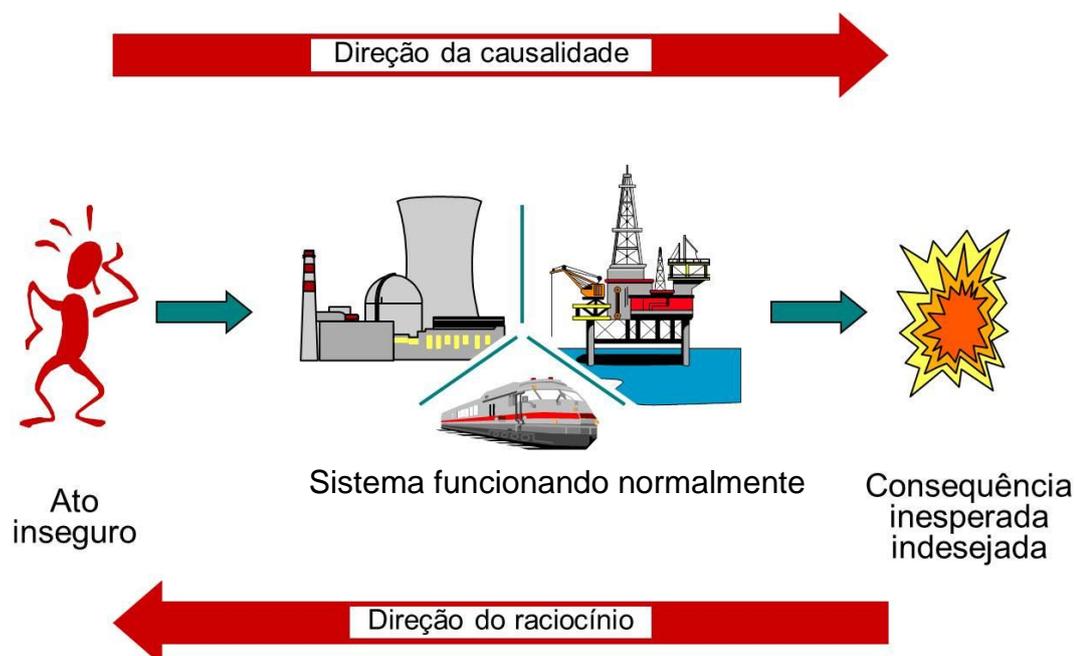


Figura 2-3– Modelo sequencial do acidente (Fonte: adaptado Hollnagel, 2002)

Uma das teorias que seguem o modelo sequencial é o modelo do dominó proposto por Heinrich em 1931 conforme observado na Figura 2-4. Neste modelo, cada dominó é representado por diferentes fatores que levam ao acidente e suas lesões. Atos inseguros ou condições inseguras são os principais fatores que levam ao acidente. De acordo com a lógica da teoria do dominó, um acidente pode ser prevenido se um ou mais blocos de dominó são eliminados.

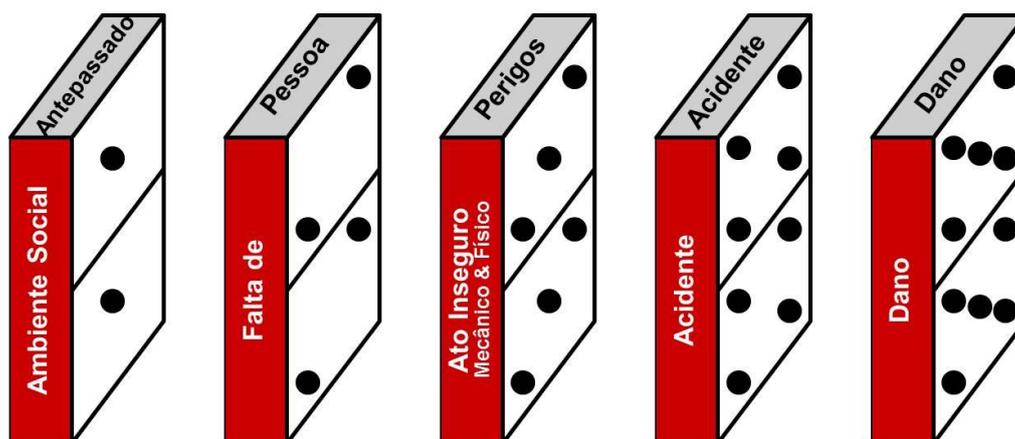


Figura 2-4– Teoria do dominó - depois de Heinrich, 1931 (Fonte: adaptado Hollnagel, 2002)

2.2.2 Modelo Epidemiológico

Neste modelo, conceitos como desvios de desempenho, condições latentes, condições ambientais e barreiras são adicionados ao modelo sequencial conforme apresentado na Figura 2-5.

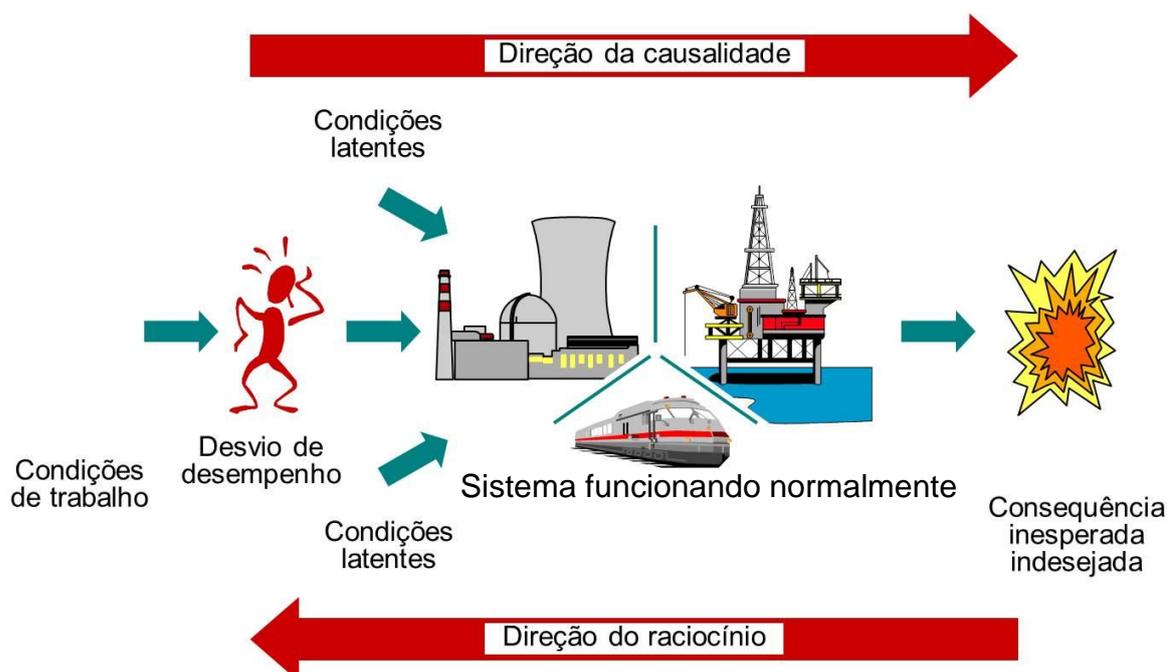


Figura 2-5– Modelo epidemiológico (Fonte: adaptado Hollnagel, 2002)

Neste modelo, o conceito de ato inseguro (sinônimo de erro humano) gradualmente vai sendo trocado pelo conceito de desvio de desempenho. Este novo termo é mais neutro e um desvio de performance pode acontecer tanto com um componente do sistema ou com uma pessoa. O modelo epidemiológico proposto por Hollnagel (2004) também considera condições que podem levar a desvios de desempenho, chamando de condições ambientais. Como conceito, foi uma forma de deixar a análise mais ampla. Condições ambientais existem, tanto para seres humanos como para tecnologia, para o primeiro caso são referidos como condições de trabalho.

A terceira característica deste modelo é o conceito de barreiras que podem prevenir as consequências não esperadas ou até impedir o desenvolvimento do acidente.

As condições latentes podem ter diferentes causas como decisões gerenciais ou organizacionais, deficiência ou falhas no projeto, deficiência ou falhas na manutenção, e degradação das funções do sistema. Condições latentes combinadas com falhas ativas podem levar ao acidente.

Um exemplo deste modelo é a teoria do queijo suíço proposto por James Reason em 1990 (apresentado na Figura 2-6). Neste modelo, as defesas organizacionais contra as falhas são modeladas em uma série de barreiras,

representadas por fatias de queijo suíço. Os orifícios no queijo representam a fraqueza individual de cada sistema, que pode ser exemplificado por um ato inseguro ou uma barreira ineficiente. Quando os orifícios de cada fatia estão alinhados, significa que o perigo ultrapassa todos os orifícios levando a falha.

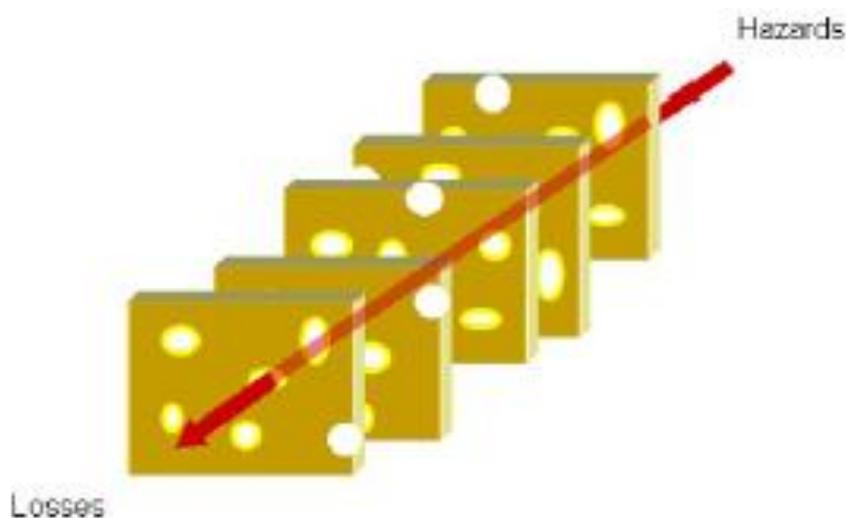


Figura 2-6– Teoria do queijo suíço, Reason 1990 (Fonte: Hollnagel, 2006)

2.2.3 Modelo Sistêmico

O modelo sistêmico proposto por Hollnagel (2004) tenta descrever as características de desempenho no nível do sistema como um todo, mais do que no nível específico do mecanismo de “causa e efeito”. As questões ambientais, propostas no modelo epidemiológico, são substituídas neste por uma forma triangular que demonstra como a falha pode surgir desde sua base até o topo como pode ser observado na Figura 2-7 e na Figura 2-8.

Outra consequência deste modelo é que não há mais indicação direta da causa. Acidentes, é claro, acontecem por algum um motivo, porém é mais enganoso sugerir a progressão simples que se originou nos modelos sequenciais. É observado que neste modelo a seta indicando a casualidade não existe mais, porém permanece a seta indicando a direção do raciocínio.

À frente (“*sharp-end*”) estão as pessoas envolvidas no trabalho, no momento e lugar onde o sinistro ocorreu, ou melhor, as pessoas que interagem com o processo. Na base (“*blunt-end*”) estão as pessoas que afetam a segurança através de restrições e recursos agindo sobre os trabalhadores.

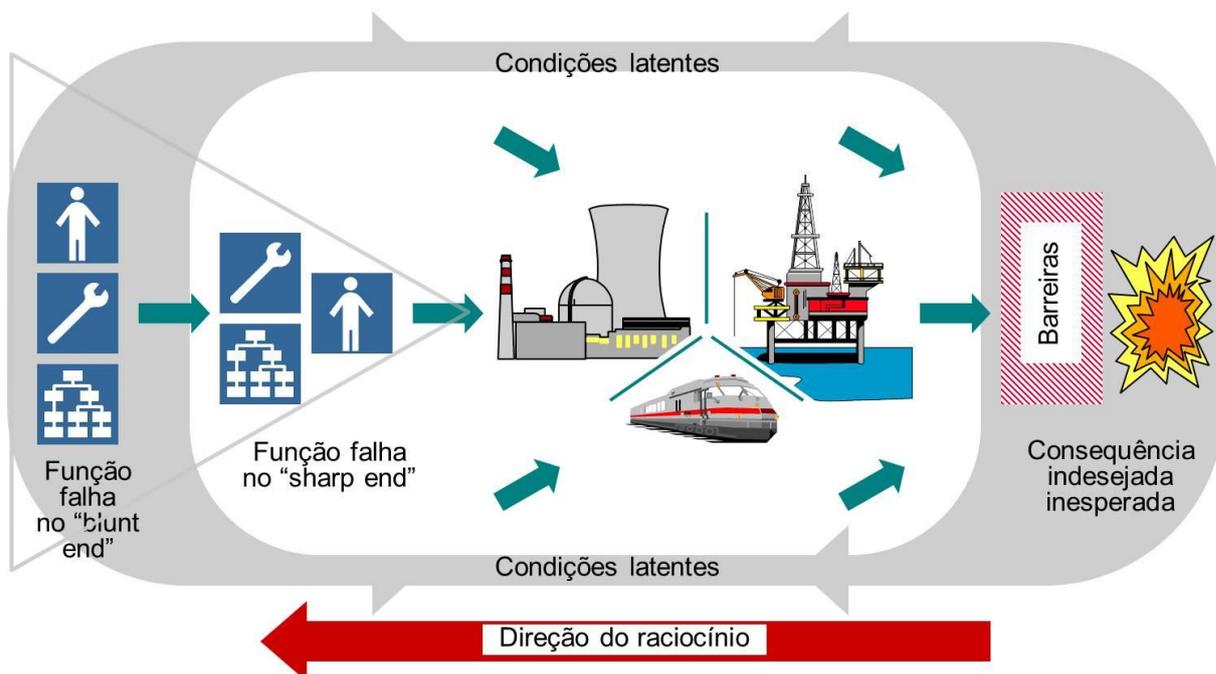


Figura 2-7– Modelo sistêmico de acidente (Fonte: adaptado Hollnagel, 2002)

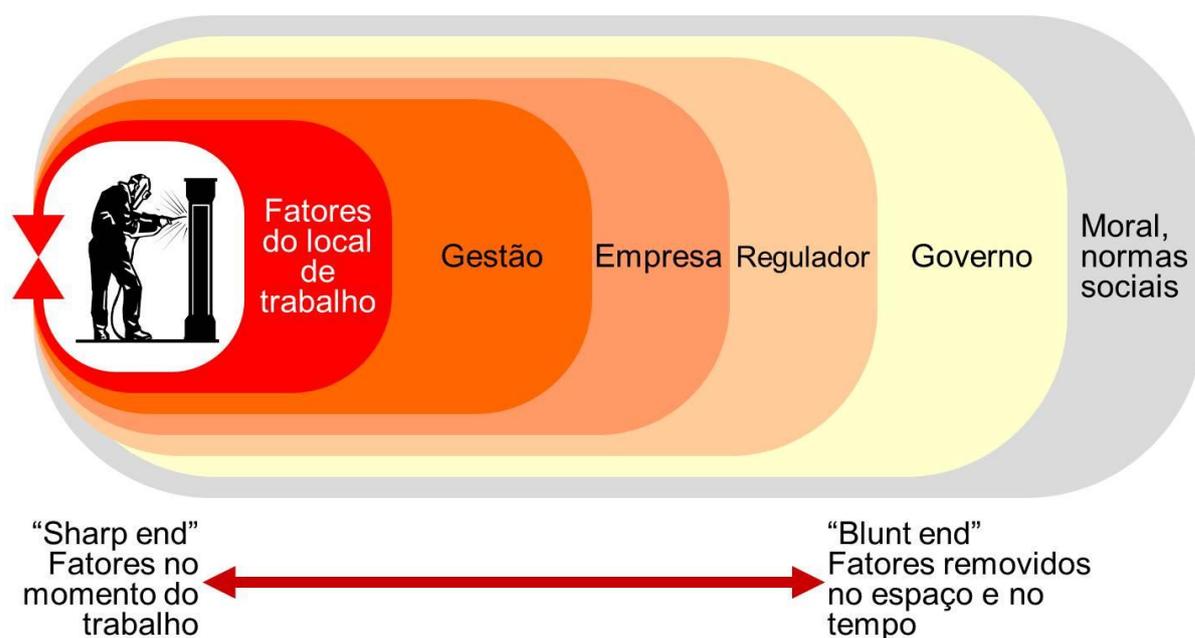


Figura 2-8– Relações entre o blunt-end e o sharp-end que levam a falha (Fonte: adaptado Hollnagel, 2002)

Em acordo com Hollnagel, Leveson (2002) também defende a ampliação da análise dos acidentes. Segundo ela, é preciso:

- Expandir a análise, levando em consideração outros fatores além de falhas de componentes e fatores humanos;
- Considerar erros na concepção de sistemas e disfunções de interações;

- c) Permitir e estimular novos tipos de análise de riscos que vão além das falhas de componentes e que possa lidar com o complexo papel que os softwares e os humanos assumem nos sistemas de alta tecnologia de hoje em dia;
- d) Mudar a ênfase dada a erros humanos em acidentes para mecanismos e fatores que modelem comportamentos humanos;
- e) Mudança da ênfase em causas – enfoque limitado e de busca de culpados – para compreensão de razões dos acidentes, isto é, por que os eventos e erros ocorrem;
- f) Examinar os processos e não apenas eventos e condições envolvidos nos acidentes;
- g) Estimular múltiplos pontos de vista e interpretações.

2.3 PREVENÇÃO DE ACIDENTES

Kletz (2001) expõe a prevenção de acidentes a partir de lições aprendidas. Conforme Hollnagel, Kletz (2001) também evita a palavra “causa” por quatro motivos:

- a) Ao invés de se perguntar qual a causa do acidente, o correto seria: O que se pode fazer de diferente para prevenir outro acidente? Com essa abordagem se pode pensar em mudanças no projeto ou no método de operar um determinado sistema;
- b) A palavra causa tem um ar de finalidade que desestimula as investigações. Caso uma tubulação falhe e a causa, por exemplo, seja corrosão, somos tendenciosos a pensar que sabemos por que ocorreu a falha, mas isto não nos ajuda a evitar novos fracassos. As perguntas que precisam ser respondidas passam por: o material de construção foi especificado corretamente? O material especificado foi realmente o utilizado? As condições de funcionamento foram às mesmas assumidas pelos projetistas? Foi realizado monitoramento de corrosão? Os resultados foram ignorados? E assim por diante.
- c) A palavra causa implica culpa e as pessoas ficam na defensiva. Há relutância em admitir que “fizemos algo errado”, porém estamos geralmente dispostos a admitir que se pode fazer melhor.

- d) Quando questionadas sobre a causa do acidente, muitas pessoas tendem a sugerir atos abstratos como falha institucional, nova tecnologia, atos de Deus ou, até mesmo, o destino. Mas instituições e tecnologia não têm vontade própria e não pode mudar por conta própria: alguém tem que fazer algo. Devemos dizer quem, o quê e quando, ou nada vai acontecer. Relâmpagos e outros, os chamados atos de Deus, não podem ser evitados, mas sabemos que eles podem e irão ocorrer e culpá-los é quase tão útil quanto culpar a luz ou escuridão. O destino é apenas uma desculpa de uma pessoa para não fazer nada.

Outro ponto que Kletz (2001) enfatiza é a irrelevância de se achar um culpado. Caso isso aconteça, é provável que nunca se descubra o que realmente aconteceu e conseqüentemente não seremos capazes de prevenir este acontecimento novamente. Uma ocasional negligência pode não ser punida, porém segundo o autor, é um pequeno preço a ser pago para prevenir novos acidentes. Um acidente pode mostrar que um trabalhador não tem a capacidade, experiência ou qualificação para realizar uma tarefa específica e este trabalhador pode ser realocado de função, mas não como punição, mas sim para adequá-lo na função correta. Ainda segundo Kletz (2001), muito poucos acidentes são resultados de negligência. Erro humano pode ser resultado de um momento de esquecimento ou aberração. Outros erros são resultados de treinamento, supervisão ou instrução inadequada. Adicionalmente, Kletz (2001) aponta que raramente acidentes são ocasionados por falha de uma única pessoa. A responsabilidade está geralmente dividida entre muitas pessoas.

Em relação aos modelos de acidentes, Kletz (2001) acredita que tais modelos podem não ser úteis. Segundo ele, o tempo pode ser gasto em ajustar os dados em um modelo e que este desvie o pensamento para descobrir maneiras menos óbvias para prevenção do acidente. Segundo sua sugestão, deve-se utilizar os modelos de acidente somente se forem úteis, mas não para se tornar um escravo, ou seja, caso acredite que um modelo não esteja ajudando, desconsidere-o.

Segundo o autor, a prevenção deve vir em primeiro lugar e os itens que ele considera mais valiosos são:

- a) Estudo de perigo e operabilidade (HAZOP) na fase de detalhamento do projeto;

- b) A variação de técnicas na fase de projeto básico, quando se decide que produto será produzido e por qual rota.
- c) Inspeção detalhada durante e depois da construção para assegurar que o projeto e os detalhes foram construídos de acordo com as boas práticas de engenharia;
- d) Auditorias de segurança durante a operação da planta.

Outros fatores que atuam na prevenção de acidentes é a mudança de atitude, comportamento e condição estrutural. Quando medidas preventivas são usadas de forma combinada e estas passam a influenciar normas sociais e fatores culturais, provavelmente serão mais eficazes do que as intervenções que afetam somente os indivíduos (modificando fatores como atitudes e crenças).

Conforme exposto por Lund (2004), embora medidas de mudança de atitude pareçam ter pouco impacto direto sobre o comportamento, estas podem ter um papel importante na prevenção de acidentes. Desafios importantes como as intervenções que influenciam as normas sociais e de segurança relacionados com aspectos da cultura e identificação das melhores combinações de medidas preventivas, permanecem em desenvolvimento. Os pontos citados acima serão abordados nos itens seguintes desta dissertação.

2.4 CULTURA DE SEGURANÇA

O conceito cultura de segurança tem recebido atenção considerável e representa uma importante e ampla perspectiva na pesquisa para prevenção de danos.

O *UK Health and Safety Executive* (GADD, 2002), define cultura de segurança como o produto de valores individuais e de grupo, atitudes, competências, padrões de comportamento que determinam o compromisso com o estilo e competência, da “saúde” de uma organização e dos programas de segurança. Já o *Center for Chemical Process Safety - CCPS* (AIChE, 2005), define que cultura de segurança é como a organização se comporta quando ninguém está observando.

Segundo Lees (2005), uma atitude positiva em relação à segurança não é, no entanto, suficiente para criar uma cultura de segurança. Gestores de uma indústria química precisam liderar de maneira bem específica. Publicidade, como panfletos e

livretos, geralmente não são eficazes para se conseguir a atenção nas questões relacionadas com a segurança, pois parecem tediosos. A abordagem mais vantajosa seria enfatizar a segurança e a prevenção de perdas como questão de profissionalismo. A contribuição da alta administração, portanto, é incentivar a profissionalização na área, atribuindo pessoas capazes, dando-lhes objetivos, recursos e a criação de sistemas adequados de trabalho. Outro fator importante para os gestores é o de valorizar as iniciativas vindas de seus trabalhadores.

Para o CCPS (AICHE, 2005), cada organização possui sua cultura de segurança, porém esta pode estar operando em qualquer nível. Os grandes desafios para a liderança de uma organização são:

- e) Determinar o nível da cultura de segurança na organização;
- f) Decidir para onde querem levar a cultura de segurança, e;
- g) Traçar e percorrer o caminho.

Sistemas de gestão e as suas políticas e procedimentos associados dependem das ações de indivíduos e grupos para que a sua implementação seja bem sucedida. Por exemplo, um procedimento pode refletir adequadamente a intenção desejada com as instruções devidamente detalhadas. No entanto, a execução com sucesso do procedimento requer as ações de indivíduos devidamente treinados que entendam a importância da intenção, que assumam a responsabilidade para a condução da tarefa, e saibam que se tomar um “atalho” potencialmente inseguro será, simplesmente, um erro.

Os valores do grupo (por exemplo, corporação e equipe turno), ajudam a moldar as crenças e atitudes do indivíduo, que por sua vez, desempenham um papel significativo na determinação do comportamento do indivíduo. Uma fraca cultura de segurança pode ser evidenciada pelas ações de indivíduos em todos os níveis da organização. Como exemplo pode-se citar, a falha de um intertravamento crítico que pode ter sido causada pelo mecânico que não conseguiu calibrar o instrumento e falsificou os registros de manutenção. Alternativamente, poderia ter sido causada pelo gerente da planta que não aprovou o recurso solicitado pelo departamento de manutenção/inspeção.

Perguntas como porque operadores utilizam “atalhos”?; porque se sentem confortáveis em realizá-lo?; ou porque supervisores toleram práticas que põem em

risco a segurança das instalações? são feitas e a partir destas respostas se procura entender os valores, crenças e atitudes que moldam as ações e omissões de um indivíduo.

Segundo CCPS (AICHE, 2005), ao identificar e tratar os desvios dentro da cultura de segurança, efetivamente se consegue abordar e tratar a causa raiz de problemas de desempenho de segurança.

Criar e manter uma cultura de segurança sólida pode ser um fator decisivo na determinação de um indivíduo e do sistema.

Conforme já abordado em Lees (2005), o CCPS (AICHE, 2005) também aborda que a responsabilidade inicial de identificar, determinar ou alterar, se aplicável, a cultura de segurança está na alta gerência, ou seja, na liderança da organização.

Porém cada indivíduo da organização tem um papel a desempenhar, pois a responsabilidade de manter e promover uma sólida cultura de segurança deve ser desdobrada desde a liderança até os operadores. Logo, se espera de uma cultura sólida de segurança, que um indivíduo interceda junto ao colega de trabalho prestes a cometer um ato inseguro, que a liderança monitore a “saúde” da cultura de segurança e a atualize caso necessário e indivíduos/grupos busquem a manutenção do sistema, caso percebam que o gerenciamento não esteja ocorrendo em conformidade com os valores da organização.

Atributos chaves para uma sólida cultura de segurança são apresentados no Quadro 2-1 baseada no livro *Guidelines for Risk Based Process Safety* do CCPS (AICHE, 2007) que coloca a cultura como um fator determinante na prática e atitudes no controle dos riscos de processos.

Quadro 2-1 – Cultura Fraca x Cultura Sólida (Fonte: AICHE, 2007)

Cultura fraca	Cultura sólida
Atribui pouco valor para segurança de processo	Integra um imperativo para operação segura nas organizações de valores fundamentais
Tem pouca percepção das vulnerabilidades da segurança de processo	Tem um foco em possíveis falhas que o conduz a buscar uma compreensão clara dos riscos e os meios para controlá-lo
Dedica recursos mínimos para controlar o risco residual.	Visa proporcionar recursos proporcionais aos riscos que visa controlar
Negligencia sinais de problemas de segurança.	Ênfase em aprender com experiências passadas a fim de evitar problemas futuros
Geralmente aceita e normaliza o desempenho cada vez mais pobres	Melhora contínua do desempenho
Depende da gestão para identificar os riscos e determinar quais ações devem ser tomadas.	Os funcionários estão envolvidos em identificar os riscos e decidir como devem ser abordados. Empregados tomam medidas para lidar com riscos, sem envolvimento da gerência.

Um exemplo de deficiência na cultura segurança e que reforça o acima exposto pode ser observado no relatório (*The report of BP U.S. Refineries Independent Safety Panel, 2007*) realizado após a explosão na refinaria da *British Petroleum* (BP) no Texas, em 2005 que resultou em 15 fatalidades e mais de 170 feridos. Este relatório foi elaborado em resposta a recomendação da *United States Chemical Safety* e da *Hazard Investigation Board*. Com isso se estabeleceu um comitê de investigação liderado pelo Secretário de Estado James Baker. O comitê tinha como objetivo fazer uma avaliação completa, independente e confiável do sistema de gestão de segurança em cinco refinarias da BP nos EUA e sua cultura de segurança corporativa. Segundo Hendershot (2007), membro do comitê, o relatório emitido em 2007 possui uma importante mensagem sobre cultura e compromisso com a segurança para qualquer organização que possua atividade perigosa.

Entre as conclusões importantes pode-se citar:

- a) Não estabeleceu a segurança de processo como um valor fundamental nas refinarias dos EUA;
- b) Falta de uma liderança eficaz ou o não estabelecimento de expectativas apropriadas em relação ao desempenho da segurança do processo;

- c) Ênfase na segurança pessoal (esforço bem-sucedido), mas não na segurança do processo, a gestão executiva não recebeu/respondeu de forma eficaz à informação de que havia deficiências na segurança processo em algumas instalações.
- d) Não assegurou a realização de um integrado, compreensivo e efetivo sistema de gestão de segurança de processo.

Ainda segundo Hendershot (2007), o comitê acredita que esses resultados não sejam exclusivos a BP e que outras organizações devem pensar sobre a eficácia e desempenho real de seu sistema de gestão de segurança de processo.

Acidentes como a liberação de gás tóxico de Bophal, o desastre da plataforma de *Piper Alpha* e a explosão da refinaria da BP na cidade do *Texas* resultaram em fatalidades, sérios danos e uma grande perda econômica. Todas as investigações destes acidentes, concluíram que uma fraca cultura de segurança foi um importante contribuinte para o acidente.

2.5 O FATOR HUMANO

Conforme modelo de Reason (Oliveira, 2008), as falhas humanas são classificadas em erro humano (ação não intencional) e violação (ação intencional) com consequências não intencionais conforme Figura 2-9. A sabotagem possui ação e consequências intencionais, é crime, e não é uma falha humana.



Figura 2-9– Modelo de Reason, 1990 (Fonte: Oliveira, 2008)

Conforme figura acima, o erro humano é classificado em deslizes, lapsos e enganos conforme Reason (1990). O significado de cada um deste é apresentado no Quadro 2-2 a seguir:

Quadro 2-2 – Erro Humano (Oliveira, 2008)

Erro Humano	
Deslizes	Falhas de Atenção <ul style="list-style-type: none"> - Ação desnecessária, - Inação - Ação reversa - Fora de ordem - Ação intempestiva
Lapsos	Falhas de Memória <ul style="list-style-type: none"> - Omissão de um passo previsto - Esquecimento da intenção
Enganos	Regras <ul style="list-style-type: none"> - Má aplicação de uma regra certa - Aplicação da regra errada Conhecimento <ul style="list-style-type: none"> - Diagnóstico errado - Má interpretação das condições - Várias outras formas

O modelo de desempenho humano, desenvolvido por Ramussen em 1986, representa várias fases que o trabalhador pode passar ao lidar com perturbações do processo.

Segundo Falzon (2009), o modelo considera competências cognitivas através do modelo Habilidades-Regras-Conhecimento, do inglês *Skill-Rule-Knowledge* (SRK), com o objetivo de tratar a dinâmica dos processos de controle das tarefas.

Através deste modelo se identifica três tipos de comportamento do colaborador no trabalho conforme descrito abaixo e apresentado na Figura 2-10 (Rasmussen, 1983):

- a) Comportamento baseado em habilidades (*Skills*) representa um desempenho sensório-motor durante atos e atividades o qual, seguindo uma intenção, são acionadas sem um controle consciente, ou seja automáticas e com alto padrão integrado de comportamento. A flexibilidade do desempenho das habilidades é devido à competência em compor em um grande repertório de sub-rotinas automáticas, os conjuntos apropriados para objetivos específicos. Adicionalmente são pouco sensíveis às condicionantes do meio ambiente e permitem reações rápidas, podendo se desenrolar paralelamente com outras atividades. Podem, certamente, originar uma ação que seja resposta inadequada ao estado do sistema.
- b) Comportamentos baseados em regras (*Rules*): a composição de sequências de sub-rotinas em uma situação familiar no trabalho é tipicamente controlada por uma regra ou procedimento o qual pode ter sido derivado empiricamente durante ocasiões prévias, comunicado por outras pessoas que possuem o conhecimento, como instruções/receitas ou preparadas em uma ocasião para solução de um problema. Os comportamentos baseados em regras são sequências de ações controladas por normas memorizadas por meio da aprendizagem. Contrariamente a anterior, este comportamento supõe uma execução e, uma coordenação das mesmas, pois correspondem a situações familiares, mas que tem um certo grau de variabilidade.
- c) Comportamentos baseados em conhecimento (*Knowledge*): São os comportamentos baseados em conhecimentos que aparecem não

familiares para as quais não existem regras pré-construídas ou conhecimento. Nesta situação o objetivo é explicitamente formulado baseado na análise do ambiente e do propósito do indivíduo.

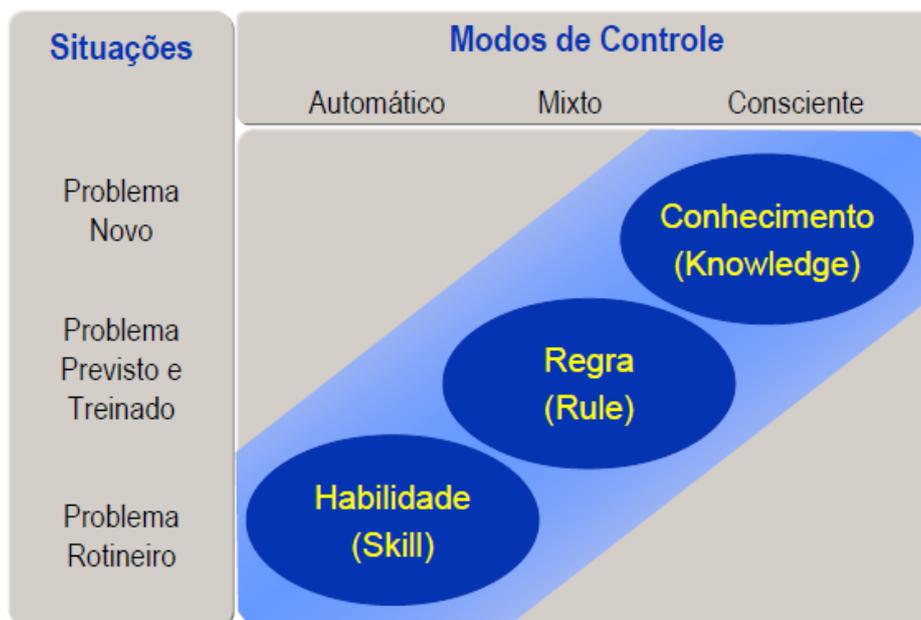


Figura 2-10– Níveis de controle das Ações (Fonte: Oliveira, 2008)

A partir do apresentado acima, Oliveira (2008) apresenta a relação dos níveis de controle de ação e o modelo apresentado por Reason. (Figura 2-11). Pode-se notar que os deslizos e os lapsos se relacionam com a habilidade e os enganos com as regras e o conhecimento.

Adicionalmente expõe que a ação intencional, a violação, otimizadora e rotineira, levam ao ganho pessoal, ou seja, na realização da tarefa mais rápida, porém às vezes não tão eficiente. Este cita também que a ação rotineira pode ser realizada para o ganho do serviço assim como a violação necessária, ou seja, ação dos gestores para privilegiar a produção.

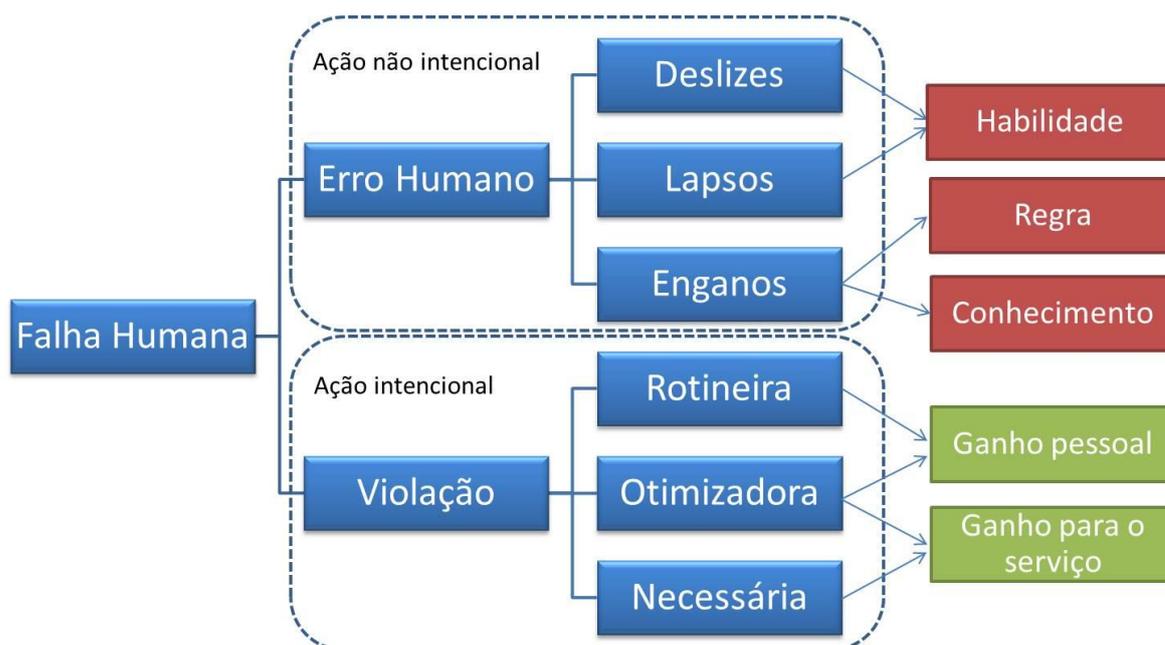


Figura 2-11– Níveis de controle das ações relacionados com modelo de Reason (Fonte: Oliveira, 2008)

É sabido que grande proporção dos acidentes é atribuída a falhas humanas (70-80%). Dizer que um acidente foi causado por uma falha humana não é suficiente para explicar as causas do acidente em um nível que possa ser utilizado para o aprendizado organizacional. Conforme exposto por Reason, erro humano é a consequência e não a causa. Muitas vezes o operador é conformado e provocado por fatores relacionados ao ambiente de trabalho e por aspectos organizacionais.

Segundo Reason, o trabalhador é o agente final, conforme já observado na Figura 2-8, que “realiza o ato inseguro”. Este cita a influência de condições latentes que correspondem aos fatores relacionados ao ambiente de trabalho e os fatores organizacionais, itens já mencionados na cultura de segurança.

Oliveira (2008) em acordo com Kletz, diz que para se atingir a excelência é importante que a organização promova a “comunicação aberta”:

- a) Empresa deve incentivar que o empregado relate voluntariamente a ocorrência de erros humanos;
- b) Empregado deve sentir-se à vontade para comunicar que cometeu um erro humano, sem correr o risco de sofrer punições ou qualquer outro tipo de constrangimento.

Nota-se que prevenção de acidentes, cultura de segurança e o fator humano estão interligados. Uma cultura de segurança da empresa deve ser construída de modo que as pessoas sintam-se motivadas a reportar os seus erros.

2.6 BARREIRAS DE SEGURANÇA

Um outro fator considerável na prevenção de acidentes são as barreiras de segurança.

As barreiras de segurança são os obstáculos que podem prevenir/impedir um determinado evento perigoso, ou caso ele ocorra, proteger os indivíduos e/ou o ambiente, impedindo ou minimizando os danos.

Segundo Hollnagel (2004), as barreiras podem ser de Prevenção ou de Proteção, devido ao fato destas atuarem antes ou depois da ação acontecer, respectivamente. As barreiras de prevenção se destinam a funcionar antes de iniciar um evento específico, servindo como um meio de prevenção. Estas barreiras possuem pretensão de assegurar que o acidente não aconteça, ou pelo menos retardar o desenvolvimento de situações que possam resultar em um acidente. As barreiras de proteção tem o objetivo de proteger o ambiente e as pessoas, assim como o próprio sistema, das consequências do acidente.

As barreiras de segurança também podem ser classificadas em ativas ou passivas. Uma barreira ativa pode envolver uma ou mais funções, e através de sua ação atingir a finalidade da barreira. Já a barreira passiva não precisa tomar nenhuma ação, ou seja, cumpre a sua finalidade apenas por estar no local do evento. Como exemplo de barreira ativa pode-se citar um intertravamento de segurança e o dique de contenção como exemplo de barreira passiva. Em relação à proteção, uma barreira ativa serve para reduzir ou desviar as consequências, enquanto uma barreira passiva contém ou detém as consequências.

A diferença entre barreiras de proteção/prevenção e ativa/passiva é ilustrada na Figura 2-12.

A Figura 2-12 é apresentada no momento em que o controle foi perdido ou alguma função falhou. Antes do fato acontecer, as barreiras atuam de forma a prevenir a ocorrência do evento (acidente). Nesta fase as barreiras podem ser ativas ou passivas. Como exemplo de barreiras preventivas ativas pode-se citar os alarmes

e detectores. Um acesso restrito a zona de perigo pode ser considerado como um exemplo de barreiras preventivas passivas. Após a perda do controle, as barreiras servem para proteger das possíveis consequências do acidente. Aqui é possível fazer uma distinção adicional entre as barreiras que atuam para desviar as consequências e as barreiras que servem para minimizar as consequências geralmente, impedindo que se propague ainda mais.

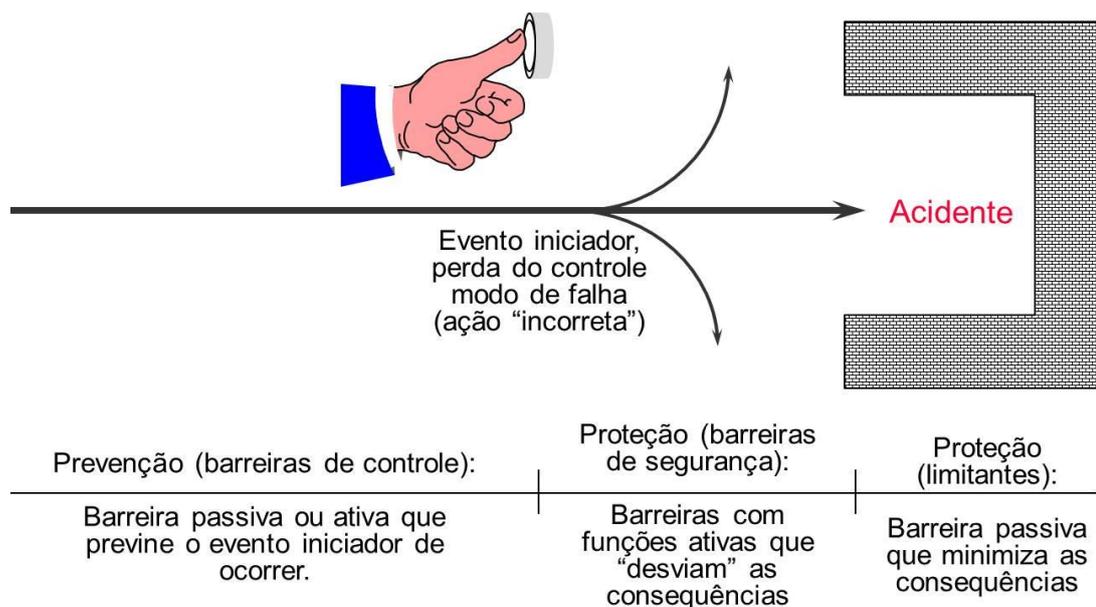


Figura 2-12– Prevenção e Proteção (Fonte: adaptado Hollnagel, 2002)

Conforme exposto do Hollnagel (2004), apesar da importância das barreiras na análise dos acidentes e sua prevenção, há poucos estudos sistemáticos disponíveis na literatura.

Um destes estudos é o das barreiras e as falhas latentes como já exposto no item 2.2. As defesas, ou barreiras, foram adicionadas como uma camada intermediária entre os atos inseguros e os acidentes. Os modelos descritos como condições de falha latentes são provenientes dos processos organizacionais que podem degradar as defesas, deixando o caminho livre para os atos inseguros se tornarem acidentes.

Este modelo descreve que as defesas possuem 6 funções:

- a) Proteção: fornecer uma barreira entre os perigos e potenciais vítimas sob condições normais de operação;

- b) Detecção: para detectar e identificar as ocorrências fora das condições normais, atos inseguros ou a presença de substâncias perigosas.
- c) Sinal de alerta: para indicar a presença e a natureza do perigo para todos aqueles que possam estar expostos aos perigos;
- d) Recuperação: para restaurar o sistema para um estado seguro, o mais rápido possível;
- e) Contenção: para limitar a propagação do perigo no caso de uma falha em qualquer ou em todas as funções defensivas anteriores;
- f) Escape: para garantir a evacuação de todas as potenciais vítimas após um acidente.

A natureza das barreiras é independente de sua origem, sua finalidade (preventiva ou proteção), e de sua localização. Os sistemas de barreira podem variar desde obstáculos físicos a regras e leis. Uma proposta, feita por Hollnagel (2004), classifica os sistemas de barreira em quatro categorias:

- a) Físicos: estas barreiras impedem fisicamente que uma ação seja realizada. Barreiras físicas também podem proteger bloqueando ou mitigando os efeitos de um evento inesperado. Este tipo de barreira apresenta um obstáculo físico para o transporte de massa ou de energia ou de informação do ponto A para o ponto B, caso não possa impedi-lo em todas as circunstâncias, ao menos poderá retardá-lo. Exemplos deste tipo de barreiras são os prédios, salas, paredes, paredes corta-fogo, etc;
- b) Funcional (ativa ou dinâmica): um sistema de barreira funcional age impedindo que o evento indesejado aconteça através de um intertravamento, lógico ou temporal. Um sistema de barreira funcional efetivamente configura uma ou mais pré-condições que devem ser cumpridos antes do evento indesejado. Essas pré-condições não requerem sempre a interpretação humana, mas podem ser interrogados ou detectados por um sistema. Como exemplo pode-se citar o intertravamento automático e o bloqueio, que pode ser físico necessitando da utilização de uma chave, ou lógico que requer algum tipo de senha ou identificação;
- c) Simbólico: essas barreiras requerem um ato de compreensão e interpretação por parte das pessoas. Podem ser usados individualmente

ou combinados e existem na forma de sinais e avisos de diversos tipos. Exemplos típicos são os avisos passivos como proibido fumar ou mantenha-se afastado e os sistemas de avisos visuais e sonoros, como instruções presentes no local, demarcações, alarmes, permissão de trabalho e etc;

- d) Imaterial: a última classe de barreiras é o imaterial ou não-material. Isto significa que a barreira não está presente fisicamente, mas depende do conhecimento do utilizador para atingir sua finalidade. Sistemas imateriais de barreira são geralmente representados na forma física como um livro ou um memorando. Típicos sistemas de barreira imateriais são: regras, diretrizes e princípios de segurança.

As ações humanas, conforme citado por Dianous (2006), também podem ser consideradas como barreiras. Porém a eficácia destas depende do conhecimento do operador no sentido de alcançar o objetivo da tarefa. As ações humanas devem ser interpretadas sem restrições, incluindo observações feitas por todos os sentidos, comunicação, pensamento, atividade física e também as regras, diretrizes, princípios de segurança, etc. As ações humanas podem ser parte de um sistema sequencial de detecção - diagnóstico - ação.

2.6.1 Qualidade e Desempenho das Barreiras de Segurança

Como é sabido, as barreiras de segurança são um importante meio para atingir os objetivos da segurança, prevenindo os acidentes. Logo um conjunto de critérios exposto por Hollnagel (2004) abordam vários aspectos de qualidade das barreiras, são eles:

- a) Eficiência: refere-se na capacidade da barreira em atingir seu objetivo;
- b) Recursos necessários: são os recursos necessários para implementar e manter uma barreira de segurança. O custo do sistema de barreira sempre é levado em conta. A eficiência nunca é considerada sem pensar no custo, logo a segurança tem sempre seu preço;
- c) Robustez: refere-se ao quão confiável e resistente a barreira é, isto é, como ela pode suportar a variabilidade do ambiente (práticas de trabalho, degradação, desgaste, etc.);

- d) Atraso na implementação: é o tempo desde a concepção até aplicação de uma barreira. Este tempo pode entrar em conflito com a necessidade de se agir rapidamente;
- e) Aplicabilidade para tarefas críticas de segurança: tarefas críticas de segurança desempenham um papel especial em sistemas sócio-técnicos. Em certas ocasiões, barreiras específicas podem ser mais necessárias, porém por outro lado estas geralmente estão sujeitas a uma série de restrições por parte da administração ou dos órgãos reguladores;
- f) Avaliação: é de grande importância pois determina se uma barreira funciona como esperado. A avaliação deve abordar a qualidade da barreira, tanto durante a concepção como durante a utilização real (inspeção de verificação prontidão);
- g) A dependência de seres humanos: a extensão em que uma barreira depende dos seres humanos a fim de alcançar o seu objetivo. A dependência refere-se à eficácia do sistema de barreira em uso em vez de, por exemplo, a necessidade de manutenção.

Conforme exposto por Dianous (2006), além da qualidade, a avaliação do desempenho das barreiras de segurança é necessária para demonstrar que uma dada função de segurança e as barreiras relacionadas são relevantes para evitar, prevenir, controlar ou para atenuar o evento. Através de três critérios, eficácia, tempo de resposta e nível de confiabilidade, é realizada a avaliação do desempenho das barreiras.

A eficácia da barreira de segurança deve ser demonstrada e adaptada para o cenário. É a capacidade para realizar uma função de segurança por um período de tempo, de um modo não-degradado e em determinadas condições. É expressa em percentual ou uma probabilidade de desempenho da função de segurança definida. Se a efetividade é apresentada em percentagem, ela pode variar durante o período de funcionamento da barreira de segurança. Por exemplo, uma válvula que não fecha completamente sob uma demanda não teria uma eficácia de 100%. Para avaliar a eficácia de uma barreira de segurança, é necessário conhecer seu projeto. Desta forma, a barreira deve ser concebida de acordo com códigos e regras, e o projeto deve ser adaptado às características dos produtos e do ambiente. As características de sua concepção devem estar de acordo com a função relacionada.

Durante a análise de risco pode ser realizada a avaliação da eficácia, considerando os dados e a experiência de fornecedores ou especialistas, a realização de testes no local, normas e guias técnicos, folhas de dados de cálculo das barreiras, entre outros.

O tempo de resposta deve estar em conformidade com a cinética do cenário do acidente considerado importante. É o tempo entre o início da atuação da barreira de segurança e a realização completa (o que é igual à eficácia) de sua função de segurança. Pode ser avaliado a partir de dados de especialistas, experiência, normas e manuais técnicos. Para as barreiras humanas, o tempo de resposta pode depender de critérios diferentes como treinamento do operador, fácil diagnóstico em caso de acidente, acesso a uma barreira, o conhecimento do operador sobre o que ele tem que fazer em caso de acidente.

O nível de confiabilidade de uma barreira de segurança é inversamente proporcional à probabilidade de falha sob demanda da barreira. Corresponde à confiabilidade da barreira de desempenhar adequadamente a função de segurança exigida de acordo com uma dada eficácia e tempo de resposta dentro de todas as condições determinadas e de um período de tempo determinado. O nível de confiabilidade das barreiras será abordado mais detalhadamente no próximo item.

2.6.2 Nível de Confiabilidade das Barreiras de Segurança

Através de estudos de análise de risco pode-se determinar o nível de integridade de segurança, ou SIL (*Safety Integrity Level*), de algumas barreiras de segurança.

O SIL é um indicador de desempenho do sistema instrumentado de segurança (SIS), medido através de sua probabilidade de falha na demanda (PFD). O SIS é uma camada de proteção instrumentada, composta de uma ou mais malhas de segurança, cuja finalidade é colocar o processo em estado seguro, quando determinadas condições pré-estabelecidas são atingidas. E a PFD é a probabilidade de uma malha de segurança falhar em resposta a uma demanda.

Com isso a função instrumentada de segurança (FIS), é uma função com um determinado nível de integridade de segurança que é necessário para que se alcance a segurança funcional.

Conforme o IEC 61508 (*International Electrotechnical Commission, 2010*), o SIL é um número inteiro que varia de 1 a 4, e reflete a probabilidade média de falha de um instrumento/equipamento quando o mesmo é chamado para atuar a fim de garantir a segurança do sistema. O Quadro 2-3 apresenta o SIL relacionado à probabilidade de falha na demanda e o fator de redução de risco, ou seja, quanto maior é o SIL, menor é a probabilidade de falha na demanda e maior é o fator de redução do risco. Em outras palavras, quanto maior SIL, mais confiável esta malha dever ser, pois o evento indesejado a ser evitado tem um risco maior quando comparado a um sistema que possui o nível de SIL menor.

Quadro 2-3 – Relação entre SIL, PFD e FRR (Fonte: IEC 61508, 2010)

Safety Integrity Level	Regime de Baixa Demanda	
	Probabilidade de Falha na Demanda (PFD)	Fator de Redução de Risco (FRR)
4	$\geq 10^{-5}$ a $< 10^{-4}$	10.000 a 100.000
3	$\geq 10^{-4}$ a $< 10^{-3}$	1.000 a 10.000
2	$\geq 10^{-3}$ a $< 10^{-2}$	100 a 1.000
1	$\geq 10^{-2}$ a $< 10^{-1}$	10 a 100

A determinação do nível de integridade pode ser realizada através da metodologia de gráfico de risco ou por análise das camadas de proteção, mais conhecida como LOPA (do inglês *Layer Of Protection Analysis*).

A determinação do SIL requerido no método de gráfico de risco é baseada em uma análise qualitativa enquanto que o LOPA é baseado em uma técnica semi-quantitativa.

O LOPA é uma técnica de análise de risco desenvolvida para avaliar o risco de cenários de acidente considerando as camadas independentes de proteção pertinentes e determinar se existem camadas suficientes para proteção dos cenários de acidente em análise.

Entre os objetivos principais para a utilização do LOPA está a possibilidade de responder a questões relativas ao número e eficiência das salvaguardas existentes, através de uma abordagem sistemática. Questões de subjetividade de classificação de cenários a que as técnicas qualitativas (exemplo: método de gráfico de risco) estão sujeitas são minimizadas nesta técnica.

Nesses estudos, as proteções, ou barreiras de um sistema são usualmente chamadas de salvaguarda.

Como definição, uma salvaguarda é qualquer dispositivo, sistema ou ação que possui potencial de prevenir ou mitigar a ocorrência de eventos indesejáveis. Porém a efetividade de algumas salvaguardas não pode ser quantificada devido à falta de dados e incertezas. Logo a partir deste ponto se define o conceito de camada independente de proteção ou IPL quando se utiliza o método de determinação do SIL requerido via LOPA.

Deve-se ressaltar que toda IPL é uma salvaguarda, porém nem toda salvaguarda é uma IPL. Para que a proteção seja classificada como IPL, os seguintes critérios devem ser obedecidos:

- a) Ser eficiente: a IPL deve ser capaz de prevenir a ocorrência das consequências do cenário que está sendo analisado. A eficiência da camada deve ser quantificável, em termos da sua probabilidade de falha na demanda (PFD), que é definida como a probabilidade que um sistema (no caso a IPL) falhe em executar sua ação ou atividade designada quando for demandado. É um valor adimensional, entre 0 e 1; quanto menor o valor de PFD, maior é a redução na frequência das consequências para o evento indesejado. Para ser considerada uma IPL, a sua PFD deve ser no máximo igual a 0,1, ou seja, deve proporcionar uma redução de riscos equivalente pelo menos a um fator de 10;
- b) Ser independente: a IPL deve ser independente em relação aos componentes de outras camadas de proteção associadas ao cenário analisado. Não deve existir também relação entre o evento iniciador e a habilidade da IPL em desempenhar sua função (por exemplo, se a causa do cenário for uma falha do sistema de controle, este não contará como IPL);
- c) Ser auditável: a camada deve ser auditável no sentido de demonstrar que atinge os requisitos para ser considerada uma IPL (eficiência e independência). A auditabilidade pode ser garantida através de documentação, revisão, teste ou outros meios.

Quanto à sua forma de atuação e quanto à sua eficiência em reduzir a frequência ou as consequências do cenário, as salvaguardas podem ser classificadas em:

- a) Ativa ou passiva;
- b) Preventiva (antes da liberação) ou mitigatória (após a liberação).

O Quadro 2-4 e Quadro 2-5 apresentam alguns exemplos de IPL ativa e passiva com sua respectiva PFD.

Quadro 2-4 – Exemplos de IPLs Ativas (Fonte: AICHE, 2001)

IPL	PFD
Dique	1×10^{-2}
Sistema de drenagem	1×10^{-2}
Suspiro aberto (sem válvulas)	1×10^{-2}
Proteção passiva contra fogo	1×10^{-2}
Parede contra explosão (blast wall/bunker)	1×10^{-3}
Projeto inerentemente seguro	1×10^{-2}
Retentor de chama (detonação/deflagração)	1×10^{-2}

Quadro 2-5 – Exemplos de IPLs Passivas (Fonte: AICHE, 2001)

IPL	PFD
Válvulas de Alívio	1×10^{-2}
Disco de Ruptura	1×10^{-2}
Sistema de Controle	1×10^{-1}
Sistema Instrumentado de Segurança (SIL1)	$\geq 1 \times 10^{-2} \leq 1 \times 10^{-1}$
Sistema Instrumentado de Segurança (SIL2)	$\geq 1 \times 10^{-3} \leq 1 \times 10^{-2}$
Sistema Instrumentado de Segurança (SIL3)	$\geq 1 \times 10^{-4} \leq 1 \times 10^{-3}$

No Quadro 2-6 a seguir apresenta exemplos de salvaguardas que usualmente não são consideradas como IPL.

Quadro 2-6 Salvaguardas que geralmente não são consideradas IPL (Fonte: AICHE, 2001)

Salvaguardas	Comentários
Treinamento e Certificação	Esses fatores podem ser considerados na determinação de PFD para a atuação do operador, porém não são IPL por si só.
Procedimentos	Esses fatores podem ser considerados na determinação de PFD para a atuação do operador, porém não são IPL por si só.
Testes e Inspeções	Em todas as avaliações de perigo assume-se perfeita execução destas atividades. Testes e inspeções afetam a PFD de algumas IPLs. O aumento do intervalo entre teste e inspeção pode aumentar a PFD da IPL.

Salvaguardas	Comentários
Manutenção	Em todas as avaliações de perigo assume-se perfeita execução desta atividade. Manutenção afeta a PFD de algumas IPLs.
Comunicações	É uma premissa básica que comunicações adequadas existam em uma instalação. Comunicações deficientes afetam a PFD de algumas IPLs.
Sinalização	Sinalizações não são IPLs por si mesmas. Estas podem estar confusas, mal localizadas, ignoradas, etc. Sinalizações podem afetar a PFD de algumas IPLs.
Sistema de Combate a Incêndio	Usualmente sistema de combate a incêndio não são consideradas como IPL, pois é um evento posterior para a maioria dos cenários e sua disponibilidade e efetividade pode ser comprometida pelo incêndio/explosão a ser contido.

2.7 SISTEMA DE GESTÃO

A norma ISO 14001 define um sistema de gestão de processo como “a parte do sistema de gestão global que inclui a estrutura organizacional, atividades de planejamento, responsabilidades, práticas, procedimentos, processos, e recursos para desenvolvimento, implantação, revisão e manutenção da política ambiental”.

A gestão da segurança de processo é uma parte do sistema de gestão global que inclui um conjunto abrangente de políticas, procedimentos e práticas com o objetivo de minimizar o risco de liberações de substâncias químicas perigosas.

O sistema de gestão de segurança de processo, também conhecido como PSM (do inglês, *Process Safety Management*), pode ter a garantia da sua efetividade seguindo o modelo *Plan-Do-Check-Act* (PDCA) muito utilizado em sistemas de gestão da qualidade que tem como princípio a melhoria contínua dos sistemas implementados seguindo quatro (4) etapas cronológica:

- a) *Plan* (Planejar): Nesta etapa se definem as metas e determinam os métodos para alcançá-las. É essencial o desenvolvimento de políticas escritas e procedimentos para definir o programa desejável (no caso, o PSM).
- b) *Do* (Executar/Fazer): Consiste em educar, treinar e executar o trabalho. Esta etapa é a fase onde os procedimentos e políticas são implementados.
- c) *Check* (Verificar/Checar): Nesta fase são verificados os efeitos do trabalho executado, ou seja, a avaliação das ações realizadas na etapa anterior,

- d) *Act* (Agir): Consiste na atuação no processo em função dos resultados. Realimentando e modificando os procedimentos e políticas, se necessário, através dos desvios avaliados.

O método de gerenciamento de processos a partir do PDCA pode ser ilustrado conforme Figura 2-13.

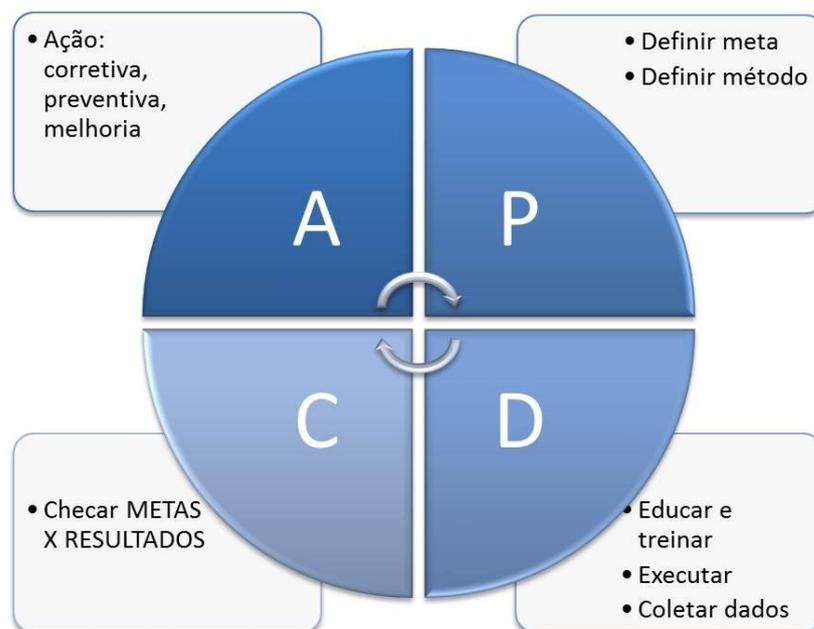


Figura 2-13– Método PDCA (Fonte: Falconi, 2002)

2.8 AUDITORIA

A auditoria é uma etapa fundamental para um efetivo programa de gestão da segurança de processo, pois tem o propósito de avaliar se os sistemas da empresa estão funcionando efetivamente, e sugerir ações corretivas quando identificados desvios que comprometem esses sistemas. Auditorias frequentemente revelam quais os elementos no sistema de gestão que não estão atingindo a intenção desejada.

A auditoria é um processo de avaliação sistemática e independente para verificar a integridade do item auditado e a sua conformidade estabelecida por normas ou diretrizes e é guiada pelo julgamento, experiência e a tendência do auditor.

No método PDCA, a auditoria está localizada na fase *Check*, a qual possui o objetivo de verificar as ações da fase anterior e dar subsídios para a etapa posterior através da proposição de ações corretivas.

A partir das auditorias pode-se verificar se as barreiras de segurança são suficientemente inspecionadas e mantidas.

2.9 BOW-TIE

Outra ferramenta que auxilia o sistema de gestão de uma empresa é a metodologia de *bow-tie*.

A metodologia de *bow-tie* permite a representação gráfica dos cenários acidentais, agregando uma perspectiva relacional entre evento, causas, consequências e barreiras, além de facilitar a visualização das possíveis ameaças e consequências associadas aos eventos de grande potencial de dano.

Em acordo com o exposto acima, Cockshott (2005), diz que esta metodologia permite que os gerentes, engenheiros, operadores e profissionais da manutenção tenham um fácil entendimento dos riscos a serem gerenciados no empreendimento. Uma das vantagens do *bow-tie* é que esta é de simples aplicação, transparente e de fácil manutenção pelos operadores da planta.

Duijm (2009) reforça que a importante vantagem neste diagrama comparado a outros métodos gráficos de análise de risco, primeiramente é a facilidade de suportar a comunicação com as partes interessadas (também conhecido como *stakeholders*) que não são especialistas no assunto e em segundo, o foco nos sistemas de segurança serve de base para a gestão e manutenção dos sistemas.

O *bow-tie* é aplicado para os cenários maiores da planta em questão. A identificação dos cenários maiores da planta podem ser determinados a partir de outras técnicas de análise de risco como a Análise de Perigo e Operabilidade - HAZOP (do inglês *Hazard and Operability Analysis*) e a Análise Preliminar de Perigos – APP. As melhores práticas e critérios para determinação dos cenários maiores envolvidos em uma planta de processo será abordada no capítulo 4.

Na sua representação, como apresentado na Figura 2-14, o evento topo está no centro da figura, com as ameaças à esquerda e as consequências à direita. Entre o evento topo e as ameaças estão as barreiras preventivas e entre o evento topo e as consequências são listadas as barreiras de recuperação ou mitigação.

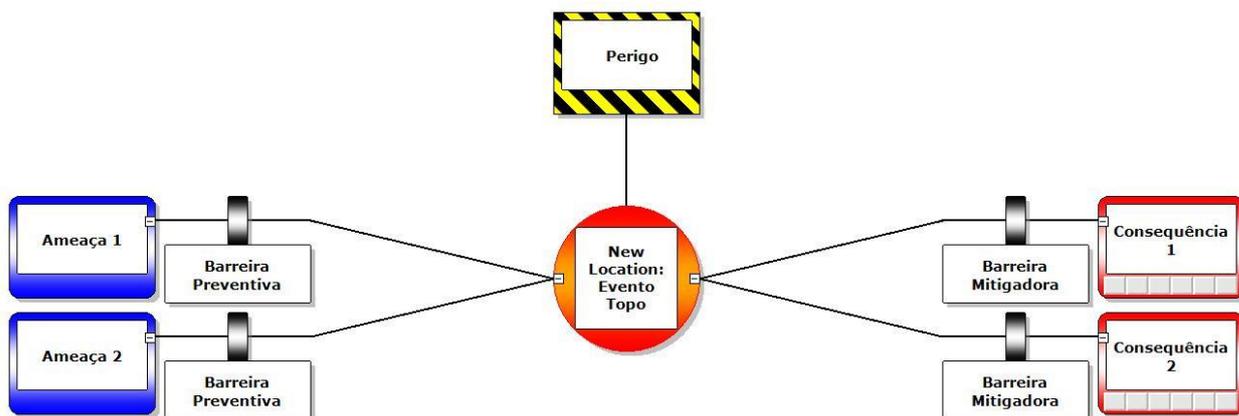


Figura 2-14– Exemplo de bow-tie

O Quadro 2-7 apresenta os campos indicados na Figura 2-14 do *bow-tie*.

Quadro 2-7 – Descrição dos campos do *bow-tie*.

Item	Descrição	Exemplos
Evento Topo	Primeiro evento na sequência de eventos não desejados	- Blowout, queda de objetos, explosão.
Ameaças	Condições que podem levar ao evento topo. Cada ameaça deve sozinha causar o evento topo.	- Falha de equipamento, erro humano, procedimento incorreto.
Barreiras Preventivas	Barreiras existentes no sistema que possam evitar as causas (ameaças)	- Projeto adequado - Procedimento para operação segura - Monitoramento de corrosão Inspeção - Proteção contra impacto
Consequências	Efeitos possíveis para pessoas, meio ambiente, ativos ou imagem da Empresa	- Fatalidade - Perda da unidade - Vazamento de hidrocarboneto para atmosfera
Barreiras Mitigadoras	Barreiras existentes que possam minimizar as consequências	- Detecção: visual, sistema de câmaras de TV Detecção de gás - Detecção de fumaça e fogo - Sistema de controle - Sistema de bloqueio (ESD, blowdown) - Sistema fixo de combate a emergências - Plano de resposta à emergência (escape,

Item	Descrição	Exemplos
		evacuação, resgate e recuperação)

O projeto ARAMIS, que estabelece uma metodologia para Avaliação de Risco de Acidentes para Indústrias orienta a utilização do bow-tie para o controle do risco e para avaliação do desempenho das barreiras de segurança.

Segundo Dianous (2006), esta metodologia, o ARAMIS, foi construída para ajudar as empresas a demonstrarem que têm um controle de risco suficiente em seu site.

A avaliação do desempenho das barreiras (tempo de resposta, eficiência e nível de confiança), conforme exposto no item 2.4, é realizada para validar que estes são relevantes para realizar a função de segurança esperada.

3 ACIDENTES QUE DEFINIRAM E DEFINEM A SEGURANÇA DE PROCESSO

Esta seção apresenta alguns acidentes que contribuíram para a definição de segurança de processo conforme citado por Aiche (2008) e Aiche (2012) através de lições aprendidas. Adicionalmente apresenta o acidente DeepWater Horizon, que representa o quanto ainda devemos aprender. Uma vez que acidentes não possuem causas singulares, conforme já citado nesta dissertação, os fatores que mais contribuíram para a ocorrência destes foram baseadas na opinião dos autores/especialistas.

Os acidentes descritos a seguir estão associados aos itens abordados neste trabalho como a identificação de perigos, liderança, plano de inspeção e de manutenção preventiva e no gerenciamento dos riscos.

3.1 DEEPWATER HORIZON (ESTADOS UNIDOS, 2010)

Segundo Bonfim, coordenador geral do centro de simulação aquaviária, a explosão na plataforma de perfuração Deepwater Horizon, de propriedade da empresa Transocean, deu início ao que é registrado como um dos mais graves acidentes do setor de Exploração e Produção de Petróleo.

Adicionalmente é considerado como o maior vazamento da história dos Estados Unidos, talvez mesmo um dos maiores a nível mundial.

3.1.1 Descrição do acidente

Numa noite de Abril/2010, um evento envolvendo técnicas e equipamentos de controle de poços permitiu que hidrocarbonetos escapassem de forma descontrolada do poço Macondo na direção da Plataforma Semi-submersível Deep Horizon, da Transocean. O resultado foram explosões, incêndio a bordo, 11 mortos e 17 feridos.

O incêndio continuou por 36 horas até que a plataforma afundou, enquanto que os hidrocarbonetos continuaram a vazar do reservatório através do poço e do equipamento de controle de poço (*Blowout Preventer* – BOP) por 87 dias, causando um derramamento de significância nacional. A *BP Exploration & Production Inc.* era a operadora da área que continha o poço Macondo.

O acidente envolveu uma falha de integridade do poço, seguida pela perda do seu controle hidrostático e por uma falha no controle do fluxo de hidrocarbonetos do poço pelo BOP. Esses hidrocarbonetos sofreram ignição já na plataforma, causando as explosões e incêndio na mesma, enquanto que o BOP foi incapaz de selar o poço, permitindo que o incêndio continuasse a ser alimentado pelos hidrocarbonetos provenientes do reservatório.

Durante a investigação realizada pelo time que a BP formou, foi utilizada a análise de árvore de causas para definir e avaliar vários cenários, modos de falha e possíveis contribuintes para o acidente. Nesta investigação foram identificados oito (8) pontos chaves para as causas do acidente que serão numerados abaixo:

1. A barreira formada pela cimentação da parede do poço não isolou de forma eficiente os hidrocarbonetos do reservatório;
2. As barreiras localizadas na sapata do revestimento de produção do poço não isolou de forma eficiente os hidrocarbonetos do reservatório;
3. O teste de pressão negativa realizado no poço foi aceito apesar de a integridade do poço como um todo não ter sido estabelecida;

4. O influxo de hidrocarbonetos (“Kick”) não foi identificado até o mesmo se encontrar na região do *Riser*;
5. As ações de controle de poço realizadas foram ineficazes na tentativa de recuperar o controle do poço;
6. Desvio dos hidrocarbonetos, através do separador de gás do fluido de completação, permitiu que os mesmos atingissem fontes de ignição na plataforma;
7. Os sistemas de detecção de gás e de incêndio não preveniram a ignição dos hidrocarbonetos;
8. O modo de Emergência do BOP falhou em selar o poço.

Dessa forma, não houve um fator único ou determinante para a sequência de eventos, mas o conjunto dos itens listados anteriormente, classificados como falhas mecânicas, julgamentos humanos, *design* de engenharia, implementação operacional e interface entre diferentes disciplinas que, juntos, permitiram e contribuíram para o acidente tomar as proporções que teve.

A Figura 3-1 ilustra de forma simples a escala de eventos e suas contribuições para o acidente, baseado no modelo do queijo suíço conforme apresentado no item 2.2.2. A Figura 3-2 ilustra o acidente da Deepwater Horizon.

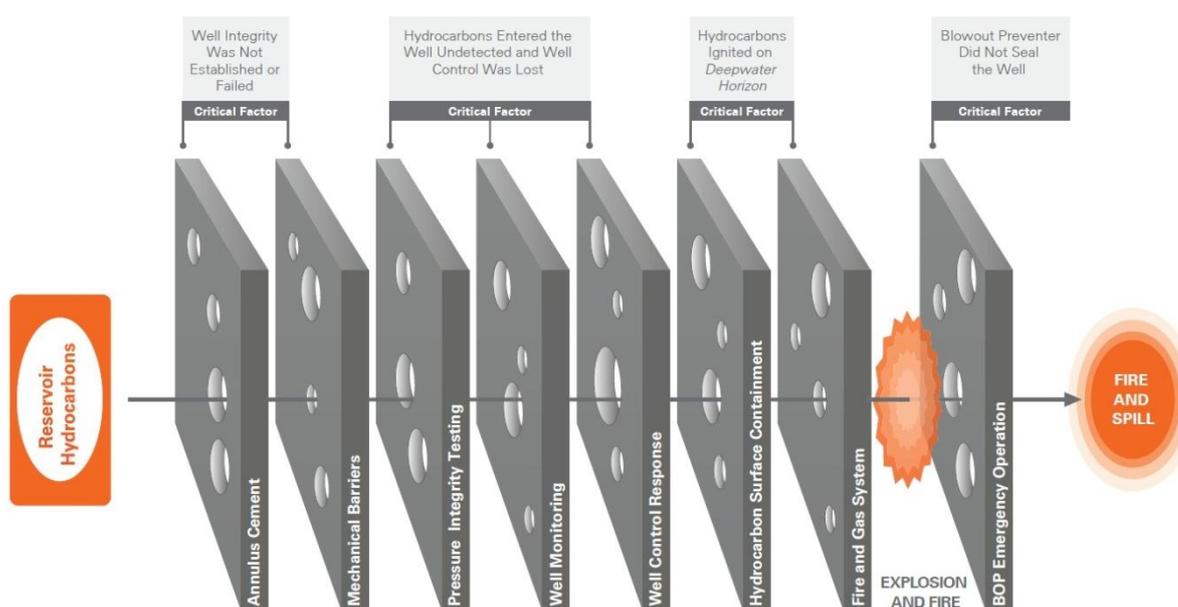


Figura 3-1– Relação das barreiras com os fatores críticos (Fonte: BP, 2010).



Figura 3-2– Acidente da Deepwater Horizon (Fonte: site BP, 2010).

3.1.2 Principais fatores para a ocorrência do acidente

Dentre as importantes causas subjacente listadas (TINMANN SVIK, et al,2011), as que ressaltam a importância do que será discutido neste trabalho são apresnetadas a seguir:

- a) Liderança não eficaz;
- b) Deficiência na comunicação;
- c) Falha no fornecimento de procedimentos oportunos;
- d) Treinamento e supervisão inadequados dos empregados;
- e) Falha em analisar e apreciar o risco adequadamente.

President Comission (2011), resalta que a maioria dos eventos e erros relacionados ao acidente deve-se a falhas no gerenciamento e na comunicação. Como exemplo este cita que a equipe de terra estava consciente dos riscos relacionados à cimentação do poço, porém não as destacaram aos trabalhadores que realizaram o teste de pressão negativa no poço. Adicionalmente este fato, evidencia a deficiência na comunicação, pois supervisores da BP não entraram em contato com especialistas em terra para relatar sobre os resultados encontrados.

O relatório *Chief Counsel* (2011), também identificou deficiências gerenciais incluindo a falha no fornecimento de procedimentos oportunos, treinamento e supervisão inadequada dos empregados. Ambas empresas, BP e Transocean, não possuíam procedimento interno e não providenciaram treinamento para conduzir e interpretar os resultados do teste de pressão negativa no poço. Para a equipe que realizou o relatório, a interpretação dos resultados do teste foi o maior contribuinte para o *blowout*.

Outro fator expressivo foi a falha em analisar e apreciar o risco adequadamente segundo o *President Commission* (2011). As causas imediatas do *blowout* de Macondo podem ser atribuídas a uma série de erros cometidos pela BP, Halliburton e Transocean que revelaram falhas sistemáticas no gerenciamento dos riscos, colocando em dúvida a cultura de segurança de toda a indústria. O sistema de gerenciamento da BP solicitou estudos de análise de risco separadamente durante a fase de planejamento do poço. Durante a fase de execução, decisões críticas foram feitas, porém não foi realizada formalmente nenhuma avaliação dos riscos após alterações. Ao mesmo tempo, para Oktad et al (2012) a tripulação tinha uma percepção de risco inadequado, pois achavam cientes de todos os perigos, enquanto provavelmente não eram capazes de manter a supervisão dos riscos.

Adicionalmente para Oktad et al (2012), a BP estava focada em tempo e custos ao invés de controle dos riscos de acidentes graves. A BP tomou uma série de decisões com prioridade sobre economia de tempo e custo. Até ao momento do acidente, a operação estava 38 dias atrasada e cerca de US \$ 58 milhões acima do orçamento. Isto pode explicar a falta de foco em assegurar a integridade do poço.

A matéria do jornal O Globo publicada em 26 de Setembro de 2012 (ORDONEZ, 2012), mostra que empresas da área de petróleo e gás vêm compartilhando experiências para avançar na segurança operacional e tomam como exemplo este acidente para evitar novos acidentes. Segundo Richard Morrison, vice presidente da BP, o acidente com a plataforma Deepwater Horizon fez uma grande diferença no mundo e que após o acidente buscam um melhor equilíbrio entre prevenção e técnicas de respostas.

3.2 PLATAFORMA P-36 DA PETROBRAS (BRASIL, 2001)

A plataforma P-36 naufragou em 20 de Março de 2001 com 11 vítimas fatais. A P-36 era uma plataforma semi-submersível com 4 colunas com terminação em dois flutuadores (*pontoons*) imersos na água conforme pode ser observado na Figura 3-3. As colunas e os flutuadores mantinham a flutuabilidade da plataforma adicionados aos tanques de lastro que sustentavam a profundidade requerida, maximizando sua estabilidade e minimizando os movimentos.

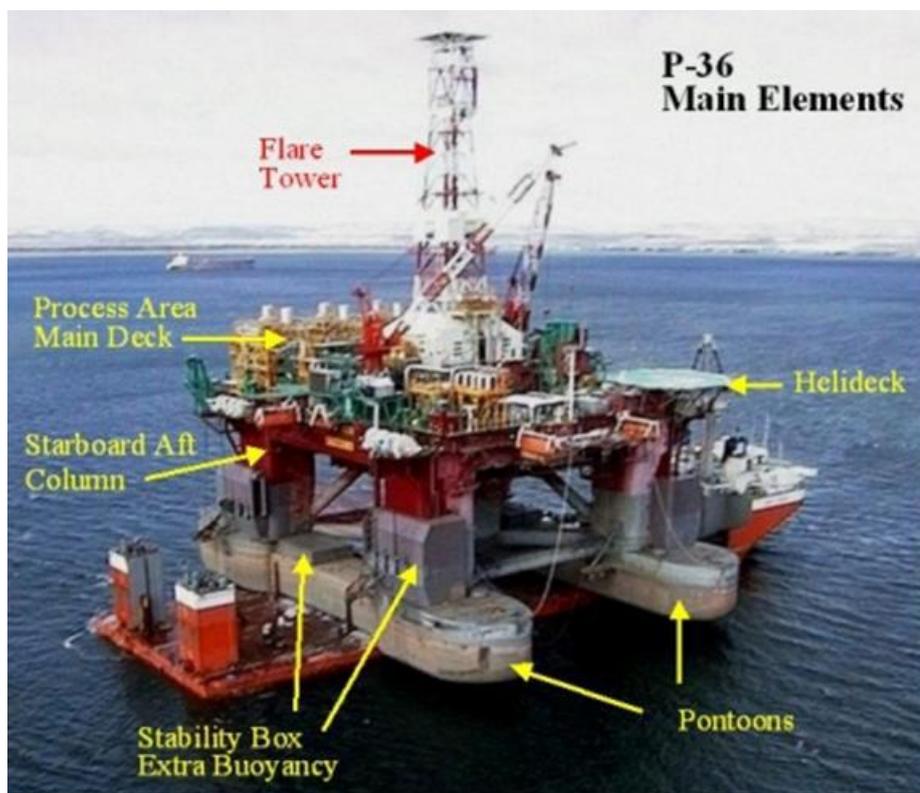


Figura 3-3–Plataforma P-36 (Fonte: ANP, 2001).

3.2.1 Descrição do acidente

A análise das causas mais prováveis do acidente, realizado pela Agência Nacional do Petróleo (ANP, 2001) em conjunto com a Marinha do Brasil, permitiu identificar o evento crítico como sendo a operação de esgotamento de água do tanque de drenagem de emergência da coluna de popa bombordo, iniciada no dia 14 de março de 2001. A água contaminada com resíduos oleosos presente no tanque seria bombeada para o manifolde (*header*) de produção da plataforma que recebe o fluxo de petróleo e gás natural proveniente dos poços produtores conforme

apresentado na Figura 3-4. Juntamente com produção de hidrocarbonetos, escoaria para a planta de processo. Entretanto, dificuldades operacionais para a partida da bomba de esgotamento desse tanque permitiram que houvesse fluxo reverso de óleo e gás pelas linhas de escoamento dos tanques e sua entrada no outro tanque (popa boreste) através de válvula presumivelmente danificada ou parcialmente aberta.

A bomba do tanque da popa boreste havia sido retirada para manutenção e o respiro do tanque bloqueado para evitar a entrada de água vindo da drenagem aberta, pois o tanque já se encontrava cheio.

A pressurização contínua deste tanque levou a seu rompimento mecânico cerca de duas horas após o início da operação de esgotamento do outro tanque, caracterizando o evento relatado como sendo a primeira explosão, ocorrido no dia 15 de março de 2001. Os fluidos do tanque rompido e de linhas e demais equipamentos também danificados passaram a ocupar o compartimento do quarto nível da coluna. Houve escapamento de gás para os conveses superiores através de aberturas nesse compartimento e por linhas de suspiro e ventilação rompidas. Cerca de 20 minutos após o rompimento do tanque, houve a explosão do gás que atingira a área do convés do tank top e segundo convés junto à coluna. Estava, assim, caracterizado o evento relatado como a ocorrência da segunda explosão, quando foram vitimadas onze pessoas da brigada de incêndio da plataforma.

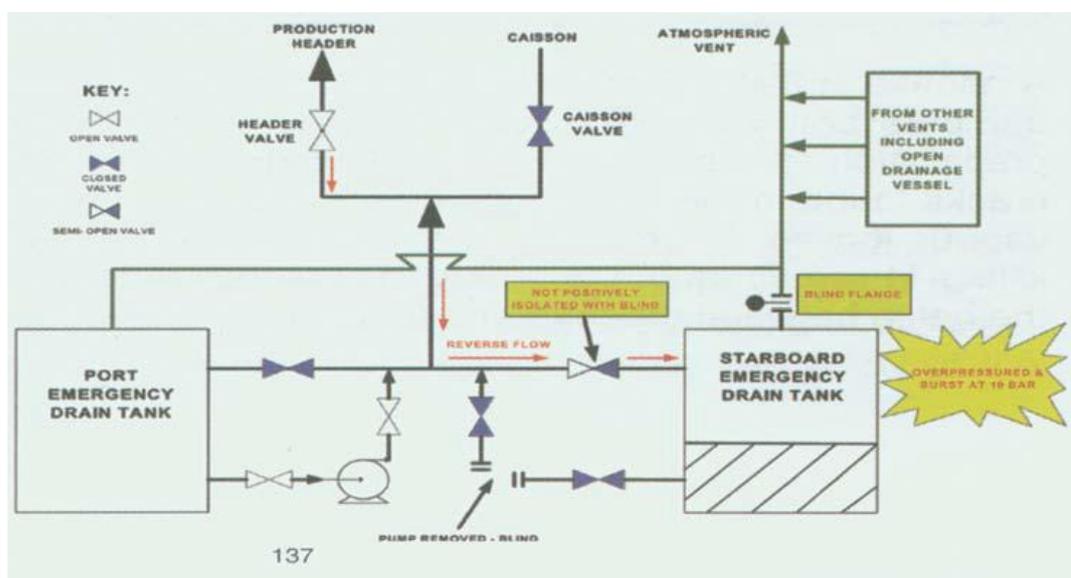


Figura 3-4– Esquemático do processo de drenagem de emergência da P-36 (Fonte: Aiche, 2008).

O colapso mecânico do tanque de drenagem de emergência de popa boreste, seguido imediatamente pelo rompimento da linha de recalque de água salgada que passava pelo quarto nível, iniciou o alagamento da coluna. A migração de água para a parte inferior da coluna se deu quando a água no compartimento do quarto nível atingiu os dampers do sistema de ventilação que deveriam fechar automaticamente; porém, devido à falha no funcionamento de seus atuadores, permitiram a passagem de fluidos.

A quantidade de líquido no interior da coluna e em parte do flutuador provocou o adernamento da plataforma que foi intensificado com a progressão da água para o tanque de lastro da coluna de popa boreste e para a caixa de estabilidade contígua. Esses espaços foram inundados porque as elipses de acesso aos mesmos haviam sido deixadas abertas desde o dia anterior ao acidente para possibilitar a inspeção do reparo de trinca verificada na caixa de estabilidade.

A submersão contínua foi intensificada pelo alagamento da coluna avariada, da inundação do tanque de lastro de popa boreste, da caixa de estabilidade contígua e da admissão deliberada de água de lastro nos tanques de proa bombordo.

Após o abandono da plataforma, foram efetuadas diversas tentativas de salvamento da unidade, particularmente a injeção de nitrogênio e ar comprimido nos compartimentos alagados para expulsão da água. Contudo, não houve êxito em manter a unidade estabilizada e sua submersão lenta e progressiva teve continuidade até às 11 h e 40 min do dia 20 de março quando afundou.

3.2.2 Principais fatores para a ocorrência do acidente

Segundo Aiche (2008), a Figura 3-5 apresenta que uma simples aplicação da técnica HAZOP teria identificado o potencial fluxo reverso do fluido de produção para os tanques de drenagem. Para os autores houve falha na identificação dos perigos. O respiro atmosférico do tanque só poderia estar fechado depois do tanque estar livre de hidrocarbonetos e com todas as conexões fechadas.

Para Aiche (2008), a localização do tanque contendo água contaminada dentro de um membro principal de suporte caracterizou este cenário com grande potencial de ocorrência. A natureza do tanque faz com que uma atmosfera inflamável seja

altamente provável e que se ignitado por qualquer meio, comprometeria a segurança da plataforma.

Outro item importante para a caracterização do acidente foi os dampers do sistema de ventilação e as elipses de acesso ao flutuador estarem abertas contrariando os procedimentos.

Uma das principais recomendações deste acidente foi a implementação de um programa de excelência operacional neste tipo de instalação. A Agência Nacional de Petróleo (ANP) recomendou que em futuros projetos que tanques ou equipamentos ligados ao processo não devem ser localizados dentro de das colunas de suporte ou dos flutuadores.



Figura 3-5– Acidente da Plataforma P-36 (Fonte: ANP, 2001).

3.3 REFINARIA TOSCO (ESTADOS UNIDOS, 1999)

A companhia de óleo Tosco operava a refinaria Avon na Califórnia até a década de 90. No final da década de 90, sérios acidentes ocorreram e contribuíram para a transferência de comando do empreendimento. Um desses acidentes catastróficos ocorreu em 23 de Setembro de 1999 durante a troca de uma tubulação conectada na coluna fracionadora de óleo.

3.3.1 Descrição do acidente

No dia 10 de Fevereiro de 1999, um vazamento foi descoberto na linha de nafta próxima a sua conexão com a coluna fracionadora de óleo. A equipe da refinaria respondeu imediatamente a ocorrência fechando 4 válvulas, isolando a linha. Porém o fechamento das válvulas não foi efetivo para sanar o vazamento. Inspeção da linha de nafta foi realizada e verificou-se que esta se encontrava com espessura fina e corroída. Durante os 13 dias entre a descoberta do vazamento e o incêndio, operadores realizaram inúmeros testes para isolar e drenar a linha de nafta. No entanto, supervisores da Tosco prosseguiram com o agendamento da substituição da linha que se encontrava aproximadamente a 46 metros de altura, enquanto a unidade estava em operação.



Figura 3-6– Acidente na Refinaria Tosco (Fonte: site CBS).

No dia do incidente, a linha continha, aproximadamente, 90 galões de nafta, pressurizada devido ao isolamento. Houve a permissão de trabalho para os funcionários drenar e remover a tubulação. Depois várias tentativas não bem sucedidas para drenar a linha, o supervisor direcionou os trabalhadores a realizar dois cortes na linha utilizando uma serra pneumática.

Depois de um segundo corte, começou a vaziar a nafta e o supervisor orientou os trabalhadores a abrirem um flange para drenar a linha. Como a linha estava sendo drenada, a nafta foi repentinamente libertada na extremidade aberta do primeiro corte. Houve vazamento de nafta na seção quente da coluna fracionadora, levando a ignição do produto, resultando no incêndio.

A chama atingiu 5 trabalhadores localizados em diferentes alturas na coluna. Neste acidente 4 pessoas morreram e 1 em estado grave.

3.3.2 Principais fatores para a ocorrência do acidente

Para Aiche (2012) este acidente é claramente um resultado de práticas não seguras de trabalho. A causa do vazamento e da corrosão foram relacionadas a mudanças nas condições operacionais um ano antes do acidente. A condição da linha deveria ter sido monitorada através de boas práticas de manutenção preventiva. Adicionalmente um plano de trabalho seguro deveria ter sido exigido para a parada da planta e purga da linha para a realização da manutenção. Há erros graves desde o planejamento à execução da manutenção.

A manutenção preventiva é um importante processo para assegurar a integridade mecânica durante a operação. Quando não se consegue assegurar a condição do equipamento ou realizar reparos de forma segura, a instalação ou partes deste devem ser parados.

Já para CBS (1999), os procedimentos de trabalho da Tosco não exigiam uma avaliação formal dos perigos para a substituição da linha de nafta. O trabalho de reparação foi classificado como manutenção de baixo risco. Apesar de perigos graves causados pela incapacidade de drenar e isolar a linha, conhecido por supervisores e trabalhadores durante a semana anterior ao o incidente, a classificação de baixo risco não foi reavaliada nem um plano de gestão foi formulado para controlar os perigos conhecidos.

Adicionalmente para CBS, a Tosco não fez o gerenciamento das mudanças para analisar os potenciais riscos relacionados às alterações realizadas no processo.

Memorandos e relatórios de incidentes da Tosco revelaram que administração reconhecia problemas operacionais e aumento da taxa de corrosão. No entanto, as ações corretivas foram não implementadas a tempo de evitar entupimentos e excessiva corrosão na tubulação de nafta.

3.4 FLIXBOROUGH (REINO UNIDO, 1974)

Segundo artigo de Pascon contido no site da empresa Processos – Soluções em Engenharia, Flixborough é um nome bastante conhecido para os profissionais da indústria química. Representa uma linha divisória na filosofia de segurança aplicada pelo setor. O inquérito que investigou este acidente foi um marco não só para o setor químico como outros setores industriais. Entretanto, para Pascon, apesar de já transcorridos 25 anos do acontecimento, suas lições ainda permanecem desconhecidas ou são negligenciadas em muitas empresas.

3.4.1 Descrição do acidente

A cerca de 16:53 horas no sábado 1 de Junho de 1974, o site da Nypro em Flixborough no Reino Unido foi severamente danificado por uma grande explosão. Vinte e oito trabalhadores foram mortos e mais de 36 feridos. Reconhece-se que o número de vítimas teria sido mais se o acidente tivesse ocorrido em um dia de semana. Consequências fora do site resultaram em cinquenta e três lesões relatadas. Propriedades na área circundante foram danificadas em graus variados.

Antes da explosão, em 27 de Março de 1974, descobriu-se um vazamento de ciclohexano por uma trinca no reator N°5. O vazamento pela trinca indicava que a parte interior de aço inoxidável no reator estava comprometida. Houve parada da planta para uma investigação. A investigação identificou que a trinca estava com extensão de 6 ft e foi tomada a decisão de removê-lo e instalar uma linha de *bypass* de 20" para conectar os reatores N°4 e N°6 para que a planta continuasse a produção. A operação foi retomada no dia 1° de abril. A linha de by-pass estava suspensa por suportes temporários que inicialmente asseguraram sua integridade. Porém foi observado um aumento no consumo de nitrogênio e no dia do acidente estava sendo investigado.

No dia 29 de Maio foi observado um vazamento na válvula de isolamento do fundo do reator e optaram por parar a planta para reparar o vazamento.

No dia seguinte, em 1 de Junho 1974, houve a partida da unidade. Segundo Less (1999) a sequência dos eventos é complexa e incerta. Houve descontrole da pressão nos reatores e falta de nitrogênio para iniciar a oxidação e verificou-se que o suprimento não chegaria até à meia-noite. O controle da pressão nos reatores poderiam ser realizada pela ventilação do *off-gas*, mas este procedimento envolveu a perda de quantidades consideráveis de nitrogênio. O relatório de Eyewitness indica que um acidente ocorreu 30 a 60 minutos antes da explosão. Não se sabe se esse acidente, um incêndio em uma linha próxima de 8", contribuiu o rompimento da linha de by-pass levando a liberação de ciclohexano. A liberação de ciclohexano formou uma nuvem inflamável que encontrou uma fonte de ignição e explodiu. A explosão causou grandes danos e começaram numerosos incêndios no local.

Não houve sobreviventes na sala de controle. Dezoito pessoas morreram devido à quebra das janelas e colapso do telhado.



Figura 3-7– Acidente de Flixborough (Fonte: AICHE, 2012).

3.4.2 Principais fatores para a ocorrência do acidente

Dentre os fatos críticos identificados na investigação deste acidente descritos por Aiche (2012), os que estão relacionados aos que serão analisados nesta dissertação foram:

a) Gerenciamento de mudanças inadequado

A trinca vertical no reator ocorreu devido a utilização de ácido nítrico para ajustar o pH da água para controlar vazamentos. Essa adição de ácido nítrico resultou em corrosão. A corrosão sob tensão de nitrato é um fenômeno conhecido pelos metalúrgicos.

Com isso, verifica-se que esta falha foi devido a não realização adequada do gerenciamento de mudanças.

Os vazamentos revelaram que algo não estava sob controle. A trinca foi a indicação que o gerenciamento de mudanças estava falho.

Revisões de segurança e engenharia deveriam ter ocorrido antes das modificações na instalação. Essas revisões deveriam ter rastreado e identificado se as mudanças propostas atendiam as condições do processo, métodos operacionais e de engenharia, segurança, condições ambientais engenharia de hardware e projeto.

b) Reconhecimento inadequado dos riscos do processo

Conforme dito anteriormente vazamentos frequentes de ciclohexano representavam um sinal de alerta. Vazamentos ocasionalmente resultam no *shutdown* do processo, porém por vezes não desencadeiam uma análise de completa de como evitá-los. Eles são eventos sérios, não aceitáveis e que requerem reconhecimento e ação preventiva. A instalação de uma linha de *bypass* contendo ciclohexano não teve devida atenção ao perigo que estava sendo imposto.

Todos trabalhadores devem ter consciência dos perigos associados a seu trabalho e capazes de determinar os riscos envolvidos em cada atividade. Neste acidente, os perigos não receberam a revisão adequada. O foco da revisão foi direcionada em como partir a planta e não como gerenciar as falhas do sistema.

c) A linha foi instalada sem teste de pressão, análise de stress ou inspeção inadequada

Para Aiche (2012), outro sinal de alerta para esse acidente foi a instalação da linha sem um teste de pressão hidrostático adequado. Uma revisão apropriada nas

condições normais e atípicas teria revelado que a linha de by-pass não estava projetada para o serviço. O teste hidrostático com a inspeção apropriada teriam indicado potenciais questões para o projeto. Este teste mostraria que a linha estava instável e inaceitável para a carga que seria aplicada. Não há cálculo de stress realizado ou métodos de proteções equivalentes provados. O cálculo realizado foi para provar que a linha tinha a capacidade para o fluxo requerido.

d) Procedimento operacional não robusto

Segundo Aiche (2012), os procedimentos operacionais não foram escritos com nível de detalhes adequados para os perigos impostos pela instalação. Estes procedimentos deveriam conter procedimento para shutdown e partida da planta e operadores deveriam ser treinados nestes procedimentos.

4 ROTEIRO E CRITÉRIOS PARA UMA BOA GESTÃO DAS BARREIRAS EXISTENTES

Este capítulo apresenta o roteiro e critérios para a gestão das barreiras de segurança existentes em uma instalação. Baseado no método PDCA, conforme apresentado no item 2.7 desta dissertação, a gestão das barreiras ocorre basicamente na etapa Check e consiste na identificação de cenários com severidade crítica e catastrófica e suas respectivas barreiras, planejamento e realização das auditorias, bem como a utilização da técnica de bow-tie para os cenários mais críticos a fim de clarificar o entendimento sobre esses cenários. Na etapa Act, portanto, são realizadas as ações corretivas para tratamento de problemas identificados na etapa Check.

4.1 IDENTIFICAÇÃO DOS CENÁRIOS

A identificação dos cenários acidentais é um elemento crítico, pois um perigo omitido é um perigo não analisado (AICHE, 2000).

O entendimento dos riscos impostos pelos perigos é essencial para se estabelecer um robusto sistema para gerenciar os perigos e seus riscos (AICHE, 2012).

Para tal entendimento, deve-se ter o conhecimento básico dos conceitos de perigo e risco.

Perigo é uma característica inerente do material, da condição física ou atividade que possui potencial de causar danos às pessoas, à propriedade ou ao meio ambiente.

Risco é definido como a combinação entre a probabilidade e consequência de ocorrência de um perigo acontecer.

Segundo o Manual de Orientação para a Elaboração de Estudos de Análise de Riscos da CETESB (P4.261, 2003), identificação de perigos é uma etapa a ser desenvolvida no estudo de análise de riscos.

A análise de risco pode ser realizada por um processo qualitativo ou quantitativo e possui o objetivo de avaliar a probabilidade e as potenciais consequências de um evento acontecer. A seleção das técnicas para a avaliação de riscos depende de diversos fatores, entre os quais: a complexidade do evento, a disponibilidade de tempo, a disponibilidades de especialistas e o interesse das partes interessadas.

Segundo a Cetesb em seu manual P4.261, homologado em 2003, ressalta que o estudo de análise e avaliação de riscos implementado durante o projeto inicial de uma instalação nova deve ser revisado periodicamente, de modo a serem identificadas novas situações de risco, possibilitando assim o aperfeiçoamento das operações realizadas, de modo a manter as instalações operando de acordo com os padrões de segurança requeridos.

Dentre as diversas técnicas que podem ser utilizadas para a identificação dos perigos, dentre as quais cabe mencionar:

- a) Listas de verificação (Checklist's);
- b) Análise "E se..." (What if...?);
- c) Análise Preliminar de Perigos (APP);
- d) Análise de Modos de Falhas e Efeitos (FMEA – *Failure Mode and Effets Analysis*);
- e) Análise de Perigos e Operabilidade (HazOp - *Hazard and Operability Analysis*).

Nesta dissertação a técnica que será abordada será a Análise Preliminar de Perigos (APP). E sta técnica é amplamente utilizada e referenciada em manuais para elaboração de estudos de análise de risco no Brasil como a Cetesb e o Instituto

Estadual do Ambiente do Rio de Janeiro (Inea). Adicionalmente esta técnica fornece todos os elementos para a análise das barreiras de segurança existentes.

4.1.1 Análise Preliminar de Perigos

A Análise Preliminar de Perigos é uma técnica que derivada do sistema de segurança militar dos Estados Unidos. (AICHE, 2008). Esta é uma técnica qualitativa que permite identificar os cenários de acidentes passíveis de ocorrer em um dado sistema, analisando suas causas e efeitos e buscando propor medidas para redução dos riscos do sistema.

A Análise Preliminar de Perigos se concentra de uma forma geral sobre os materiais perigosos e processo principal de uma planta.

Segundo Aiche (2008) ilustra um bom custo-benefício para identificar os riscos no início de uma vida da planta. Devido à sua herança militar, a técnica de Análise Preliminar de Risco é, por vezes utilizada para analisar as áreas de processo onde a energia pode ser liberada de forma descontrolada.

Esta metodologia pode ser usada para sistemas em início de desenvolvimento ou em fase de projeto e, também, como revisão geral de segurança de sistemas já em operação.

Na APP são levantadas as causas de cada um dos possíveis eventos acidentais e as suas respectivas consequências e, em seguida é feita uma avaliação qualitativa do risco associado a cada cenário acidental, avaliando a frequência de ocorrência do evento acidental, segundo suas causas e avaliando a severidade do cenário de acidente. Portanto, os resultados obtidos são qualitativos, não fornecendo estimativa numérica.

Adicionalmente, a APP é realizada por uma equipe multidisciplinar, composta pelas pessoas que participam das operações das atividades, o responsável pela segurança e os responsáveis pelas manutenções.

O desenvolvimento desta análise é realizado através de uma planilha estruturada conforme o modelo apresentado na Figura 4-1 e conforme a descrição a seguir:

Análise Preliminar de Perigos (APP)								
Empresa:				Sistema:			Data:	
Elaborado por:				Referência:				
Perigo	Causas	Efeitos	Salvaguardas	Freq	Sev	Risco	Observações / Recomendações	Cenário

Figura 4-1– Planilha APP (Fonte: Adaptado AICHE, 2008)

- a) 1ª Coluna: Perigo - Esta coluna contém os potenciais de danos identificados para o módulo que será estudado. De uma forma geral, estes perigos estão relacionados a eventos acidentais que têm potencial para causar danos às instalações, aos operadores, ao público e ao meio ambiente;
- b) 2ª Coluna: Causas - As causas de cada evento são discriminadas nesta coluna. Estas causas podem envolver tanto falhas intrínsecas de equipamentos (vazamentos, rupturas, falhas de instrumentação, etc.) como erros humanos de operação/manutenção;
- c) 3ª Coluna: Efeitos - Os possíveis efeitos danosos/consequências de cada situação identificada são listadas nessa coluna. São considerados tanto distúrbios operacionais, como perda de produto e interrupção da transferência ou parada da unidade, bem como efeitos que possam gerar incêndios, explosões ou danos ao homem, meio ambiente e instalações.
- d) 4ª Coluna: Salvaguardas - Nesta coluna são indicadas práticas padrão, assim como sistemas de proteção dos equipamentos (alarmes, intertravamentos e bloqueios), que atuem como fatores que indicam, detectam, atenuam ou impeçam a ocorrência de situações de risco.
- e) 5ª Coluna: Categorias de Frequência do Evento Acidental (Freq) - Um evento acidental é definido como o conjunto formado pela origem do acidente (perigo) e suas possíveis causas. Cada evento de acidente deve

ser classificado em categorias de frequência, as quais fornecem uma indicação qualitativa da frequência esperada de ocorrência para os eventos identificados. Uma sugestão de categorização da frequência do evento acidental é apresentada no Quadro 4-1.

Quadro 4-1 – Descrição categoria de frequência (Fonte: Haddad e Morgado, 2002)

Categoria	Denominação	Descrição
A	Extremamente Remota	Conceitualmente possível, mas extremamente improvável de ocorrer durante a vida útil do Processo/instalação
B	Remota	Não esperado ocorrer durante a vida útil do Processo/instalação
C	Improvável	Pouco provável de ocorrer durante a vida útil do Processo/instalação.
D	Provável	Esperado ocorrer até uma vez durante a vida útil do Processo/instalação
E	Frequente	Esperado ocorrer várias vezes durante a vida útil do Processo/instalação

- f) 6ª Coluna: Categoria de Severidade do Evento Acidental (Sev) - Os cenários de acidente são classificados em categorias de severidade, as quais fornecem uma indicação qualitativa do grau de severidade das consequências de cada um dos cenários identificados (composto pelo evento acidental e possíveis desdobramentos). Uma sugestão de categorização da severidade do evento acidental é apresentada no Quadro 4-2.

Quadro 4-2 – Descrição categoria de severidade (Fonte: Haddad e Morgado, 2002)

Categoria	Denominação	Descrição
I	Desprezível	<ul style="list-style-type: none"> - Sem danos ou danos insignificantes aos equipamentos, à propriedade e/ou ao meio ambiente; - Não ocorrem lesões/mortes de funcionários, de terceiros (Não funcionários) e/ou pessoas (indústrias e comunidade); o máximo que pode ocorrer são casos de primeiros socorros ou tratamento médico menor.
II	Marginal	<ul style="list-style-type: none"> - Danos leves aos equipamentos, à propriedade e/ou ao meio ambiente (os danos materiais são controláveis e/ou de baixo custo de reparo); - Lesões leves em funcionários, terceiros e/ou em pessoas.
III	Crítica	<ul style="list-style-type: none"> - Danos severos aos equipamentos, à propriedade e/ou ao meio ambiente; - Lesões de gravidade moderada em funcionários, em terceiros e/ou em pessoas (probabilidade remota de morte de funcionários e/ou de terceiros); - Exige ações corretivas imediatas para evitar seu desdobramento em catástrofe.
IV	Catastrófica	<ul style="list-style-type: none"> - Danos irreparáveis aos equipamentos, à propriedade e/ou ao meio ambiente (reparação lenta ou impossível); - Provoca mortes ou lesões graves em várias pessoas (em funcionários, em terceiros e/ou em pessoas).

g) 7ª Coluna: Categoria de Risco - Combinando-se as categorias de frequência com as de severidade obtém-se o risco baseada em uma Matriz de Riscos. De acordo com a Matriz apresentada no Quadro 4-3, os cenários da região em verde encontram-se numa região de risco baixo (soluções necessárias a longo prazo), a região em amarelo indica cenários de acidente cujo risco é moderado (soluções necessárias a médio prazo) e em vermelho estão os cenários considerados de risco alto (soluções imediatas).

Quadro 4-3 – Matriz de Risco (Fonte: Haddad e Morgado, 2002)

		Frequência				
		A	B	C	D	E
Consequência	IV	2	3	4	5	5
	III	1	2	3	4	5
	II	1	1	2	3	4
	I	1	1	1	2	3

Severidade	Frequência	Risco
I - Desprezível	A - Extremamente Remota	1 - Desprezível
II - Marginal	B - Remota	2 - Menor
III - Crítica	C- Improvável	3 - Moderado
IV - Catastrófica	D - Provável	4 - Sério
	E - Frequente	5 - Crítico

- h) 8ª coluna: Recomendações/Observações - Esta coluna contém as recomendações que visam a melhoria da condição de segurança, a minimização dos efeitos dos possíveis acidentes ou observações pertinentes ao cenário em estudo.
- i) 9ª coluna: Cenário - Esta coluna contém um número de identificação do cenário de acidente, sendo preenchida sequencialmente para facilitar a consulta a qualquer cenário de interesse.

4.1.2 Seleção dos cenários

Além dos aspectos técnicos acima mencionados, a análise de risco, é um elemento fundamental no conhecimento dos riscos, de suas barreiras e de toda gestão de Segurança de Processo. Sem uma sistemática efetiva de análise dos riscos em seus diversos níveis de complexidade e metodologias, não se consegue evoluir eficientemente na Segurança de Processo, muito menos no conhecimento e gestão das barreiras de proteção dos cenários.

Para a seleção dos maiores cenários acidentais escolhem-se aqueles que foram classificados com as maiores categorias de severidade, caso de utilização do Quadro 4-2, os cenários que foram classificados com as categorias crítica e catastrófica na APP. Para esta análise é importante que a seleção dos cenários acidentais seja baseada na severidade e não no risco. Como este último é baseado

na combinação de uma frequência de ocorrência e sua possível consequência, o cenário com grande potencial de dano pode ter seu risco reduzido pela baixa frequência a ele associada podendo ser desconsiderado da análise.

A escolha dos cenários pela severidade viabiliza a identificação dos cenários de maior relevância em termos de consequência às pessoas, meio ambiente e a instalação, os quais são prioridades no sistema de gerenciamento.

O foco desta etapa consiste em entender e selecionar os principais cenários/perigos (*Major Accident Hazards*) no empreendimento a ser analisado. A partir desta seleção, a próxima etapa consiste na identificação de seus mecanismos de controle, ou seja, suas barreiras de proteção.

4.2 IDENTIFICAÇÃO DAS BARREIRAS DE SEGURANÇA PARA CADA CENÁRIO SELECIONADO

Para cada cenário selecionado na etapa anterior verificam-se todas as barreiras de proteção (preventivas ou mitigatórias), no exemplo desta dissertação, a 4ª coluna da planilha de APP (salvaguarda) ou em outros estudos de análise de risco realizado para o empreendimento. Adicionalmente verificam-se todas as recomendações realizadas durante a análise de riscos para o cenário identificado.

Todas as barreiras identificadas, preventivas ou mitigadoras, deverão ser validadas pelo responsável de cada planta de processo do empreendimento.

4.3 VERIFICAÇÃO DA INTEGRIDADE DAS BARREIRAS DE SEGURANÇA IDENTIFICADAS PELO PROCESSO DE AUDITORIA

A integridade de uma barreira está relacionada ao desempenho desta à função que se destina. Em relação à integridade, uma barreira pode ser classificada em íntegra ou degradada. Uma barreira com bom desempenho está relacionada à sua manutenção dentro dos padrões esperados, os quais são atingidos através do cumprimento de práticas de inspeção, manutenção, auditorias dentre outros (BARDY et al, 2012b).

Uma barreira é considerada íntegra quando se encontra efetiva no desempenho de sua função e degradada quando está abaixo dos padrões esperados, logo poderá não ser efetiva no desempenho de sua função quando demandada.

É importante ressaltar que caso uma barreira falhe, não necessariamente indica que a mesma está degradada, pois cada barreira possui uma taxa de falha intrínseca. Um dos fatores que pode levar a degradação é, por exemplo, o não cumprimento dos planos de manutenção e inspeção.

A verificação da integridade das barreiras de segurança pode ser realizada pela metodologia de auditoria. Segundo Bardy (2012a), além de verificar o status das barreiras de segurança dos maiores cenários para a planta em análise, o resultado da auditoria de barreiras auxilia a alta gestão:

- a) na visão integrada do sistema de gestão e dos fatores que podem reduzir perdas;
- b) definir e acompanhar os indicadores de processo;
- c) o compromisso dos líderes e trabalhadores com a segurança de processo;
- d) verificação do nível de implementação de princípios e políticas da segurança de processo na instalação;
- e) no desenvolvimento de uma cultura de segurança de processo.

Adicionalmente, como resultante da auditoria, uma lista de recomendações para as barreiras analisadas como degradadas é elaborada com o objetivo de melhorar suas condições para que estas possam vir a ser consideradas como íntegras.

Para a identificação do status das barreiras através da auditoria, uma equipe multidisciplinar é consultada envolvendo especialistas das áreas de engenharia de processo, operação, manutenção, instrumentação e segurança.

Conforme citado anteriormente, para cada cenário selecionado, as barreiras preventivas e mitigadoras são validadas pelo responsável da área. Após essa validação as barreiras são divididas por disciplina em que estas são geridas para facilitar a análise. O Quadro 4-4 apresenta um exemplo de divisão da equipe responsável por cada barreira a ser analisada.

Quadro 4-4 – Áreas responsáveis pela gestão das barreiras

Área Responsável	Barreiras
Inspeção	Programas de inspeção e manutenção em linhas, equipamentos e acessórios. Sistema de alívio para equipamentos e linhas pressurizadas.
Instrumentação	Programa de testes de instrumentos e equipamentos de segurança. Alarme de segurança em sistemas de operação. Função Instrumentada de Segurança – Intertravamentos. Sistema de controle (Pressão, Temperatura, Nível, etc.). Válvulas de bloqueio (com acionamento manual ou remoto).
Operação	Programas de treinamentos em operação e procedimentos críticos. Procedimentos operacionais e de manutenção. Detectores de gases. Área de carregamento/descarregamento de carretas/caminhões. Câmeras de vídeo. Botoeira de emergência.
Civil	Proteção/Pavimentação do solo Canaletas para tratamento ou substituição das pluviais. Diques de contenção. Sistema de canaletas cercando ruas e áreas de processo.
Segurança	Preservação do sistema de combate a incêndio, e operação do sistema. Plano de Ação de Emergência. Verificação dos status das recomendações realizadas durante estudos de análise de risco
Manutenção	Programas de manutenção em equipamentos rotativos.

Após a divisão das barreiras por disciplina, as barreiras são auditadas baseadas em um protocolo desenvolvido especificamente para a mesma visando avaliar sua integridade, item este que será abordado a seguir nesta dissertação.

Além dos protocolos a serem preenchidos, as recomendações dos estudos de análise de risco existentes também devem ser verificadas durante a auditoria. Em caso de não atendimento, deve-se verificar se há registros de justificativa ou se foram substituídas/modificadas através de recomendações que garantam um nível de segurança semelhante. Uma vez que, de acordo com boas práticas aplicadas para Gerenciamento de Risco, todas as recomendações geradas devem ser acompanhadas ou justificadas formalmente em caso da não implementação das mesmas.

4.3.1 Protocolos

Conforme mencionado acima, para auxiliar no processo da auditoria das barreiras, utilizam-se os protocolos.

O protocolo define o escopo da auditoria e fornece estrutura e orientação para a equipe de auditores (AICHE, 2012).

Aiche (2012) ainda expõe que a equipe de auditores deve utilizar diversos métodos para medir a conformidade da barreira analisada. Este deve incluir uma inspeção detalhada das políticas e procedimentos, verificação através da inspeção dos documentos registrados e validação através de entrevistas com a equipe da instalação, ou seja, se basear em evidências.

Com isso cada tipo de barreira de proteção deve possuir um modelo de protocolo correspondente à sua função com questões e/ou critérios usados para coletar evidências necessárias para chegar a conclusões acerca do *status* dos elementos auditados.

Conforme exposto acima, cada protocolo deverá conter uma série de questões de forma sistemática, na qual orienta o auditor a perguntar sobre a situação atual em que a barreira se encontra. Caso nesta etapa, a barreira seja identificada como degradada, sugestões, ações e recomendações para alcançar a integridade desejada deverão ser elaboradas pela equipe presente na auditoria.

Nos casos em que a barreira estiver com ao menos um quesito não atendido, a mesma será considerada como “Degradada”. Caso todos os itens estejam atendidos, a barreira será considerada como “Íntegra”.

Um exemplo de itens que devem ser avaliados durante a auditoria para um sistema instrumentado de segurança encontra-se na Figura 4-2.

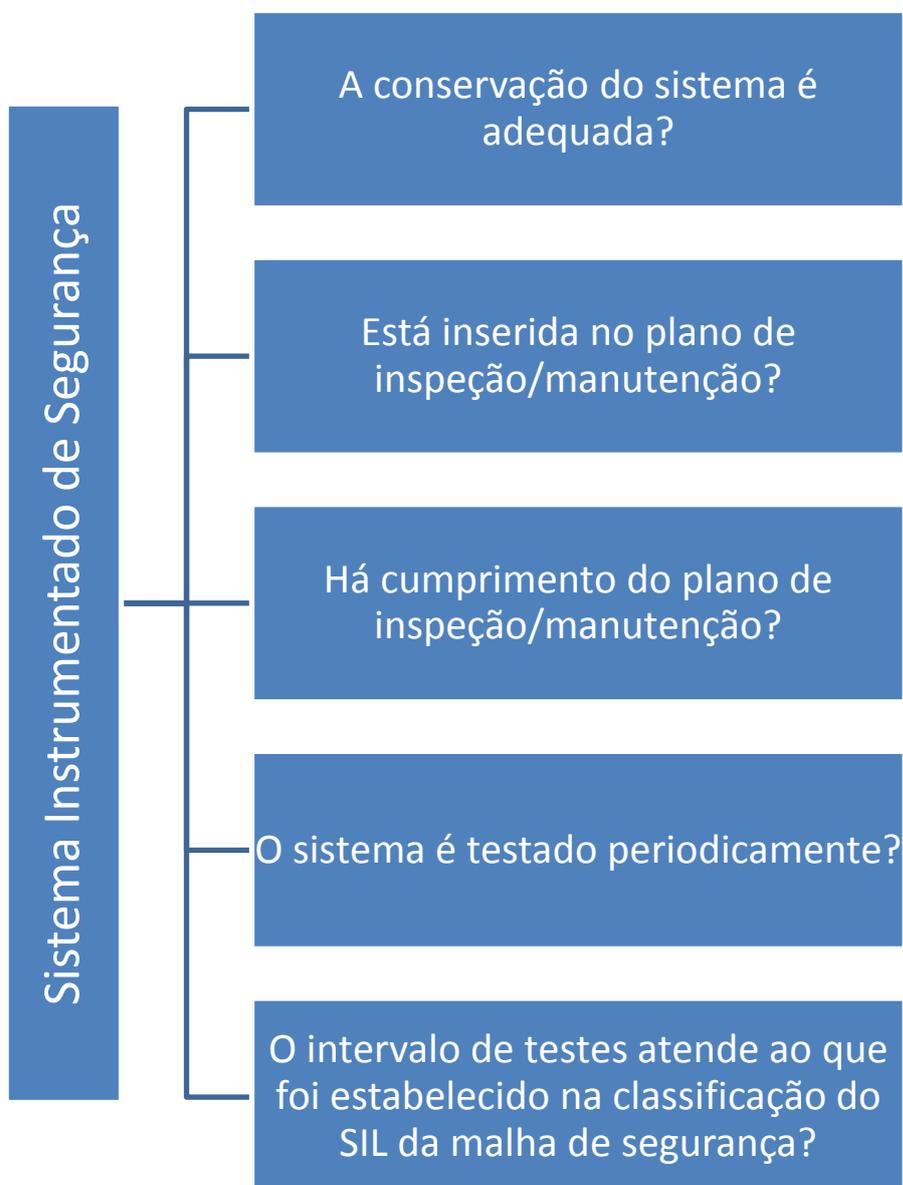


Figura 4-2– Exemplo de itens a serem avaliados em sistemas instrumentados de segurança.

Os itens a serem avaliados em cada protocolo devem ser elaborados baseados em normas nacionais e internacionais, boas práticas e a expertise da equipe.

4.3.2 Verificação da criticidade das barreiras de segurança identificadas

Outro fator que pode ser avaliado durante a auditoria é a classificação das barreiras quanto a sua criticidade (crítica ou não-crítica). Esta classificação, baseado na expertise da equipe da instalação, visa identificar as barreiras mais importantes

para os cenários avaliados facilitando a priorização de ações necessárias para mantê-las íntegras.

Adicionalmente a barreira pode ser classificada em barreiras principais ou secundárias.

Segundo Bardy et al (2012b), uma barreira principal é classificada como crítica quando esta é capaz de atuar diretamente impedindo a ocorrência do evento, no caso das barreiras preventivas, ou impedindo o desdobramento do evento nas consequências possíveis (barreiras mitigadoras).

A barreira principal também pode ser classificada como não críticas, ou seja, aquelas que não são suficientes para impedir a ocorrência necessitando de barreiras adicionais. Porém estas ajudam a reduzir a ocorrência do evento ou minimizar seus impactos.

Já as barreiras secundárias, relacionadas a um fator de escalonamento de uma barreira principal, seguem o mesmo critério para determinação de sua criticidade. Esta é avaliada quanto à manutenção da barreira principal a qual ela está relacionada e não ao evento ou suas consequências como adotado para as barreiras principais, conforme descrito acima.

Através deste critério, as barreiras críticas são prioridades frente a barreiras não críticas e com isso os gestores conseguem verificar quais barreiras devem ser priorizadas caso estejam degradadas.

4.4 BOW-TIE

A partir dos resultados da auditoria, um bow-tie pode ser construído para os cenários mais críticos analisados. É válido lembrar que o bow-tie é uma ferramenta que agrega uma perspectiva relacional entre evento, causas, consequências e barreiras, além de facilitar a visualização das possíveis ameaças e consequências associadas aos eventos de grande potencial de dano.

Baseado nos itens 4.3 e 4.4, a Figura 4-3 apresenta um exemplo de representação no bow-tie da integridade das barreiras onde a cor vermelha representa que a barreira está degradada e cor verde representa a integridade da barreira. Adicionalmente pode-se verificar a classificação das barreiras em críticas e não-críticas representados na Figura 4-3 por CRI e NÃO-CRI respectivamente.



Figura 4-3– Representação de Criticidade e Integridade no diagrama de bow-tie (Fonte: Bardy et al, 2012b).

A Figura 4-4 apresenta um exemplo de um bow-tie resultante da aplicação dos itens mencionados acima para uma estocagem de etileno em uma planta de processo. Esta Figura 4-4 apresenta graficamente as barreiras preventivas e mitigatórias para o evento de liberação de gás inflamável com a classificação quanto a criticidade e integridade.

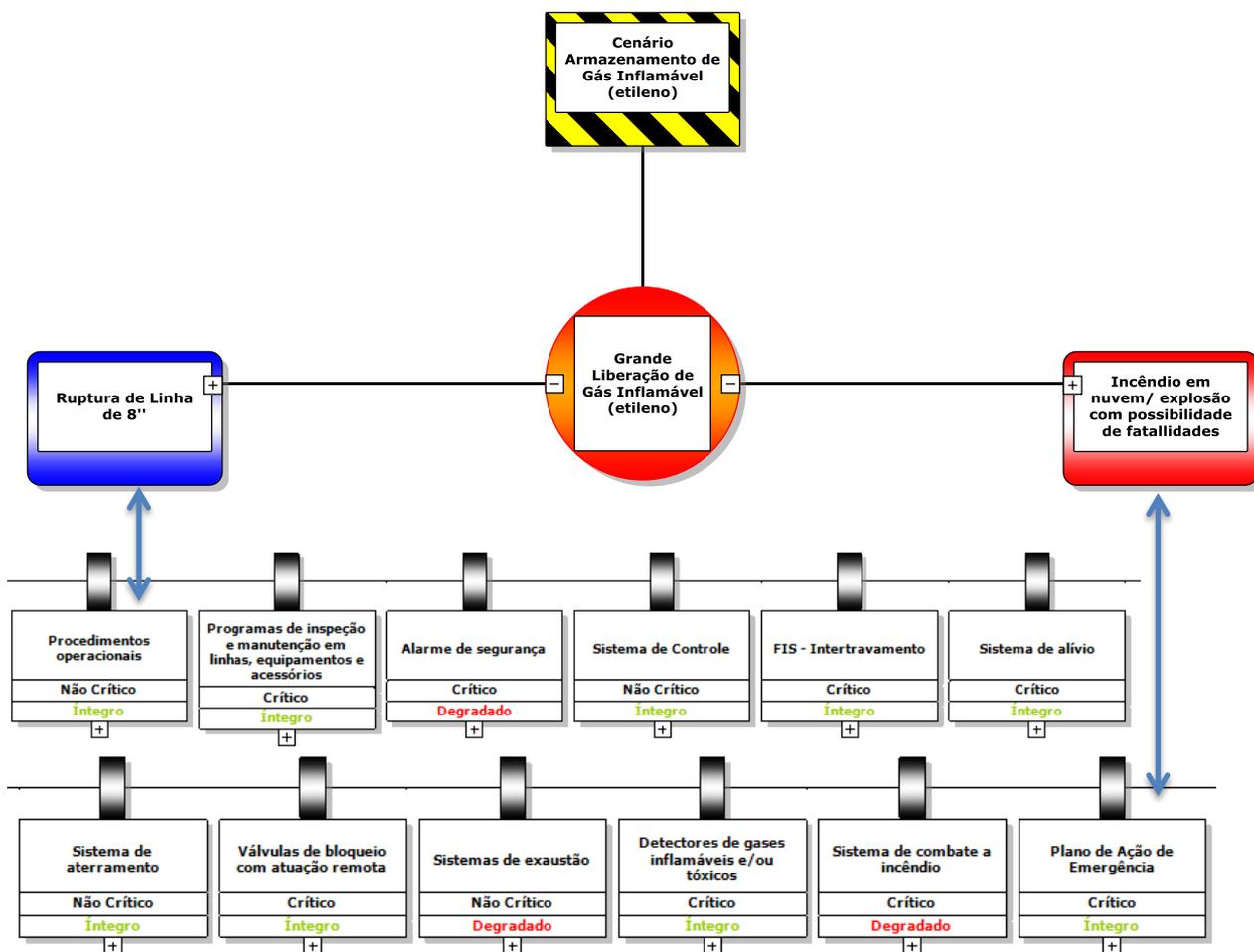


Figura 4-4– Bow-tie para o cenário de liberação de gás inflamável.

4.5 TRATAMENTO DE NÃO CONFORMIDADES

Um elemento essencial de qualquer programa de gestão é o monitoramento do que existe da perspectiva de sua performance futura. Portanto, para a melhoria contínua do desempenho em segurança de processo, é importante o estabelecimento de indicadores e a definição da estrutura de governança para seu monitoramento. Tal como para qualquer dimensão sistêmica, o monitoramento da gestão das barreiras de proteção dos principais cenários de acidente de processo é também crucial.

Com isso, não basta identificar o problema, um plano de ação deve ser realizado para a melhoria contínua da instalação.

Este plano de ação deve ser baseado nos cenários de maiores risco para a instalação com os resultados da auditoria realizada. Conforme citado no capítulo

anterior, recomendações durante a auditoria são elaboradas com a finalidade de melhorar as condições operacionais e de segurança em uma instalação. Adicionalmente as recomendações dos estudos de análise de risco não atendidas ou não justificadas também devem ser contemplados no plano de ação.

Quando auditorias subsequentes apontam repetidas resultados de auditorias anteriores ou mesmos pontos de melhoria, isto pode representar um sinal na deficiência no progresso inadequado dos resultados da auditoria ou inapropriado acompanhamento e monitoramento do sistema.

Quando as recomendações de estudos de análise de risco não estiverem atendidas/justificadas ou resultado de auditorias apresentarem repetidas não conformidades, segundo Aiche (2012), perguntas devem ser feitas a fim de determinar a importância deste “sinal de alerta”.

- a) Porque esta não conformidade ainda está aberta?
- b) Existe algum plano de ação desenvolvido para essa não conformidade?
- c) A instalação está rastreando o progresso do plano de ação regularmente?
- d) O plano de ação está sendo priorizado?
- e) A gestão sênior local (ou e se aplicável, o corporativo) conhece e suporta o plano de ação?
- f) Qual será a possível consequência caso esta não conformidade não ser solucionada em tempo hábil?

O monitoramento e gerenciamento do plano de ação são usualmente de responsabilidade da instalação.

A responsabilidade para o desempenho da segurança de processo repousa sobre o gerente sênior/gestores do negócio ou da instalação. Tal responsabilidade requer uma avaliação de desempenho eficaz.

Membros da alta gestão, ou pessoas qualificadas delegadas pelos mesmos, devem participar da reunião de fechamento da auditoria para entender e conhecer o status da segurança de processo no âmbito do comprometimento das barreiras de segurança da instalação em análise.

Cópias do relatório de auditoria devem ser enviadas aos gestores a fim dos mesmos terem a oportunidade de responder a perguntas relacionadas com os resultados.

Adicionalmente deve-se verificar se a instalação tem recursos para atender os resultados de forma adequada e eficiente.

Para instalações com múltiplas instalações e linhas de negócios diferentes com gerência executiva associadas, podem elaborar uma estrutura para o monitoramento do status das barreiras e da implementação das recomendações oriundas das auditorias/analises de risco. Esta pode ser dividida para os diferentes níveis de liderança onde o maior nível hierárquico, por exemplo uma gerência executiva, fique responsável pelo monitoramento dos 10 maiores cenários de todo o empreendimento, a alta gerência da empresa responsável pelos 5 maiores cenários de cada planta e a planta com todos os seus cenários de maior risco.

5 BOAS PRÁTICAS PARA GESTÃO DAS BARREIRAS DE SEGURANÇA

Este capítulo visa identificar pontos importantes a serem seguidos durante todo o processo que envolve a gestão das barreiras de segurança dos maiores cenários da instalação. Boas práticas relacionadas aos itens descritos no capítulo anterior e ferramentas que auxiliam na gestão das barreiras serão expostas neste item como se segue:

- a) Auditoria
- b) Integridade dos Ativos
- c) Gerenciamento dos Riscos
- d) Cultura de segurança

Essas boas práticas foram baseadas em vivências de campo para estudos de gestão de barreiras em empresas da área petroquímica e de óleo e gás em conjunto com o livro do Aiche, *Recognizing Catastrophic Incident Warning Signs in the Process Industries*, 2012.

5.1 AUDITORIA

Durante a auditoria, algumas dicas são importantes para que o resultado deste processo seja eficaz.

Um efetivo programa de auditoria é uma das melhores defesas contra a complacência. No entanto, um programa de auditoria ineficaz pode desperdiçar

recursos valiosos e produzir informação enganosa, podendo assim sugerir que a instalação é/está melhor do que seu *status* atual.

5.1.1 Pré-auditoria

Antes da realização da auditoria, é grande importância que os auditores passem por um treinamento para a uniformização dos conceitos e métodos que serão abordados durante a auditoria. Após o treinamento, os auditores devem:

- a) Ter o conhecimento básico do processo da instalação que será analisada;
- b) Conhecer as políticas, elementos estratégicos em termos da segurança de processo bem como a estrutura organizacional da empresa;
- c) Ter o mesmo entendimento em relação às perguntas elaboradas em cada protocolo;
- d) Ter o conhecimento para o preenchimento dos protocolos de maneira uniforme. Este item pode ser sanado através da elaboração de um guia de preenchimento o qual deverá ser fornecido pela empresa.

Adicionalmente, caso da metodologia de auditorias de barreiras já esteja implementada na empresa, é válido realizar uma revisão nos protocolos e itens a serem avaliados durante este processo, pois procedimentos podem ter sido alterados e/ou novas condutas definidas pela empresa.

5.1.2 Durante auditoria

Caso durante a auditoria se verifique que resultados de auditorias anteriores ainda estão em aberto, deve-se investigar o motivo pela qual a mesma não está finalizada. Há uma significativa diferença entre ações incompletas no plano de ação que está sendo priorizada e ter recursos alocados para completar a ação baseado na avaliação do risco com um resultado de auditoria o qual não tem um plano definido.

5.1.3 Resultados da auditoria

Geralmente, na maioria das organizações, o corporativo está mais envolvido em monitorar o progresso do plano de ações a completar e reportar o progresso para os gerentes da organização. Porém, todos os envolvidos na auditoria, desde os auditores ao gerente da planta devem ter a consciência de como monitorar a ação e

acompanhar o progresso dos resultados. Surpresas nestas funções são raramente produtivas.

Quando resultados da auditoria e subsequente acompanhamento e monitoramento do desempenho não são revisados com os gerentes responsáveis, dois fatores podem ter sido determinante para tal fato:

- a) Falha no sistema de gestão da empresa;
- b) Ou a falta de compromisso e importância dos gestores com os resultados da auditoria.

Itens esses que devem ser rastreados e verificados, pois representam uma importante lacuna no sistema de gestão da segurança de processo.

Adicionalmente outro fator de grande relevância para a gestão das barreiras são que os resultados/relatórios da auditoria não estejam somente disponíveis para os gestores. Todos os funcionários envolvidos no processo tem o direito de saber o *status* do desempenho da organização para qual ele trabalha. Os resultados da auditoria podem motivar os empregados a participar/ajudar propondo soluções no gerenciamento das atividades do sistema.

Para organizações com diversos sites e localidades diferentes, é importante que os resultados da auditoria sejam divulgados a todos, pois permite que melhores práticas e lições aprendidas possam ser compartilhadas.

Organizações com diversos sites e áreas de negócios diferentes possuem riscos e processos específicos. O esforço em se atingir um programa de segurança de processo sustentável para organizações deste porte é grande, pois padrões e orientações a serem cumpridas podem ser muito abrangentes e ambiciosas para todos os sites. Embora a maioria dos programas de segurança de processo geralmente possui o mesmo objetivo, o ideal é que os programas tenham adaptações para riscos específicos e necessidades para cada site.

Para finalizar, quando a auditoria encontra resultados negativos, pode acontecer explicitamente, pelos gerentes da instalação, que estes resultados sejam amenizados ou até mesmo retirados do relatório preliminar da auditoria. Por vezes, quando a auditoria realizada é externa, os auditores com a intenção de manter a relação com a organização, podem tender a concordar com esta demanda. Não importa a influência ou a razão, auditores não devem alterar suas impressões a

menos que tenha esquecido uma evidência ou novas evidências são fornecidas durante a revisão do relatório preliminar da auditoria que suporte a alteração dos resultados iniciais.

5.2 INTEGRIDADE DOS ATIVOS

A integridade de ativos e a confiabilidade dos equipamentos são atividades de implementação sistemática que vão desde o projeto até a operação em uma instalação. Essas atividades auxiliam a garantir que o equipamento estará seguro e confiável durante sua operação. O objetivo primário da integridade de ativos é o desempenho confiável dos equipamentos para a contenção segura, prevenção ou mitigação das consequências devido à liberação de energia ou material perigoso. A integridade de equipamentos e acessórios irá determinar a probabilidade de ocorrência de um acidente que envolve uma grande perda.

5.2.1 Manutenção Preventiva e Plano de Inspeção

Um grande aliado à gestão de barreiras é o método como a instalação conduz a manutenção preventiva de instrumentos e a inspeção em equipamentos e acessórios. Um programa de manutenção preventiva e um plano de inspeção eficaz são itens chaves para que uma barreira esteja íntegra.

Manter o equipamento confiável requer que a instalação inspecione todos os equipamentos físicos de acordo com o planejamento programado baseado em códigos e práticas aplicadas.

Alguns componentes chaves para que o plano de manutenção e inspeção sejam elaborados de forma eficiente são:

- a) As rotinas de inspeção e manutenção devem estar de acordo com códigos da indústria e práticas reconhecidas, incluindo recomendações do fabricante, quando aplicável;
- b) Conduzir a realização das tarefas usando operadores qualificados e treinados, os quais utilizam procedimentos aprovados e atualizados e que completam a tarefa no tempo programado;
- c) Utilização de materiais de alta qualidade durante a manutenção/reparo;
- d) Manter o arquivo com o histórico de reparos do equipamento atualizados.

Além do histórico de reparos atualizado para cada equipamento, toda instalação deve possuir um sistema onde registre a periodicidade da realização da manutenção ou inspeção do equipamento/acessório/instrumento em questão. Este mesmo sistema deve apontar a equipe responsável quais equipamentos devem ter a manutenção realizada no próximo mês, por exemplo.

Atrasos na inspeção em vasos de processo, válvulas de alívio, e outros itens de segurança ou equipamentos críticos são de grande preocupação para as indústrias de processo. Vale ressaltar que nenhuma instalação ou programa de integridade é perfeito. A troca de uma peça de um equipamento pode estar vencida por alguns dias ou semanas devido a diversas circunstâncias, como exemplo, a alta demanda de produção ou redução de custos devido à baixa demanda.

Além dos critérios estabelecidos pela política da empresa no que tange a periodicidade e criticidade de um sistema pela confiabilidade, outra forma para auxiliar a instalação a rastrear os sistemas mais críticos é basear-se nos cenários maiores identificados para instalação. Logo, pode-se identificar os equipamentos, acessórios e instrumentos que exercem função de proteção nos cenários maiores da planta, e desta forma, priorizar os elementos para a realização da manutenção ou inspeção.

Durante a auditoria, etapa *Check* apresentada no modelo PDCA, a manutenção preventiva e a inspeção são elementos que devem ser amplamente explorados pelo auditor, verificando além do cumprimento do plano, o status das recomendações realizadas durante uma inspeção para o caso de linhas e equipamentos e manutenção para instrumentos.

Problemas como a reprogramação das recomendações na inspeção e recomendações em aberto por corrosão em linhas e acessórios degradados são alguns dos exemplos que podem ser encontrados pelo auditor e que devem estar contemplados no relatório da auditoria para serem tomadas as devidas ações.

5.2.2 Gerenciamento de Alarmes

Alarmes e instrumentos formam uma vital comunicação entre o processo e os operadores. Sem o funcionamento devido dos alarmes e instrumentos, torna-se mais difícil verificar o status operacional do processo e do equipamento de segurança.

Estes instrumentos podem estar diretamente ligados a um sistema de controle da planta ou estes podem indicar qual ação deve ser tomada pelo operador.

Os alarmes devem ser testados e calibrados e ter uma rotina de inspeção definida. Adicionalmente devem ser cuidadosamente instalados e localizados de uma maneira que garanta operações precisas e confiáveis.

Caso durante a identificação dos cenários, alarmes sejam reconhecidos como uma barreira de segurança do processo, esses elementos devem ser analisados durante a auditoria. Itens como a manutenção preventiva, testes e calibração devem ser verificados, bem como se o operador tem conhecimento de que aquele alarme é uma barreira de segurança para tal cenário. Como subsídio pode-se verificar no procedimento operacional da planta se o alarme relacionado está contemplado no mesmo.

Adicionalmente é comum verificar durante visitas ou conversas com operadores que existem alarmes desabilitados na planta. Quando a autorização para desabilitar o alarme é recorrente ou se alarmes e sistemas estão desabilitados por longos períodos, um sinal de alerta para o sistema de gestão deve ser acionado. Um estudo detalhado deve ser realizado na planta para se verificar a acuracidade e funcionalidade dos alarmes distribuídos na planta. Este estudo pode entrar no plano de ação para a melhoria da gestão das barreiras.

5.2.3 Sistemas Instrumentados de Segurança

Sistema instrumentado de segurança (SIS) é um nível independente de proteção para processos que possuem alto risco em caso de falha. Um SIS é composto por três elementos: iniciadores (sensores, ex. sensor de nível e sensor de pressão), executor da lógica (CLP - controlador lógico programável) e elemento final (atuadores, ex. válvula de bloqueio, bombas). Esses sistemas são independentes dos controles normais do processo e normalmente são projetados para atingir um alto desempenho. A Figura 5-1 apresenta o importante papel das SIS e de outras camadas de proteção para alcançar a redução do risco necessário.

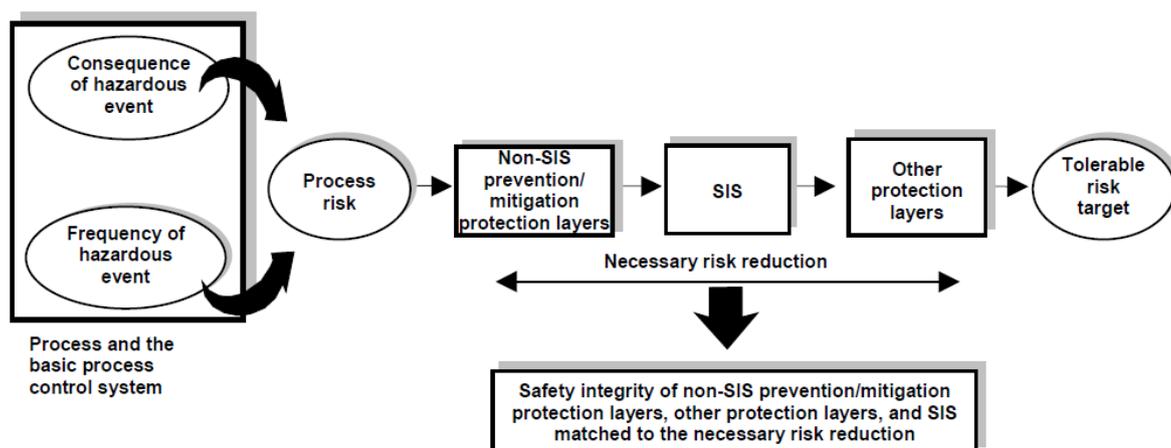


Figura 5-1– Importância das funções instrumentadas de segurança (Fonte: IEC61511-3, 2003).

Observa-se hoje que muitas empresas já possuem como procedimento interno a realização do estudo para verificação do nível de SIL requerido para as funções de segurança para seus empreendimentos. Esta verificação pode ser realizada através de duas metodologias: gráfico de risco e/ou LOPA. Para maiores detalhes destas metodologias, vide norma IEC-61508. Com base neste estudo a empresa tem subsídios para a compra dos instrumentos que atendam ao nível de SIL requerido da função de segurança.

Porém não basta que esses instrumentos sejam comprados com o nível de confiabilidade estabelecido durante o estudo. Testes e calibrações de toda função instrumentada de segurança, desde os iniciadores da função até seus atuadores, são necessários e de grande importância para assegurar seu desempenho. Adicionalmente testes nestas funções devem ser considerados de alta prioridade, pois caso não atuem quando demandadas podem gerar sérios danos para as pessoas, meio ambiente e instalação.

Tendo em vista que é de grande importância que o SIS seja testado no intervalo ótimo calculado para que sua função de segurança seja mantida íntegra, pode-se citar que o cálculo do intervalo de teste é uma prática já realizada e pode ser baseado em duas propostas: na formulação proposta pelo *International Electrotechnical Commission* (IEC) da Norma IEC-61508 e no SINTEF *Industrial Management Safety and Reliability* pela publicação, “*Reliability Quantification of Control and Safety Systems. The PDS-II Method*”.

Logo, é de grande importância que as SIS sejam testadas no intervalo ótimo calculado para que sua função de segurança seja mantida íntegra.

5.3 GERENCIAMENTO DOS RISCOS E DE MUDANÇAS

Como já mencionado nesta dissertação, a análise de risco é um elemento fundamental no conhecimento dos riscos, de suas barreiras e de toda gestão de Segurança de Processo. Sem uma sistemática efetiva de análise dos riscos em seus diversos níveis de complexidade e metodologias, não se consegue evoluir eficientemente na Segurança de Processo, muito menos no conhecimento e gestão das barreiras de proteção dos cenários.

Durante a operação de uma planta o gerenciamento de risco é uma função de contínuo empenho. Durante o projeto e a construção de uma instalação, riscos específicos são levados em conta e sistemas são utilizados para gerenciá-lo. Por conseguinte, durante a vida útil, mudanças e ampliações são realizadas na instalação e o gerenciamento dos riscos precisa acompanhá-las aplicando as boas práticas para gestão da segurança de processo.

Gerenciar mudanças durante a vida da instalação é um elemento chave na gestão dos sistemas na indústria para identificar e gerenciar os riscos.

Durante a fase de projeto ou nos primeiros anos da vida útil da instalação, os cenários identificados pela equipe de uma Análise Preliminar de Perigos, por exemplo, estão limitados aos produtos químicos presentes e seu processo. Revalidações permitem a equipe aplicar as lições aprendidas que ocorreram na instalação. Esta revisão permite a equipe ter uma visão holística de todas as mudanças realizadas desde a última revisão ou da versão original.

O risco de um incidente pode aumentar significativamente caso uma mudança no projeto não seja analisada de forma eficaz. Uma efetiva identificação dos perigos e um efetivo programa de avaliação dos riscos permite a organização acompanhar de forma correta os maiores cenários da instalação e identificar suas barreiras de proteção. Adicionalmente, devem motivar os trabalhadores a serem mais responsáveis e gerenciar sua própria segurança, pois frequentes mudanças podem resultar em indecisões/distúrbios como a definição do seu papel, suas responsabilidades e suas ações.

Os trabalhadores devem ser encorajados a parar qualquer situação ou comportamento que possa representar perigo às pessoas, ao meio ambiente e a instalação. Com isso cada trabalhador passa a exercer seu importante papel no gerenciamento dos riscos.

A revalidação dos riscos, além de representar uma boa prática, é também questão regulada em muitos países. No Brasil, por exemplo, segundo o INEA e a CETESB, estudos de análise de risco devem ser revisados a cada 5 anos.

Um importante fator a ser considerado é quanto ao treinamento dos líderes que irão conduzir as análises de risco. Quando se trata de uma empresa que possui diversas instalações e que possui líderes para condução das análises é imprescindível que os mesmos tenham o entendimento uniforme das técnicas que serão aplicadas adicionadas aos critérios de tolerância ao risco e dos procedimentos internos para a condução dos estudos.

Logo, para garantir abrangência, qualidade e consistência nos estudos de análise de risco realizados, é indispensável rever a sistemática de realização dos mesmos incluindo treinamento ou reciclagem das técnicas de análise de risco com validação externa, inclusão de exemplos e revisão/inclusão de instruções nos procedimentos internos.

5.3.1 Plano de Ação de Emergência

O Plano de Ação de Emergência estabelece procedimentos a serem adotados em situações de emergência. Esses procedimentos definem ações imediatas e eficazes com o objetivo de preservar vidas, proteger comunidades vizinhas e minimizar impactos ao meio ambiente e para o patrimônio.

Portanto é de suma importância manter o plano de ação de emergência atualizado e abrangendo os maiores cenários da instalação com suas proteções evidenciadas e as ações a serem tomadas.

A partir do plano atualizado, a instalação deve criar uma sistemática de treinamentos e simulados uma vez que a preparação é ponto fundamental para a realização de um atendimento adequado a uma emergência.

Está prática deve ser adotada, pois promove à prevenção e a aplicação corretamente dos requisitos de segurança visando o sucesso do atendimento as situações emergenciais.

Durante a auditoria de barreiras, o plano atualizado e a realização dos simulados são pontos fundamentais a serem abordados e evidenciados.

5.3.2 Bow-tie

Com os resultados do bow-tie é possível verificar o status de integridade das barreiras de segurança dos principais cenários acidentais da instalação e a partir destes dados desenvolver meios de manter a melhora contínua da integridade das barreiras e adequar as barreiras degradadas aos padrões de qualidade esperados.

Portanto, é imprescindível que os bow-ties sejam revisados continuamente pela equipe responsável para se adquirir o retrato atualizado dos cenários a serem gerenciados auxiliando na tomada de decisão das próximas ações a serem realizadas.

5.4 CULTURA DE SEGURANÇA

Conforme mencionado no item 2.4 desta dissertação, a cultura de segurança tem recebido atenção considerável e representa uma importante e ampla perspectiva na pesquisa para prevenção de danos.

A cultura organizacional, segundo Aiche (2012), geralmente é descrita como “a maneira como nos comportamos quando ninguém está vendo”. A cultura de segurança de processo é um subconjunto da cultura geral da organização.

A cultura de segurança surge como um conjunto comum de valores, comportamentos e normas que quando aplicados, influencia no desempenho da segurança de processo. A instalação com uma efetiva cultura de segurança de processo irá revelar excelentes índices e reconhecerá mais facilmente os sinais de alerta que precedem os acidentes catastróficos.

Os conceitos de disciplina operacional e cultura de segurança de processo formam um ciclo de *feedback* positivo. Um alto nível de disciplina operacional suporta uma efetiva cultura de segurança de processo, sendo o inverso também verdadeiro. Um bom líder e uma equipe de liderança serão alertados a qualquer

sintoma de deslize da cultura de segurança de processo e baixos índices de disciplina operacional.

Todos os itens citados nesta dissertação desde ao roteiro, apresentado no capítulo 4, quanto os elementos e boas práticas para uma boa gestão das barreiras só terão continuidade caso a empresa tenha uma forte cultura de segurança, e uma forte cultura de segurança só se sustenta com uma boa liderança.

Segundo Aiche (2012), características de uma boa liderança são:

- a) Comunicação aberta. Líderes precisam ouvir seus subordinados. Quando um trabalhador observa que algo inaceitável ou fora das normas, este deve se sentir encorajado a relatar o problema sem sentir medo de repressão.
- b) Responsabilidade. Líderes e seus subordinados precisam se responsabilizar pelo trabalho atribuído e metas associadas. Um líder responsável proporciona ferramentas e recursos que auxiliam a equipe a realizar a tarefa de forma segura e auxiliará na remoção dos obstáculos quando os mesmos acontecerem. Líderes responsáveis não “se escondem” atrás de desculpas ou negam presença ou não se importam com os sinais de alerta.
- c) Uma boa liderança é a habilidade de capacitar seus empregados e não somente de gerenciá-los.

Em concordância com Aiche (2012), Falconi (2010) explicita que existem três fatores fundamentais para a obtenção de resultados em qualquer iniciativa humana conforme observado na Figura 5-2.

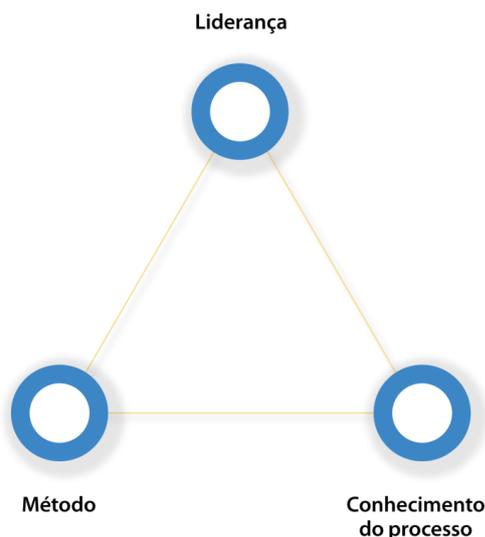


Figura 5-2– Fatores fundamentais para obtenção de resultados (Fonte: Falconi, 2010).

Dos três fatores citados na Figura 5-2, Falconi (2010), cita que a liderança é o item mais importante em uma organização. Para Falconi, ser um bom líder é conseguir resultados por meio das pessoas, logo o mesmo deve investir uma parte substancial de seu tempo no desenvolvimento de sua equipe.

Partindo do pressuposto de que a boa governança é condição fundamental ao exercício da liderança, os itens a seguir, de acordo com a Figura 5-2, apresentam o desenvolvimento do conteúdo de liderança em relação à cultura apresentados por Falconi (2010) que está alinhado com o exposto acima por Aiche (2012):

- a) Criar metas que sejam críveis e desafiadoras;
- b) Promover o domínio do método pela equipe, bem como num perfeito gerenciamento da rotina;
- c) Capacitar à equipe através de treinamentos;
- d) Supervisionar a maneira de trabalhar de sua equipe e aconselhar, fazendo ajustes de procedimento;
- e) Promover uma cultura que valoriza a verdade e não escondendo os fatos como são. É a cultura onde se espera que os gerentes comuniquem, para o time e para cima, não somente os bons resultados, mas também o que não está indo bem, para que possa ser consertado. Uma cultura onde se valorizam a busca de fatos e dados para analisar eventos e não somente opinião e intuição.

Com isso, a transformação da cultura de segurança pela busca de excelência é de extrema importância, pois é o líder quem promove e direciona para uma atuação focada na melhoria contínua.

5.4.1 Treinamento

Um treinamento efetivo proporciona aos trabalhadores, iniciantes ou experientes, o desenvolvimento de competências para exercer seu trabalho de forma segura com qualidade, responsabilidade ambiental e sucesso econômico. Um treinamento só é efetivo quando a mudança no comportamento é observada e a competência é avaliada durante demonstrações práticas no trabalho.

A competência é um conjunto de conhecimentos, habilidades e atitudes, que combinados resultam no desempenho dos trabalhadores.

Trabalhadores competentes são essenciais para prevenir acidentes catastróficos. Tanto o treinamento em salas de aula quanto aqueles realizados durante o trabalho (também conhecido do inglês, *on the job training*) são essenciais. Uma verificação regular e a aplicação de procedimentos auxiliam a confirmar que os trabalhadores são de fato competentes e possuem corretas atitudes na realização de suas tarefas. A gerência pode verificar os ganhos de um treinamento comparando o comportamento de sua equipe antes e depois do mesmo.

Um plano formal de treinamento irá ajudar a assegurar os trabalhadores operarem a planta com o projeto pretendido de maneira segura e eficiente. Treinamentos formais devem ser planejados e conduzidos para atender os requisitos operacionais do projeto e dos padrões de operação e as normas de funcionamento estabelecido pelo sistema de gestão.

5.4.2 Procedimentos

Procedimentos são instruções para a realização de um trabalho com um resultado desejado. Procedimentos ajudam a assegurar que todos os trabalhadores realizam suas tarefas de forma segura, correta e consistente. Procedimentos bem escritos devem incluir detalhes dos equipamentos, perigos e precauções. O nível de detalhes deve variar baseado na complexidade da tarefa e das potenciais

consequências caso ocorra um erro. Procedimentos são especialmente importantes nas situações de maiores perigos ou quando se lida com equipamentos complexos. Adicionalmente são importantes quando diferentes trabalhadores são solicitados a trabalhar em conjunto para realizar determinadas tarefas ou atividades.

Sem os procedimentos, a instalação não teria garantias que os métodos pretendidos pela organização seriam utilizados por cada operador. Procedimentos fornecem o suporte essencial para as atividades na planta, como a partida de um compressor ou um comissionamento em um forno.

Com isso os procedimentos devem estar sempre atualizados baseados na última revisão dos fluxogramas de engenharia (P&ID – *Piping and Instrument Diagram*). Adicionalmente as etapas descritas no procedimento devem ser equivalentes a atual prática dos trabalhadores durante a operação da planta.

Uma boa prática para que o fato exposto acima se fundamente é a utilização dos procedimentos durante o treinamento. Tal fato ajuda a assegurar que os procedimentos se tornarão familiar para os operadores bem como utilizá-lo para realizar a tarefa de forma correta. Complementando, a utilização destes em treinamentos permite que os operadores e especialistas identifiquem que as instruções não estão bem organizadas e/ou confusas.

Os itens a seguir apresentam indicadores importantes para realização de um bom procedimento:

- a) Procedimentos devem conter os limites seguros para a operação do processo em questão;
- b) Procedimentos devem identificar as consequências caso ocorra um desvio dos limites operacionais;
- c) Procedimentos devem ser objetivos e claros;
- d) Procedimentos devem ser verificados periodicamente para conferir se a atual prática está alinhada a prática pretendida;
- e) A cultura organizacional da empresa deve incentivar/estimular a utilização dos procedimentos.

6 CONCLUSÃO

Este trabalho apresentou a gestão das barreiras de segurança como um elemento chave para a prevenção de acidentes.

Na introdução, foi abordada a evolução dos estudos voltados para a segurança do processo, porém os acidentes ocorridos nos últimos 10 anos alertam que o tema ainda é um assunto sério e preocupante e que ainda há muito a ser feito. Como citado por Bardy (2012a), os acidentes demonstraram e intensificaram a importância das barreiras de segurança na prevenção de acidentes ou na redução dos seus efeitos.

Na visão da gestão de segurança de processo, podemos perceber ao longo deste trabalho que o diversos elementos contribuem para sua boa performance, desde fatores humanos como a cultura e atitude dos empregados, passando por fatores técnicos como confiabilidade dos equipamentos utilizados até outros elementos de gestão como planos de manutenção preventiva e treinamentos. Todos estes elementos, são entendidos por este trabalho como barreiras de segurança e se submetidos ao processo proposto aqui, serão muito mais efetivos quando demandados.

A partir da auditoria de barreiras, ponto chave para a gestão das mesmas, identifica-se necessariamente as fragilidades dos cenários mais críticos, e ainda sugere por similaridade ações para outros cenários similares, mesmo que não tenham sido avaliados. Estas ações visam tratar as barreiras de forma ampla como mencionado acima, e tendo como foco a concepção da barreira ideal para a criticidade identificada.

Apesar desta complexa interpretação do que é considerado barreira de segurança, avançou-se um pouco mais na direção da contribuição que a cultura da empresa e o engajamento da alta gestão representam para este contexto. Ou seja, sem a participação ativa da alta gestão não se consegue permear os diferentes níveis da organização e para facilitar o envolvimento dos mesmos, este trabalho propôs seu envolvimento a partir da técnica de bow-tie. Desta forma, acredita-se que aliando a capacidade de comando ao correto e aprofundado entendimento da liderança dos desafios que seu negócio oferece, a gestão de segurança como um todo estará bem mais robusta.

Finalizou-se o trabalho com boas práticas de mercado em termos de gestão de barreiras de segurança, a partir de estudos que mostra sua efetividade no dia a dia, além do detalhamento de acidentes que, de forma clara, mostram o alinhamento de problemas relacionados à gestão de barreiras. Além disto, Kletz (2001) complementa esta conclusão na medida em que identifica a partir destes acidentes oportunidades de melhoria para a segurança de processo.

7 REFERÊNCIAS BIBLIOGRÁFICAS

AICHE. **Building Process Safety Culture: Tools to Enhance Process Safety Performance**, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA 2005. Disponível em: <http://www.aische.org/uploadedFiles/CCPS/Resources/KnowledgeBase/Culture_frontend_matter_Rev3.pdf>. Acesso em: 23 jun. 2012.

AICHE. **Guidelines for Chemical Process Quantitative Risk Analysis**. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA. 2000. 770p.

AICHE. **Guidelines for Hazard Evaluation Procedures**. 3ed. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA. 2008. 536p

AICHE. **Guidelines for Risk Based Process Safety**. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New Jersey, USA. 2007. 706p.

AICHE. **Incidents that Define Process Safety**. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA. 2008. 336p

AICHE. **Layer of Protection Analysis – Simplified Risk Assessment**. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA. 2001. 258p.

AICHE. **Recognizing Catastrophic Incident Warnings Signs in the Process Industries**. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA. 2012. 227p

ALMEIDA, T. S. S. **Avaliação de Segurança de Processo Aplicada à Indústria de Gases**. 2011. 166 f. Monografia (Especialista) - Curso de Pós-Graduação em Engenharia de Segurança do Trabalho, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, 2011.

ANP & DPC. **Análise do acidente com a plataforma P-36**. Relatório da Comissão de Investigação ANP / DPC. 2001.

BARDY, M., OLIVEIRA, K., DINIZ, A. **Evaluation of Management of Safety Barriers for Major Hazard Accidents**. 8th Global Congress on Process Safety, Center for Chemical Process Safety of the American Institute of Chemical Engineers, Texas, USA, 2012a.

BARDY, M., et al. **Gestão de Barreiras de Segurança de Processo Combinando Bowtie e Auditoria**. 4th Latin American Conference on Process

Safety, Center for Chemical Process Safety of the American Institute of Chemical Engineers, Rio de Janeiro, Brasil, 2012b.

BAKER, J.A.III, et all, **The Report of the BP U.S. Refineries Independent Safety Review Panel.** 2007. Disponível em: <http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/SP/STAGING/local_assets/assets/pdfs/Baker_panel_report.pdf>. Acesso em: 23 jun. 2012.

BONFIM, D. T. **Deepwater Horizon: Acidente e Lições Aprendidas.** Disponível em: <http://www.sindmar.org.br/uploads/artigos/pdf/Cpia_de_ArtigoDiego.pdf>. Acesso em: 25 ago. 2012.

BP. **Deepwater Horizon – Accident Investigation Report.** BP investigation team. 2010. Disponível em: <http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/incident_response/STAGING/local_assets/downloads_pdfs/Deepwater_Horizon_Accident_Investigation_Report.pdf>. Acesso em: 26 ago. 2012.

CSB. **Federal Investigation of Tosco Refinery Fire Finds Flawed Management Supervision.** Disponível em: <<http://www.csb.gov/newsroom/detail.aspx?nid=62>>. Acesso em: 18 ago. 2012.

CSB. **Investigation Report, Refinery Fire Incident, Tosco Avon Refinery.** U.S. Chemical Safety and Hazard Investigation Board. 1999. Disponível em: <http://www.csb.gov/assets/document/Tosco_Final_Report.pdf>. Acesso em: 26 ago. 2012.

CETESB. **Manual de Orientação para a Elaboração de Estudos de Análise de Riscos.** P4.261, Maio, 2003.

CHIEF COUNSEL. **Macondo – The Gulf Oil Disaster.** Chief Counsel's Report, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011. Disponível em: <<http://www.oilspillcommission.gov/chief-counsels-report>>. Acesso em: 26 ago. 2012.

COCKSHOTT, J. E., **Probability Bow-Ties - A Transparent Risk Management Tool.** Process Safety and Environmental Protection, Institution of Chemical Engineers, v.83(B4), p. 307–316. 2005.

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO. **Análises de Risco.** Disponível em: <<http://www.cetesb.sp.gov.br/gerenciamento-de-riscos/Emeg%C3%A4ncias-Qu%C3%ADmicas/4-Introdu%C3%A7%C3%A3o>>. Acesso em: 10 jun. 2012.

DIANOUS, V., FIÉVEZ, C., **ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of**

safety barrier performance. Journal of Hazardous Materials, Elsevier, v.130 p. 220–233. 2006.

DUIJM, N. J., **Safety-barrier diagrams as a safety management tool.** Reliability Engineering and System Safety, Elsevier, v.94 p. 332–34. 2009.

FALCONI, V. **Gerenciamento da Rotina do Trabalho do Dia-a-Dia**, 8.ed Belo Horizonte: Editora de Desenvolvimento Gerencial, 2002. 259p.

FALCONI, V. **O Verdadeiro Poder – Práticas de Gestão que Conduzem a Resultados Revolucionários**, 1.ed Belo Horizonte: Editora de Desenvolvimento Gerencial, 2010. 159p.

GADD, S., COLLINS, A. M. **Safety Culture: A review of the literature.** Health and Safety Laboratory. **Sheffield, Inglaterra, 2002.** Disponível em: <http://www.hse.gov.uk/research/hsl_pdf/2002/hsl02-25.pdf>. Acesso em: 23 jun. 2012.

HADDAD, A., MORGADO, C. **Elementos de Segurança Ambiental.** Editora Aquarius, 2002.

HENDERSHOT, D. **Process Safety Culture.** Journal of Chemical Health & Safety, Elsevier, p. 39-40. 2007.

HOLLNAGEL, E. **Barriers and Accident Prevention.** Human-Technology Integration Colloquium Series, Air Force Research Laboratory Human Effectiveness Directorate, 2002

HOLLNAGEL, E. **Barriers and Accident Prevention**,1.ed Inglaterra: Ashgate, 2004. 219p

HOLLNAGEL, E., WOODS, D.V., LEVESON,N. **Resilience Engeneering – Concepts and Precepts**,1.ed Inglaterra: Ashgate, 2006. 337p.

HSE. **Flixborough (Nypro UK) Explosion 1st June 1974.** Disponível em:<<http://www.hse.gov.uk/comah/sragtech/caseflixboroug74.htm>>. Acesso em: 18 ago. 2012.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61508. **Functional safety of electrical/electronic/programmable electronic safety-related systems.** 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61511. **Functional safety – Safety instrumented systems for the process industry sector –** 2003.

KLETZ, T. **Learning from Accidents**. 3.ed Oxford: Gulf Professional Publishing, 2001. 345p.

LESS, F. P. **Loss Prevention in the Process Industries – Hazard Identification, Assessment and Control**. 3.ed v.1 Oxford: Elsevier, 2005.

LEVESON, N. G. **A New Approach to System Safety Engineering**. Aeronautics and Astronautics Massachusetts Institute of Technology, 2002. Disponível em: <<http://ocw.alfaisal.edu/NR/rdonlyres/Aeronautics-and-Astronautics/16-358JSpring-2005/7A17C38C-F622-4244-ABF0-5BD2B768661C/0/book2.pdf>>. Acesso em: 22 jun. 2012.

LUND, J., AARØ L. E. **Accident Prevention. Presentation of a Model Placing Emphasis on Human, Structural and Cultural Factors**. Safety Science, Pergamon, v. 42, p. 271–324. 2004.

OKSTAD, E., et al. **In the aftermath of the Deepwater Horizon accident: Inadequate risk management as a common feature of major offshore well operations accidents**. ESREL, Helsinki, Finlândia, 2012.

OLIVEIRA, L. F. **Falhas Humanas e Medidas Disciplinares: Contribuição para o Desenvolvimento de um Procedimento para Aplicação de Medidas Disciplinares**. 7º Seminário Sobre Programa de Gerenciamento de Risco no Polo. Comitê de Fomento Industrial de Camaçari (COFIC), Salvador, Brasil, 2008.

ORDONEZ, R. **Empresas Compartilham Experiências para Avançar em Segurança Operacional**. O Globo, Rio de Janeiro, 26 de set. 2012. Disponível em: <<http://oglobo.globo.com/economia/empresas-compartilham-experiencias-para-avancar-em-seguranca-operacional-6200910>> Acesso em: 26 set. 2012.

PASCON, P. E. **FLIXBOROUGH – 25 ANOS** Disponível em: <http://www.processos.eng.br/Portugues/PDFs/flixborough_25_anos.pdf> Acesso em: 25 ago. 2012.

PITBLADO, R. **Global Process Industry Initiatives to Reduce Major Accident Hazards**. Journal of Loss Prevention in the Process Industries, Elsevier, v.24, p.57-62. 2011.

PRESIDENT COMMISSION. **Deep Water. The Gulf Oil Disaster and the Future of Offshore Drilling**. Report to the president, 1. ed, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, U.S. Government Printing Office, 2011.

RASMUSSEN, J. **Skills, Rules and Knowledge; Signals, Signs and Symbols, and Other Distinctions in the Human Performance Models**, IEEE Transactions on Systems, Man, Cybernetics, v.smc-13, nº 13, 1983.

TINMANNSVIK, R. K., et al. **Deepwater Horizon-ulykken: Årsaker, lærepunkter og forbedringstiltak for norsk sokkel (Executive Summary: The Deepwater Horizon accident: Causes, lessons learned and recommendations for the Norwegian petroleum activity)**. SINTEF A19148, 2011.

VIEIRA, N. M. V. **Metodologia para Cálculo do Efeito Dominó na Análise de Riscos de uma Instalação Industrial Química**. 2001. 101 f. Dissertação (Mestre) - Curso de Pós-Graduação em Tecnologia de Processos Químicos e Bioquímicos da Escola de Química, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Rj, 2001.