# METODOLOGIA PARA ANÁLISE DOS MODOS DE FALHA APLICADA À SEGURANÇA DE CONDICIONADORES DE AR

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

# METODOLOGIA PARA ANÁLISE DOS MODOS DE FALHA APLICADA À SEGURANÇA DE CONDICIONADORES DE AR

**Dissertação submetida à**

**UNIVERSIDADE FEDERAL DE SANTA CATARINA**

**para a obtenção do grau de**

**MESTRE EM ENGENHARIA MECÂNICA**

**VADIS BELLINI**

**Florianópolis, dezembro de 2008**

# CAPÍTULO 1
# INTRODUÇÃO

Atualmente, no Brasil, o parque instalado de aparelhos condicionadores de ar tipo janela e *split* já ultrapassa os trinta milhões de produtos, segundo dados da Pesquisa Mercado CA Multibras S.A. (WHIRLPOOL, 2003). O mercado anual desse produto está em torno de dois milhões de unidades vendidas (ABRAVA, 2008). Por conta desses números, de legislações recentes, voltadas para a segurança do consumidor e, ainda pelo entendimento das organizações quanto a sua responsabilidade social perante as comunidades, as empresas vêm buscando tornar os seus produtos cada vez mais robustos e seguros para o consumidor final.

Processos de *recall*[1] que até pouco tempo não faziam parte da realidade brasileira, estão se tornando freqüentes, principalmente devido à mudança cultural, que vem afetando de modo complementar consumidores e organizações. Os consumidores estão mais atentos aos seus direitos e, conseqüentemente, cobram das organizações, de forma efetiva, suas responsabilidades pelos produtos comercializados. Constata-se, no entanto, que o custo embutido no processo de cobrança (ou compensação por danos) devido a incidentes é ainda relativamente pequeno para as empresas brasileiras quando comparado ao mercado estadunidense, por exemplo. Contudo, fica evidente que o passivo gerado por problemas de segurança em seus produtos é algo que pode, de um momento para outro, inviabilizar a continuidade de uma determinada empresa.

Além disso, a busca pela fidelidade de seus consumidores está obrigando as organizações a assumirem novos padrões de atendimento e comprometimento perante a eles. A segurança dos produtos nesse contexto passa a assumir nova dimensão fazendo com que as indústrias procurem adequar e, muitas vezes, exceder as regulamentações legais de forma a oferecer produtos que não venham a expô-las em processo legal por perdas e danos. O processo de *recall* que costumava potencializar o comprometimento da organização atualmente apenas evidencia a ineficiência das organizações em projetar e ou controlar seus processos de forma a evitar falhas que possam afetar a segurança dos produtos. Essa conjuntura está levando as organizações a reverem seus produtos e processos de desenvolvimento de forma a reduzir efetivamente o passivo existente e o passivo que possa vir a ser gerado em projetos futuros.

---

[1] Um **recall** (do inglês, significa "chamar de volta", "chamamento") ou **recolhimento de produto** é uma solicitação de devolução de um lote ou de uma linha inteira de produtos feita pelo fabricante. Geralmente, isto ocorre pela descoberta de problemas relativos à segurança do produto. O *recall* é uma tentativa de limitar a responsabilidade por negligência corporativa (que pode motivar severas punições legais) e aprimorar ou evitar danos à publicidade da empresa.

Uma questão pode ser formulada: como atuar nesse contexto para garantir produtos seguros para o consumidor, mesmo para grande escala de produção? Observa-se que existe metodologia que prevê a inserção do atributo de segurança nas fases iniciais do processo de projeto de produto, porém muitos de seus aspectos se perdem ao longo do processo de projeto em detrimento de outros requisitos mais apelativos. A dificuldade na acessibilidade pelos projetistas ao conhecimento específico referente à segurança, como Legislação, Normas Técnicas e princípios de solução já adotados, supõe-se ser um fator que contribui, geralmente, para a não inserção de alguns dos aspectos relativos à segurança no produto, ou sua não permanência ao longo das macro-fases de projeto, fabricação, uso e até mesmo o descarte. A dificuldade pode estar também relacionada à grande quantidade de informação sobre segurança, com a diversidade da informação, com a mudança conceitos, exigências e paradigmas até então não valorizados, com a generalidade da metodologia de projeto que está sendo adotada, entre outras.

Ao pesquisar o tema percebe-se que muitas são as sistemáticas de projeto presentes na literatura, tais como Romano (2003), Pahl & Beitz (1996) e Back (1983), e de uma forma geral, elas abordam as diversas fases do processo do projeto: informacional, conceitual, preliminar e detalhado.

Focando o interno da fábrica, mais especificamente o processo de projeto desenvolvido pela Whirlpool, nota-se que ele contempla algumas ferramentas de projeto com foco em segurança como FMEA, FTA etc. As ferramentas são mencionadas na descrição das tarefas ao longo do processo de projeto, porém sem uma definição clara do momento correto para sua aplicação e da interação que deve existir entre elas.

A inexistência de definições claras sobre o momento correto de aplicação das ferramentas e do nível de interação que deve existir entre elas, afeta de forma significativa a sua eficácia. Em decorrência, problemas que podem ser detectados e tratados nas fases de definição do conceito, em algumas situações, não são detectados e em outras tantas são identificados apenas após a fase da conversão do projeto em produto com conseqüentes implicações de custo e prazo.

A percepção é que muitas ações relacionadas à segurança não são organizadas no início do processo do projeto. Assim, este trabalho dedicou-se a identificar e inserir os requisitos de segurança nas fases iniciais, informacional e conceitual, bem como atuar para facilitar a integração e interação das diversas ferramentas de projeto voltadas para a segurança ao longo das fases informacional, conceitual, preliminar e detalhado do processo de projeto.

Ao mesmo tempo, optou-se por desenvolver a metodologia para ser aplicada no projeto de condicionadores de ar. Tal decisão é justificada pelo entendimento que no aspecto

relacionado à segurança deve-se desenvolver processos específicos de controle de projeto e fabricação contemplando, no projeto de condicionadores de ar, o máximo possível de restrições legais e normas específicas. Esse entendimento deve-se também à percepção de que não está disponível uma clara definição de quais ferramentas de projeto e a que tempo devem ser aplicadas para uma eficiente identificação e tratamento dos modos de falha relacionados à segurança de condicionadores de ar.

## 1.1 Objetivos

### 1.1.1 Objetivo geral

Analisando-se o tema que está sendo proposto, pode-se afirmar que há forte desenvolvimento de metodologias para o projeto para segurança, ao mesmo tempo em que há outras já sendo implementadas e utilizadas ao longo da história de desenvolvimento de produtos. Contudo, os acidentes continuam a ocorrer e os custos relacionados a eles tendem ser cada vez mais significativos. Para entender melhor esta constatação, formulou-se algumas hipóteses que devem servir de base para a definição do objetivo deste trabalho:

- A evolução tecnológica, com a implementação de novos componentes e materiais, contribui para gerar uma defasagem entre o conhecimento do corpo técnico e os requisitos necessários para aplicação dessas novas tecnologias de forma segura.
- Há abordagem limitada dos conceitos de segurança e confiabilidade, e por vezes, um incorreto entendimento destes atributos no contexto do projeto de produto específico. Conforme Dias *et al.* (2005) esses dois atributos têm, na grande maioria dos casos, objetivos conflitantes, o que pode produzir abordagens não adequadas para todo o ciclo de vida.
- A capacidade das organizações de reter e transmitir o conhecimento adquirido pelo corpo técnico ao longo dos anos entende-se ser outra causa que afeta de forma consistente a robustez dos projetos para segurança.

Por exemplo, o produto condicionador de ar, abordado neste trabalho, é um produto para uso doméstico, sujeitos aos mais variados tipos de instalação e que utiliza eletricidade como fonte de energia. Nos últimos anos tem-se observado nesse tipo de produto um alto índice de substituição do aço por polímeros em geral. Essa substituição, por sua vez, tem provocado dificuldades ao corpo técnico na avaliação das conseqüências de determinados modos de falha. Falhas até então conhecidas como, por exemplo, o superaquecimento de uma conexão elétrica que em muitos casos não eram percebidas ou tinham como conseqüência

apenas problemas de qualidade, passam a ter um efeito catastrófico nos produtos atuais. Nos últimos 10 anos estima-se que apenas um dos grandes fabricantes mundiais de eletrodomésticos arcou com um custo de aproximadamente $300.000.000 (Dólares) devido a problemas de segurança em seus produtos, envolvendo a substituição e ou reparo de cerca de 4.000.000 de produtos produzidos e comercializados em diferentes continentes.

Essas e outras percepções apontam para a necessidade de elaborar uma sistemática para que as experiências e conhecimento adquirido sejam transmitidos e fiquem disponíveis para constante consulta.

Assim, o objetivo geral deste trabalho é desenvolver uma metodologia que seja precisa e ao mesmo tempo facilite a identificação de requisitos de segurança e ajude a produzir as especificações para serem consideradas ao longo do processo de projeto de condicionadores de ar.

Numa visão mais geral deve-se contribuir com o projeto para segurança de produtos de uso doméstico, cujos princípios de solução se aproximam do que está sendo abordado. A abordagem deve contemplar as fases do ciclo de vida que vão do planejamento até o descarte sem que este traga conseqüências para o meio ambiente.

### 1.1.2 Objetivos específicos

Este trabalho tem como objetivos específicos:

- Prover ao corpo técnico o conhecimento necessário para considerar o atributo de segurança, durante todo o ciclo de vida do produto.
- Minimizar os riscos gerados pelos produtos em relação à integridade dos consumidores e de suas propriedades.
- Garantir a viabilidade comercial dos produtos e das empresas.
- Adequar as ferramentas de projeto e tarefas com foco na segurança para cada fase, principalmente nas fases de projeto informacional e conceitual.
- Caracterizar os fatores de influência na segurança de condicionadores de ar.

## 1.3 Metodologia da pesquisa

- Pesquisar na literatura geral de projeto e na literatura específica de projeto para segurança os passos e procedimentos que estão sendo considerados para o projeto para segurança.

- Pesquisar na legislação, Normas técnicas Nacionais e Internacionais, Normas Regulamentadoras, as determinações relativas à segurança de condicionadores de ar.
- Aplicar e avaliar a metodologia desenvolvida e o modelo proposto em um estudo de caso de projeto de condicionador de ar.

## 1.4 Resultados esperados

Entende-se que este projeto oferece as seguintes contribuições:

- Metodologia,
- Ferramentas,
- Processos de análise.

Revisão da Metodologia atualmente aplicada de forma enfatizar o uso das ferramentas apropriadas para cada etapa do projeto informacional, conceitual, preliminar e detalhado. Geração de novas ferramentas que tornem o processo de desenvolvimento mais robusto na identificação, detecção e tratamento dos aspectos de segurança para o consumidor final.

De forma geral as metodologias de projeto indicam a utilização de diversas ferramentas de projeto com foco na segurança, porém é possível agregar algum valor em termos de métodos e ferramentas para cada etapa do projeto.

Será ainda detalhada a interface entre as diferentes ferramentas de projeto com foco na segurança de forma a estabelecer a ligação entre as respectivas entradas e saídas destas no sentido de potencializar a concepção de um produto seguro.

## 1.5 Conteúdo da Tese

O conteúdo da presente tese é apresentado em 7 capítulos conforme descrição a seguir.

No Capítulo 1, ora em tela, é delineado o escopo desta tese. Inicialmente foi apresentada uma breve contextualização. Na seqüência foi delimitado o problema, indicando que este trabalho visa avaliar a segurança de condicionadores de ar em todo o ciclo de vida do produto.

No Capítulo 2 é caracterizado o modelo da corrente causal para análise de incidentes e realizada uma revisão dos conceitos relacionados com segurança, visando identificar ferramentas e métodos que poderão ser úteis neste trabalho.

No Capítulo 3 são abordados diversos modelos de projeto de produto para a segurança e caracterizados os principais fatores de influência na segurança de produtos.

No Capítulo 4 é apresentada a metodologia para a concepção de condicionadores de ar seguros, objetivo principal deste trabalho.

No Capítulo 5 a metodologia desenvolvida é empregada em um estudo de caso, na avaliação do sistema de controle de um condicionador de ar.

No Capítulo 6 são apresentadas as conclusões deste trabalho, objetivos alcançados e contribuições geradas.

Bibliografia consultada que deu suporte a este trabalho.

No Anexo 1 é apresentado o resumo da norma ANSI referente a comunicação de risco.

No Anexo 2 é apresentado um resumo sobre o Código de Defesa do Consumidor.

No Apendice 1 é apresentada a descrição dos níveis que compõe o índice SOD, Severidade, Ocorrência e Detecção.

No Apendice 2 é apresentada a lista de verificação para aspectos de segurança elaborada neste trabalho.

No Apendice 3 é apresentada as matrizes de criticidade elaboradas neste trabalho.

No Apendice 4 é apresentada a matriz componentes versus requisitos, elaborada neste trabalho.

No Apendice 5 é apresentado o FMEA elaborado neste trabalho.

# CAPITULO 2
# CONCEITOS BÁSICOS EM SEGURANÇA DE PRODUTO

## 2.1 Introdução

Nas últimas décadas tem-se observado uma enorme evolução na percepção da segurança aplicada a produtos. Novos requisitos e necessidades impulsionam a evolução acadêmica e industrial para o desenvolvimento de novos materiais e para sistemas mais complexos. Esses novos materiais e sistemas mais complexos têm aguçado a percepção por mais segurança por parte da sociedade, em face dos novos perigos que trazem com eles.

É a partir desse contexto que este capítulo aborda os principais conceitos relacionados com segurança e metodologia de projeto, e que serão utilizados ao longo deste trabalho.

Para tanto, alguns termos que serão abordados repetidamente neste trabalho necessitam ser evidenciados quanto ao seu significado no contexto.

Risco - O conceito de risco está, em geral, associado à incerteza de um resultado, podendo este resultado ser positivo ou negativo. No entanto, conforme definido por Peres (2006), no que concerne aos sistemas técnicos, o risco está associado apenas aos resultados negativos.

Na literatura algumas definições de risco podem ser encontradas:

- Possibilidade de perigo ou de sofrer algum dano ou perda (OXFORD, 1995);
- Uma chance de perda, um grau de probabilidade de perda, a quantidade possível de perda (HAMMER, 1993);
- É a probabilidade de se concretizar um evento (SALDANHA, 2000).

Neste trabalho risco será definido como a chance do perigo vir a se tornar um determinado incidente ou produzir conseqüências danosas para o homem e/ou ambiente.

Incidente - A norma ISO/IEC GUIDE 51 *Safety aspects – Guidelines for their inclusion in standards* define incidente como um evento que, em sua ocorrência, resulta em dano à saúde de pessoas, à propriedade ou ao meio ambiente. Também é comum na literatura o uso do termo acidente, que muitos diferenciam de incidente – considerando este último um quase-acidente. Acidentes, nesse caso, seriam os eventos que resultam em dano ao homem ou ao ambiente. Note-se que a definição de incidente proposta pela norma ISO/IEC GUIDE 51 engloba o conceito de acidente.

Neste trabalho, o termo incidente será adotado para designar todo evento que interferir negativamente na segurança do produto. Assim, o termo incidente também será utilizado em substituição de acidente.

Perigo – A norma ABNT ISO/IEC GUIA 73 (ABNT, 2005) define perigo como a fonte potencial de dano. Mosleh *et al.* (2004, p. 19) ampliam esse conceito e definem perigo como "qualquer ato (omissão ou ação), condição ou estado do sistema – ou uma combinação desses – com o potencial de resultar em um incidente".

Dessa forma, para sistemas técnicos mais especificamente condicionadores de ar, perigo aqui será definido como condição e ou estado do produto com o potencial de resultar em um incidente.

Segurança - Nada é completamente seguro, segurança é relativa e não absoluta. A Política Nacional de Defesa Civil (BRASIL, 2007) e o plano de Segurança Global da População (BRASIL, 2007) publicados pela Secretaria Nacional de Defesa Civil definem que a segurança global da população fundamenta-se no direito natural à vida, à saúde, à segurança, à propriedade e à incolumidade das pessoas e do patrimônio, em todas as condições, especialmente em circunstâncias de desastres. Esse conceito pode ser aplicado na íntegra quando analisado sob a perspectiva de produtos e serviços fornecidos à população.

Nesse contexto, segurança pode ser definida como o estado de confiança individual ou coletiva, baseado no conhecimento e no emprego de normas de proteção e na convicção de que os riscos de incidentes foram reduzidos, em virtude de terem sido adotadas medidas mitigadoras.

Falha - Segundo o *International Electrotechnical Commission* IEC 50 (191) (1990) falha é definida como a impossibilidade de um equipamento desempenhar a sua função.

O entendimento do conceito e a correta identificação dos modos de falha de um sistema são fundamentais para análise e incremento da segurança dos sistemas.

Conforme definido, a falha em um sistema técnico implica em perda ou impossibilidade dele desempenhar a função. A perda de uma determinada função, por sua vez, pode ter como efeito o não funcionamento parcial ou total do sistema ou ainda a geração de algum perigo para os usuários do sistema.

A NBR 5462, Confiabilidade e Mantenabilidade, desdobra o conceito de falha. Alguns destes conceitos serão aplicados neste trabalho:

- Falha crítica – Falha que provavelmente resultará em condições perigosas e inseguras para pessoas, danos materiais significativos ou outras conseqüências inaceitáveis.
- Falha não crítica – Falha que não seja crítica.
- Falha por uso incorreto – Falha devida à aplicação de solicitações além dos limites especificados ou a erros de instalação ou operação.

- Falha por manuseio – Falha causada por manuseio incorreto ou falta de cuidado com o item.
- Falha de projeto – Falha de um item devido ao projeto inadequado.
- Falha de fabricação – Falha de um item devido a não conformidade da fabricação com o projeto ou com os processos de fabricação especificados.

Os tipos de falhas citadas, de projeto, de fabricação, por uso incorreto ou ainda por manuseio podem, por sua vez, originar uma falha crítica ou não crítica.

Neste trabalho, portanto a utilização do termo falha estará sempre associada ao conceito de falha crítica. Por sua vez, a perda da função pode gerar algum perigo para os usuários e ou meio ambiente que interagem com o produto.

Há de se salientar que o conceito de "falha" zero ou "quebra" zero é uma utopia. Todo sistema técnico desgasta-se naturalmente ao longo da vida útil. Esse fato é inevitável, de modo que, conforme Dias (2005), nunca ocorre de uma máquina se recuperar, passando a operar como nova depois de ter apresentado uma falha operacional.

A taxa de falha de um determinado componente é definida pelo seu projeto, manufatura e condições específicas de aplicação. No que tange às condições de aplicação, os mecanismos de desgaste ou deterioração que atuam sobre um componente podem ser de natureza mecânica, elétrica, térmica, química ou operacional e estão sempre presentes nas máquinas. O efeito cumulativo dos mecanismos de desgaste manifesta-se pela falha. As falhas de forma geral ocorrem sob condições específicas de estresse. Hammer (1993) ressalta que reduzindo o estresse sob a maneira como um determinado componente deve operar irá provavelmente reduzir a sua taxa de falha. Como exemplo cita que um dos principais estresses que afetam a vida de componentes elétricos e eletrônicos é o incremento da temperatura. Uma maneira de reduzirem-se os efeitos causados pela temperatura (*derating)* seria providenciar um sistema de refrigeração para reduzir a temperatura de operação ao nível mais baixo possível, minimizando dessa forma as falhas.

Em uma análise focada na segurança do produto é pertinente considerar-se o conceito de falha segura. Falha, como definido anteriormente, é inerente a qualquer sistema e não pode ser evitada, porém o modo como ela se manifesta pode ser estudado, previsto e controlado. Quando devidamente avaliados, os sistemas podem ser projetados para que as falhas sejam seguras não expondo os usuários dos produtos a qualquer situação de risco. O conceito de falha segura pode ainda ser associado ao modelo da corrente causal, na qual, por definição, barreiras devem ser postas ao longo do caminho causal para eliminar a condição de perigo, diminuir o potencial e/ou a probabilidade (chance) de ocorrência do incidente, ou ainda,

mitigar as conseqüências. O modelo da corrente causal será abordado na seqüência deste trabalho.

## 2.2 Modelo da corrente causal para análise de incidente

A Figura 2.1 apresenta o modelo de ocorrência de incidentes proposto por Mosleh e Dias (2004), no qual, o incidente é resultado de uma condição perigosa aliada a um evento deflagrador (gatilho), perpassando as barreiras se elas não forem suficientes para evitá-lo.

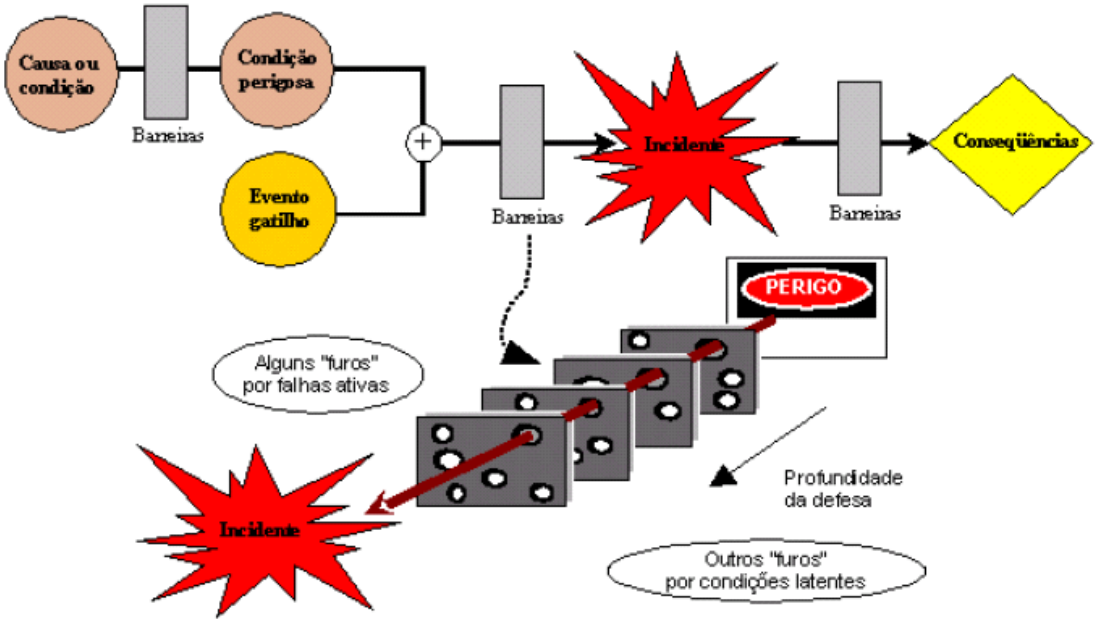



Figura 2.1 - Modelo da corrente causal para análise de perigo e trajetória de incidentes através de barreiras (adaptado de MOSLEH e DIAS (2004) e REASON (1997)

Todo sistema técnico é portador de perigo (Dias *et al.*, 2005). Esse perigo pode, ao longo do ciclo de vida, evoluir para uma condição perigosa. A combinação dessa condição com um evento gatilho pode provocar um incidente.

Conforme definido por Dias *et al.* (2007), o evento deflagrador pode estar associado a uma falha oculta no sistema, de origem no próprio sistema técnico, no sistema humano (organizacional) ou no meio ambiente.

Barreiras devem ser postas ao longo do caminho causal para eliminar a condição de perigo, diminuir o potencial e/ou a probabilidade (chance) de ocorrência do incidente, ou ainda, mitigar as conseqüências.

As barreiras desempenham funções específicas em cada posição que se encontram ao longo da corrente causal. Contudo, as barreiras apresentam furos (falhas) por onde evoluem os

perigos para o incidente e também para as conseqüências. As barreiras podem ser barreiras físicas, procedimentos, manuais, normas, regulamentação, educação, capacitação, motivação ou qualquer medida que vise atuar na corrente causal evitando o incidente ou minimizando suas conseqüências. No sentido de reduzir o risco de ocorrer o incidente ou mitigar suas conseqüências, recomenda-se a adoção de mais de uma barreira, o que é designado por Reason (1997) como “defesas em profundidade”. As barreiras estão fortemente relacionadas à própria análise probabilística de risco ou, em alguns casos, confundem-se com as próprias ações de gerenciamento – que a ABNT ISO/IEC GUIA 73 (ABNT, 2005) divide em quatro partes: análise/avaliação, tratamento, aceitação e comunicação de riscos.

De modo semelhante, Kumamoto e Henley (1996) afirmam que o incidente é resultado de uma falha ou de um distúrbio, como apresentado na Figura 2.2.

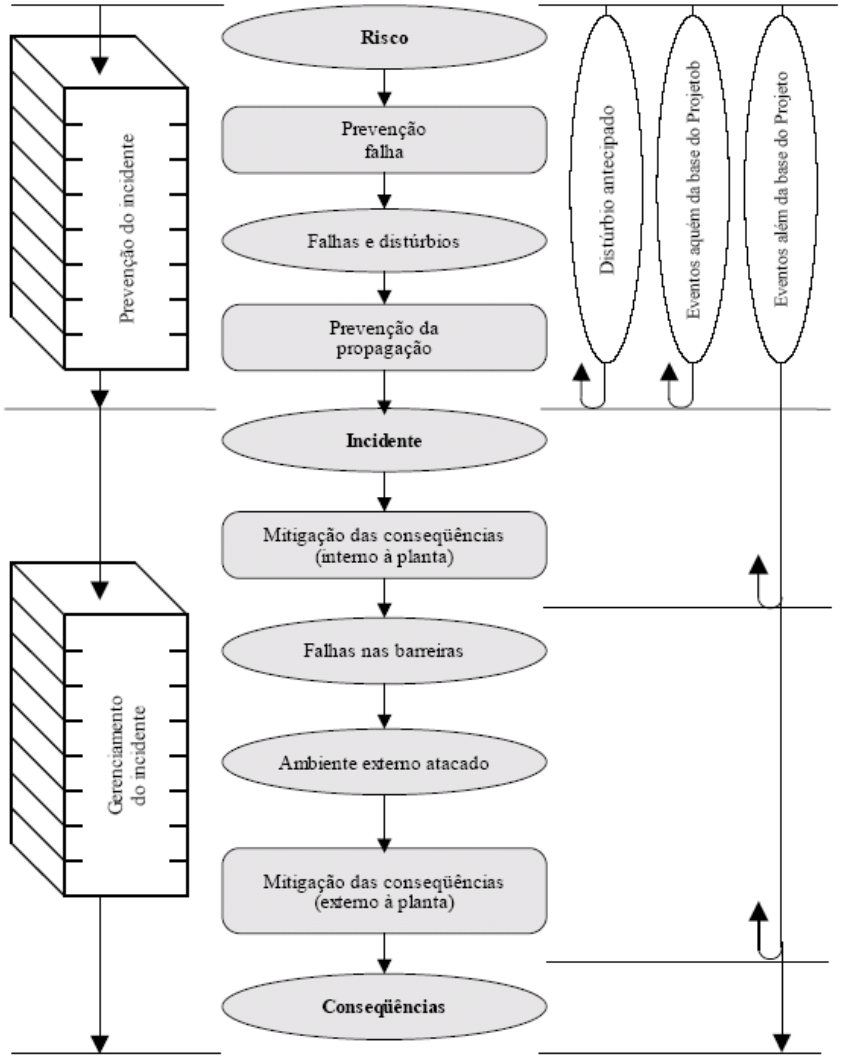



Figura 2.2 - Modelo de ocorrência de um incidente (adaptado de KUMAMOTO e HENLEY, 1996)

Na Figura 2.2, a trajetória do incidente está destacada em cinza. Nela, as elipses representam o estado do sistema ou componente e os retângulos as medidas para prevenir ou gerenciar o incidente (representadas pelas duas caixas à esquerda). Para os autores, a primeira medida para se prevenir o incidente é a prevenção da falha. Mas, dado a ocorrência da falha (ou de um distúrbio), pode-se prevenir sua propagação e, por conseqüência, o incidente – o que está representado pelas setas provenientes das duas elipses em branco, retornando no ponto que encontram a prevenção da propagação. No entanto, se a prevenção da propagação falha ou se o distúrbio supera as premissas de projeto (um vento acima do que a estrutura é capaz de suportar, por exemplo), o incidente irá ocorrer – o que está representado pela terceira elipse.

Nessa situação, pode-se agir no sentido de mitigar as conseqüências dentro da planta e não permitir que elas extrapolem os limites da organização. Os autores apresentam nessa condição a fase denominada de gerenciamento do incidente. No entanto, caso elas extrapolem, existe, ainda, a possibilidade de mitigar as conseqüências fora dos limites da organização – ou graves conseqüências ocorrerão.

## 2.3 Conceitos de prevenção de incidente

A constante evolução tecnológica tem resultado em produtos mais complexos. Da mesma maneira, nos casos mais perigosos, os riscos aos quais os consumidores ficam expostos crescem a cada ano. Novos materiais são constantemente desenvolvidos e incorporados aos produtos. Esses materiais, por sua vez, podem introduzir novos modos de falha aos produtos os quais podem ou não conter algum perigo. Esse perigo pode ou não evoluir para um risco e até gerar um incidente.

O número, diversidade e severidade de perigos que as pessoas estão expostas são consideráveis e vêm aumentando constantemente, demandando das organizações processos mais robustos para detecção, identificação e tratamento dos modos de falha. O ritmo das mudanças tecnológicas por muitas vezes não é acompanhado pela evolução dos processos de engenharia para a prevenção de incidentes. Quando os incidentes se manifestam, os custos para sua mitigação são por vezes altos. Há que se ressaltar, porém, que o conforto nas novas tecnologias leva a sociedade moderna, de forma geral, a aceitar o perigo presente nessas novas tecnologias.

Alguns conceitos errôneos têm sido assumidos e utilizados como desculpa pelas organizações para justificar a não implementação de processos focados na segurança. Hammer (1993) relaciona alguns destes conceitos, citados a seguir:

*a)* Segurança não vende. Um consumidor que compra um produto espera que ele seja seguro. Ele pode, portanto, não pagar mais por segurança, porém ele não comprará o produto se este tiver qualquer indício de que ele não seja seguro.

b) Falha é a principal causa de incidentes. Muitos ferimentos e danos a propriedades não são causados por falhas dos produtos e sim por características que expõem os consumidores aos riscos. Produtos que possuam sistemas dinâmicos, por exemplo, podem causar incidentes caso os sistemas de proteção concebidos não sejam utilizados ou ainda se algum ato inseguro é praticado pelo usuário do produto. Outros exemplos de características de produtos que podem causar incidentes:

• Sistemas de aquecimento – resistências incandescentes e outros tipos podem causar incidentes quando não instalados de maneira adequada;

• Sistemas elétricos – podem causar choque elétrico quando procedimentos de manutenção e ou limpeza não são seguidos.

c) Produtos que possuem certificação de um organismo acreditado é um produto seguro: Pode-se aqui chamar atenção para alguns mitos, ou crenças que nem sempre se confirmam. O certificado apenas atesta que o produto atende os requisitos de segurança a qual o produto foi confrontado. Esses requisitos de certificação, no entanto, podem ser inadequados para garantir que o produto seja seguro. Em muitas vezes, a certificação é feita para uma determinada probabilidade de ocorrência, exemplo $1x10^{-6}$ incidentes/falha, o que Kumamoto e Henley (1996) chamam de "aceitação do risco" (acidente automotivo). Existem outras situações em que há casos que produzem a "aversão do risco", como o de um acidente aéreo, nuclear, químico.

d) Um produto projetado e manufaturado de acordo com as normas vigentes para a indústria será um produto seguro: normas das indústrias definem os requisitos mínimos e usualmente não são suficientes para garantir a segurança dos produtos. Normas internas das organizações são geralmente melhores que as normas aplicadas pela indústria visto que as normas internas das organizações são focadas nos produtos por elas produzidas.

f) Fabricar um produto ou operação segura aumenta custos: Normalmente não aumenta o custo ao fabricar um produto seguro se ele for projetado e fabricado corretamente. Alterações para incremento da segurança e ou correção de problemas tendem a aumentar o custo. Segurança pode em alguns casos aumentar o custo de produção de um determinado produto, porém os seus custos tendem a ser menores quando se define ao longo do projeto para segurança

g) É muito difícil determinar os problemas de segurança de um produto antes de construí-lo: mas há um esforço muito grande em gerar métodos de análise que permitam gerar cenários de riscos dos produtos antes de construí-los fisicamente. Nos casos em que se dispõe de metodologia consolidada de projeto de produtos, as probabilidades de se definir os cenários de incidentes são mais seguras.

h) Se um produto é utilizado de forma inadequada, o fabricante não pode ser responsabilizado por qualquer dano: as cortes têm julgado que os fabricantes devem estar aptos a prever todos razoáveis possíveis usos para o produto. Autores como Reason (1997) consideram que há necessidade de considerar como de origem organizacional a causa principal da maioria dos incidentes.

i) Advertências de risco são defesas adequadas para garantir a segurança dos produtos: uma advertência é uma indicação de que o fabricante conhece o perigo presente e adverte para o risco. Uma advertência é justificável apenas quando não existe meio viável de eliminar o risco.

Alguns desses conceitos foram alterados devido à pressão econômica causada por perdas infligidas às indústrias em função de processos judiciais e perda de credibilidade perante os consumidores. Outro fator de mudança desses conceitos foram os programas de segurança desenvolvidos pela indústria bélica, aeroespacial e nuclear. Algumas idéias foram ainda desenvolvidas fora do âmbito da indústria bélica. A integração de todas essas idéias e conceitos dentro do processo de gerenciamento de risco e engenharia de segurança é um processo em constante evolução. O gerenciamento de risco deixa de ser uma verificação pontual e passa a ser um processo contínuo abrangendo todas as etapas de desenvolvimento e ciclo de vida dos produtos.

## 2.4 Segurança versus Confiabilidade

A relação entre os conceitos de segurança e confiabilidade deve ser abordada para um correto entendimento desses atributos no contexto do projeto de produto. Conforme Dias *et al.* (2005) esses dois atributos, por vezes, são considerados sinônimos, porém na grande maioria dos casos possuem objetivos conflitantes. Armas de fogo podem ser citadas como exemplos extremos de equipamentos que podem possuir alta confiabilidade, mas ainda assim são inseguros.

Devido a fatores como erro humano, meio ambiente e características específicas dos produtos presentes em qualquer projeto, a confiabilidade deve ser abordada não como o único, mas como um dos aspectos para incremento da segurança.

A confiabilidade de um sistema pode ser também expressa pela probabilidade de ocorrência de um determinado incidente conforme definem Kumamoto e Henley (1993).

Nesse contexto há de se considerar também o conceito de “falha aberta” e “falha fechada” no sentido de contribuir para o aumento da confiabilidade do sistema no que tange à segurança. Como exemplo, pode-se citar um sistema no qual a falha fechada permite passar energia enquanto a falha aberta interrompe sua passagem. Cada uma deve ser pensada para que a probabilidade de falha seja menor naquela com maior probabilidade de risco. O exemplo acima pode ser caracterizado tomando-se como referência o sistema de proteção contra superaquecimento de um motor elétrico aplicado a um condicionador de ar. Esse componente em condição normal de uso permite a passagem de corrente elétrica. A ocorrência de uma “falha aberta” no protetor térmico do motor implica na perda da função ventilação. A falha no caso irá afetar a confiabilidade do sistema para atender a função a qual foi projetado sem, no entanto, implicar em qualquer risco para o usuário do produto. Por outro lado, a ocorrência de uma “falha fechada” em um protetor térmico de um motor significa que ele não irá interromper o fluxo de energia ao motor quando solicitado. Nesse caso, a confiabilidade do sistema de ventilação é preservada, no entanto os perigos presentes nessa falha aumentam o risco consideravelmente.

A avaliação probabilística do risco é normalmente uma fase mais científica (KUMAMOTO e HENLEY, 1993), pois envolve analises técnicas, formais e quantitativas dos sistemas para identificar a probabilidade de falha. Idealmente a avaliação probabilística de risco deve ser baseada em dados cientificamente comprovados. Entretanto, é muitas vezes afetada pelo uso de dados subjetivos baseados na intuição, experiência pessoal, dados incompletos e teorias não comprovadas, constituindo as maiores fontes de incerteza na avaliação do risco.

A análise probabilística de risco requer informações não facilmente obtidas ou quantificadas tais como dados de confiabilidade de componentes e sistemas, índices de falha, severidade das falhas. Obviamente, a resultante de qualquer análise será tão boa quanto à qualidade dos dados de entrada. Portanto, a análise probabilística de risco tende a ser utilizada com mais freqüência quando boas informações estão disponíveis ou o projeto garante a geração dos dados necessários. Um dos aspectos de maior dificuldade da análise probabilística de risco é a determinação de qual quantidade de risco é desprezível e qual não é. Respondendo a essas difíceis perguntas antes de iniciar a análise podem-se melhorar os resultados.

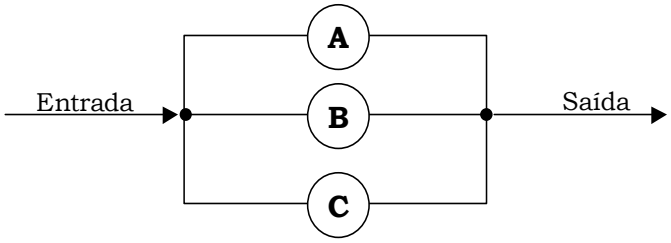
## 2.5 Sistemas redundantes

A aplicação de sistemas redundantes tem como objetivo principal minimizar a probabilidade do evento já conhecido causar a perda de uma função específica quando da ocorrência do evento. A aplicação da redundância pode ser resumida em dois objetivos principais: incremento da segurança e minimizar perdas por parada não prevista de um componente ou sistema.

Quando o foco é segurança, os sistemas redundantes são aplicados com mais freqüência em equipamentos cuja perda da função principal afeta a segurança do usuário. Neste contexto, Hammer (1993) salienta que a redução da taxa de falha obtida pela redução do estresse aplicado a componentes e sistemas é geralmente muito menor que as reduções obtidas pela aplicação de sistemas redundantes. Por outro lado, sistemas redundantes tendem a aumentar a complexidade e custo do produto final. Existem alguns tipos de arranjo usualmente aplicados:

a) Redundância em Paralelo Ativa – O sistema é projetado de forma que dois ou mais componentes, circuitos ou subsistemas, executam a mesma função simultaneamente. Desse modo, se uma ou mais unidades falham, as demais remanescentes ainda podem executar a função do produto. A Figura 2.3 apresenta um modelo com arranjo em paralelo ativo. Esse tipo de redundância é normalmente aplicado a produtos que requerem funcionamento contínuo, ou seja, quando a perda da função possa implicar em algum risco para o usuário do equipamento. Como exemplo, pode-se citar o sistema de freio de um automóvel. Também é utilizado quando a confiabilidade do componente individualmente não é admitida para uma determinada condição. Nesse arranjo, a confiabilidade do sistema é maior do que a do item individualmente, como pode ser visto no exemplo da Figura 2.3.

$R_A$ = Confiabilidade de A  $Q_A$ = Probabilidade de Falha de A
$R_B$ = Confiabilidade de B  $Q_B$ = Probabilidade de Falha de B
$R_C$ = Confiabilidade de C  $Q_C$ = Probabilidade de Falha de C
$R_{SAÍDA}$ = Confiabilidade do Sistema - Equipamento permanece em operação, a menos que A, B e C falhem simultaneamente.

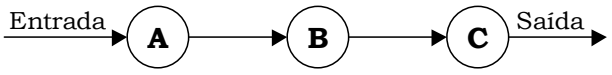



Considerando:
$R_A = R_B = R_C = 0,90$
$R_{SAÍDA} = 1 - Q_A.Q_B.Q_C$
$R_{SAÍDA} = 1 - (1 - R_A) . (1 - R_B) . (1 - R_C)$
$R_{SAÍDA} = 1 - (1 - 0,90) . (1 - 0,90) . (1 - 0,90)$
$R_{SAÍDA} = 1 - 0,001 = 0,999$

Figura 2.3 - Redundância dupla em paralelo (Adaptado de HAMMER, 1993)

b) Redundância em Série – Múltiplas unidades arranjadas em série em que todas devem operar para permitir uma saída constituem um arranjo de redundância em série. A figura 2.4 apresenta um modelo com arranjo em série. Esses arranjos são utilizados, geralmente, para prevenir eventos não desejados que pudessem causar algum incidente. Nos arranjos em série a falha de qualquer item do sistema leva à perda da função do sistema, o que diminui a confiabilidade. Contudo, para a segurança é bom dado que todos os itens em série devem falhar para que o incidente ocorra. Portanto, a probabilidade de ocorrência é geralmente baixa. Esse tipo de arranjo pode ser encontrado em sistemas de aquecimento nos quais a proteção contra superaquecimento do sistema é feita por dois ou três dispositivos instalados em série com o elemento de aquecimento. Nele, basta a atuação de um dos dispositivos existentes para que a proteção do sistema seja efetiva.

$R_A$ = Confiabilidade de A $Q_A$ = Probabilidade de Falha de A
$R_B$ = Confiabilidade de B $Q_B$ = Probabilidade de Falha de B
$R_C$ = Confiabilidade de C $Q_C$ = Probabilidade de Falha de C
$R_{SAÍDA}$ = Confiabilidade do Sistema de Proteção - Equipamento não irá operar a menos que A, B e C estejam operando simultaneamente.




Não haverá sinal de saída a menos que A, B e C estejam operando simultaneamente:
Considerando:
$R_A = R_B = R_C = 0,90$
$R_{SAÍDA} = 1 - Q_A.Q_B.Q_C$
$R_{SAÍDA} = 1 - 0,10 \times 0,10 \times 0,10$
$R_{SAÍDA} = 1 - 0,001 = 0,999$

Figura 2.4 - Redundância tripla em série (Adaptado de HAMMER, 1993)

## 2.6 Métodos e ferramentas aplicadas para análise de segurança e confiabilidade

O desenvolvimento da indústria aeroespacial foi o principal agente que potencializou a geração de ferramentas e metodologias de projeto focadas na segurança. Os custos econômicos e sociais resultantes de incidentes motivaram a criação de uma série de ferramentas e técnicas que permitissem a prevenção e detecção de situações que pudessem expor os usuários e equipamentos a riscos eminentes, desde o início da concepção do projeto até sua obsolescência. A complexidade dos sistemas e gama de situações em que poderiam ser aplicados ao longo do seu ciclo de vida tornaram necessária a utilização de técnicas qualitativas e quantitativas para análise, identificação e controle dos perigos inerentes ao projeto. Algumas dessas ferramentas são apresentadas a seguir.

### 2.6.1 FTA

FTA (*Fault Tree Analysis*) é uma ferramenta usada para análise de sistemas complexos. Ela foi originalmente desenvolvida pelos laboratórios Bell em 1961 para evitar desastres com mísseis na Força Aérea dos EUA. Seu objetivo é fazer relacionamentos causa-efeito para evidenciar o caminho crítico da falha, por isso o *cutset* é tão importante na FTA. Por *cutset* entende-se o conjunto de eventos que causam a ocorrência do evento topo. Um *cutset* pode ser um evento simples ou um conjunto de eventos. Diferentes *cutsets* podem incluir diferentes combinações para o mesmo evento

O FTA permite uma representação gráfica dos eventos não desejados indicando o inter-relacionamento entre eles. A partir de um evento topo (que pode ser originado do FMEA), pode-se visualizar toda a árvore de eventos que contribuem para a ocorrência do evento da falha em análise. Uma vez completada, os analistas podem utilizar a árvore para avaliar o sistema identificando o caminho crítico seja por número de eventos ou por probabilidade de ocorrência. Podem também identificar os eventos-chave (eventos que se não ocorrerem garantem que o evento topo não irá acontecer).

A análise quantitativa do FTA determina a probabilidade dos eventos e usa o relacionamento lógico entre eventos para calcular o risco do projeto. Como qualquer análise probabilística de risco, o FTA requer informações não facilmente obtidas ou quantificadas sendo, portanto, a qualidade da análise proporcional à qualidade dos dados nela utilizados.

O FTA proporciona alguns benefícios potenciais na análise de um sistema, tais como:

- Evidencia o inter-relacionamento entre componentes e falhas potenciais, que por vezes são dificilmente visualizadas no FMEA.
- Erro humano que contribui para a falha de um sistema pode ser identificado de modo mais evidente. Por exemplo: falha na rotina de manutenção de um sistema.
- Possibilita priorização de esforços e recursos atuando de forma mais efetiva na eliminação da falha.
- Possibilita também identificar de forma clara as causas, que podem ser imediatas, intermediárias ou causa raiz.
- Permite identificar componentes críticos para a segurança.
- Pode ser utilizado como ferramenta para investigação de incidentes.
- Possibilita avaliar mudanças de projetos.

### 2.6.2 FMECA / FMEA

A Associação Brasileira de Norma Técnicas (ABNT), na norma NBR 5462 (1994), adota a sigla originária do inglês FMEA (Failure Mode and Effects Analysis) e a traduz como sendo Análise dos Modos de Falha e seus Efeitos. Observa-se que a norma utiliza o termo pane para expressar falha. Ainda segundo a norma, o FMEA é um método qualitativo de análise de confiabilidade que envolve o estudo dos modos de falhas que podem existir para cada item, e a determinação dos efeitos de cada modo de falha sobre os outros itens e sobre a função específica do conjunto.

Tanto a FMEA quanto a FMECA buscam a excelência em qualidade e confiabilidade. A FMEA com o indicador de Risco e a FMECA com as criticidades de cada modo de falha e do produto estudado. Vale ressaltar que na FMECA, um estudo estatístico de confiabilidade é necessário, entretanto na FMEA os critérios que qualificam o Risco podem e devem ser rigorosos. Como neste projeto não serão diferenciadas as ferramentas, a denominação FMEA será utilizada de forma genérica para identificar ambas.

FMEA é uma técnica analítica utilizada por uma pessoa ou grupo de engenharia como uma maneira de garantir que, até onde o seu conhecimento for capaz de cobrir, os modos potenciais de falha, suas causas e os mecanismos associados tenham sido considerados e localizados. Na sua forma mais rigorosa, o FMEA é um sumário do conhecimento das pessoas do grupo de engenharia, sobre uma análise de itens que poderiam falhar, com base na experiência e em assuntos passados, de como um produto ou processo é desenvolvido.

Na execução de uma análise quantitativa, analistas deveriam quantificar o risco pelo uso de uma probabilidade de ocorrência e severidade. Infelizmente tais informações freqüentemente não existem e podem ser difíceis de serem obtidas. Na sua ausência, a qualidade da análise quantitativa e, portanto sua validade, pode ser muito prejudicada,

Entretanto o FMEA é particularmente bem sucedido quando os usuários não estão certos de que problemas podem ocorrer ou como pequenos problemas podem preceder problemas de maior gravidade. Esse tipo de análise é muito efetivo para sistemas nos quais a interação entre falhas é de baixa complexidade.

Algumas abordagens diferenciadas do FMEA procuram priorizar o quesito segurança. Uma das formas atualmente aplicadas relaciona-se com a composição do índice “SOD” (severidade, ocorrência e detecção). Usualmente adotado como a multiplicação dos três índices, o SOD passa a ser adotado como a combinação dos três índices priorizando sempre a severidade (Figura 2.5).

| Componente / Sistema | Função | Potencial Modo de Falha | Potencial Efeito da Falha | Sev | Potencial Causa do Mecanismo de Falha | Ocorr | Atual Controle de Projeto | Detec | SOD |
|---|---|---|---|---|---|---|---|---|---|
| Sistema de Aterramento | Garantir integridade do usuario durante uso do produto | Não garantir integridade do usuario | Choque elétrico | 9 | Fixação do fio terra não efetiva | 3 | torque mínimo de 2 Kgf.m | 2 | 932 |

Figura 2.5 – Determinação índice "SOD" priorizando a segurança (Adaptado de Whirlpool Corporate Product Safety, 2003)

FMEA é uma ferramenta que pode e deve se estender por praticamente todas as fases do projeto. Deve ser iniciada na fase conceitual para auxílio na escolha do conceito e se estender até a fase teste de aprovação final, para validação do projeto e do produto. A Figura 2.6 apresenta uma revisão do modelo de integração do FMEA nas diferentes fases de projeto proposto pelo Centro de Pesquisa Lewis (NASA). Nesse modelo foram adicionadas as informações provenientes da pós-venda referente a hábitos de uso, falhas evidenciadas e ainda incidentes que possam ter ocorrido. Esses dados devem retornar como fonte de atualização do projeto ou ainda como banco de dados para futuros projetos de produtos similares.

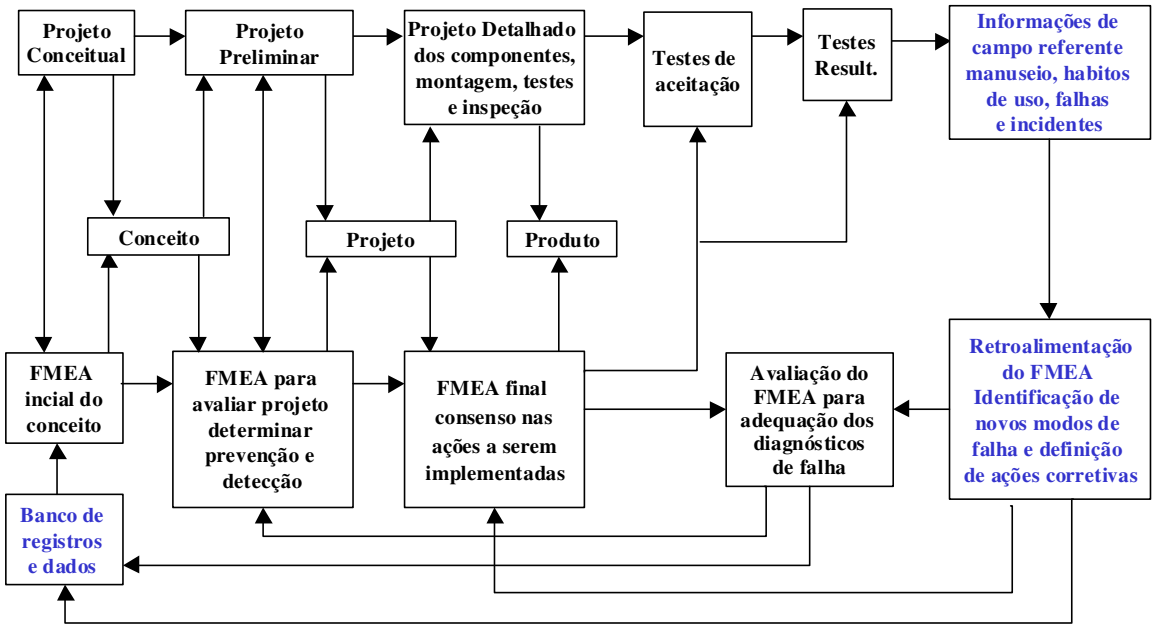



Figura 2.6 – Revisão do modelo de integração do FMEA as fases de projeto proposto pelo Centro de Pesquisa Lewis (Adaptada de NASA, 2003)

2.6.3 Ferramenta para classificação e mitigação de risco (PHM)

PHM (*Product Hazard Management)*, segundo a Whirlpool Corporate Product Safety (2003) é um processo desenvolvido pela *Whirlpool Corporation* com objetivo de avaliar e documentar os potenciais riscos de segurança e as ações tomadas para o seu tratamento. O processo direciona a solução do problema de forma hierárquica priorizando na ordem: alteração do projeto para eliminação do risco, inclusão de salvaguardas, criação de controle e por fim inclusão de avisos de advertência. Possibilita também uma classificação dos riscos quanto a sua gravidade e probabilidade de ocorrência direcionando e definindo a necessidade de tomada de ação. O processo em questão é reconhecido pela *U.S. Consumer Product Safety Commission*[2] como uma das melhores práticas da indústria americana, referente ao tratamento dos aspectos de segurança de produtos. O PHM é uma ferramenta que estimula e disciplina o raciocínio crítico dos engenheiros e pode ser aplicada isoladamente para tratamento de risco potencial identificado ou ainda em complementação a outras ferramentas como FMEA, auxiliando na documentação e fechamento dos itens identificados.

**SEVERIDADE**

| | | | | | |
|---|---|---|---|---|---|
| **Risco de Vida** | X ← X | | | | |
| **Dano Pessoal Grave** | X ← X | | | | |
| **Dano Pessoal Médio ou Grave Dano à Propriedade** | | X | | | |
| **Dano Pessoal Pequeno ou Dano a Propriedade** | | | X | | |
| **Dano ao Produto** | | | X | | |
| | **Impossível/ Improvável** Não pode ser distinguido de zero | **Remoto** Não provável, mas possível de ocorrer | **Ocasional** Possível de ocorrer algumas vezes | **Provável** Possível de ocorrer várias vezes | **Freqüente** Possível de ocorrer repetidamente |

**Probabilidade de Ocorrência**

Figura 2.7 - Matriz PHM – Severidade X Probabilidade de Ocorrência (Whirlpool Corporate Product Safety, 2003)

A Figura 2.7 apresenta a matriz inicial para classificação do risco em função de sua severidade e probabilidade de ocorrência, sempre que a classificação acontecer na área cinza

[2] Ou Comissão de Segurança de Produtos ao Consumidor dos Estados Unidos é a agência reguladora responsável pelo Código de Regulamentos Federal (*Code of Federal Regulations-CFR*). Criada em 1972 pela *Consumer Product Safety Act*, tem como objetivo proteger consumidores de riscos de lesões associados a produtos de consumo. Nota do autor.

uma ação deve ser tomada obedecendo a hierarquia para eliminação do risco apresentada na Tabela 2.1 de forma a reposicionar a classificação na área branca.

Tabela 2.1 – PHM – Hierarquia para tratamento dos riscos (Whirlpool Corporate Product Safety, 2003)

| | OPÇÕES | SIM/ NÃO | AÇÃO NECESSÁRIA SE A RESPOSTA FOR SIM |
|---|---|---|---|
| **1** | Pode o risco ser razoavelmente eliminado? | | Alterar o projeto |
| | Explique a resposta. | | |
| **2** | Pode o risco ser razoavelmente protegido? | | Alterar o projeto |
| | Explique a resposta. | | |
| **3** | Pode o risco ser razoavelmente controlado por uma mudança de processo? | | Alterar o processo |
| | Explique a resposta. | | |
| **4** | Risco está classificado na área Branca? | | Nenhuma ação |
| **5** | É o risco um risco óbvio? | | Nenhuma ação |
| **6** | Comunicação de risco é necessária? | | Desenvolver comunicação de risco |
| **7** | O risco é menor ou igual às normas existentes na indústria? | | Nenhuma ação |

### 2.6.4 Listas de verificação

A utilização de listas de verificação é uma das maneiras mais efetivas e estruturadas para identificar as características e ou falhas que possam vir a afetar a segurança do produto ao longo do seu ciclo de vida. Hammer (1993) apresenta alguns modelos de listas de verificações, que segundo o autor disciplinam o raciocínio dos projetistas induzindo-os a avaliar uma vasta gama de questões que envolvem da especificação às diferentes situações de uso do produto. Blanchard *et al.* (2005) apresentam uma lista de verificação genérica, a qual segundo os autores, pode ser utilizada para caracterizar se o sistema incorpora características de boa mantenabilidade. Muitas das questões relacionadas por Blanchard *et al.* envolvem itens relacionados à segurança do sistema e podem ser utilizadas como base na formulação de formulários específicos para determinados produtos.

Entende-se que maior é a efetividade das listas de verificação quanto mais forem focadas, elaboradas e atualizadas com base nos produtos a que serão aplicadas. As listas de verificação auxiliam na identificação de possíveis situações de risco. No entanto, elas por si só não conduzem a uma solução efetiva do problema identificado. Para tal, a utilização de

listas de verificação deve estar sempre associada a outras ferramentas de projeto para garantir que as informações geradas pela análise sejam tratadas de forma adequada. A integração destas informações e uso de outras ferramentas é um dos objetivos desta dissertação. Um modelo de lista de verificação focada para condicionadores de ar será apresentado no Apêndice 2 deste trabalho.

## 2.7 Normas Técnicas

No Brasil, a Portaria n.º14, de 24 de janeiro de 2006, define requisitos de segurança para condicionadores de ar a serem comercializados no mercado brasileiro. Esse regulamento tem como base a Norma Mercosul NM 60335-1 (2006) – Segurança de aparelhos eletrodomésticos e similares. A NM 60335-1 (2006) é complementada pela norma específica para condicionadores de ar IEC 60335-2-40 (2005) – *Particular requirements for electrical heat pumps, air-conditioners and dehumidifiers.*

Essas normas definem os requisitos gerais e específicos que os produtos devem atender para serem considerados em conformidade com os padrões mínimos de segurança. Por se tratar de uma norma de verificação de conformidade, o foco principal está na verificação do cumprimento dos requisitos técnicos. Portanto, poucas são as informações, conceitos e determinações que poderão ser levadas em consideração nas fases informacional e conceitual do projeto sem que haja um conhecimento profundo dos engenheiros e projetistas para interpretação e tradução desses requisitos em soluções de projeto.

Este trabalho tem como objetivo organizar as informações contidas nestas normas tornando-as mais acessíveis aos projetistas. As normas específicas de um determinado segmento da indústria definem os critérios mínimos de conformidade que determinado produto deve atender para ser considerada como tendo sua segurança de acordo com o padrão mínimo estabelecido. Na busca por produtos mais seguros, normas estabelecidas para outros seguimentos podem e devem ser pesquisadas e incorporadas sempre que possam trazer algum benefício para a segurança. Um exemplo dessa prática seria a aplicação no projeto de eletrodomésticos da norma CPS04 – *Chocking Hazard* desenvolvida originalmente para a indústria de brinquedos. Essa norma define tamanho mínimo e força mínima de extração de peças que podem ser removidas do produto com o objetivo de evitar que as peças sejam removidas e engolidas por crianças causando risco de sufocamento. Apesar de ser um requisito não encontrado na normatização específica para a indústria de eletrodomésticos, pode ser aplicada na sua plenitude para incremento da segurança do produto.

## 2.8 Comentários finais

Em linha geral, tanto o modelo da corrente causal (MOSLEH e DIAS, 2004) quanto o modelo proposto por Kumamoto e Henley (1996), evidenciam que o incidente é resultado de uma condição perigosa mais um evento deflagrador (gatilho), e uma ineficiência das barreiras feitas com fim específico de conter o incidente. A importância do estudo da segurança, aliado ao estudo da confiabilidade dá-se em face do incremento tecnológico dos sistemas, em complexidade e em quantidade de fontes e eventos portadores de perigo

Esse aumento de complexidade gera uma deficiência no processo de projeto no que tange ao tratamento do atributo segurança levando as organizações, conforme Hammer (1993), a assumir e utilizar uma série de conceitos errôneos os quais têm sido utilizados como desculpa para justificar a não implementação de processos focados na segurança.

Nesse contexto fica evidente que o processo de projeto utilizado pelas organizações deve ser atualizado para que o atributo segurança seja tratado adequadamente.

Este trabalho está focado em detalhar aspectos relacionados com os recursos, fontes de perigo e propor facilidades para utilizar métodos e ferramentas para evidenciar aos projetistas as ações que devem ser feitas para projetar sistemas mais seguros.

# CAPITULO 3
# PROJETO DE PRODUTO PARA SEGURANÇA

## 3.1 Introdução

Diversas sistemáticas de projeto podem ser encontradas na literatura, como as apresentadas por Romano (2003), Back (1983) ou Dias *et al.* (2007). O projeto de engenharia é entendido de forma muito semelhante pelos autores que estudam metodologia de projeto. A abordagem sistemática da atividade de projeto pode ser percebida na definição de projeto apresentada por Roozenburg & Eekels (1995) que entendem o projeto de um produto como um processo mental orientado, pelo qual problemas são analisados, objetivos são definidos e ajustados, propostas de soluções são definidas e a qualidade dessas soluções são medidas.

De uma forma geral, as sistemáticas de projeto abordam fases similares do projeto: projeto informacional, projeto conceitual, projeto preliminar e projeto detalhado. Algumas caracterizam ainda o projeto informacional de fase de requisitos e necessidades.

Como enfatizado por Alonço (2004), em geral, os autores que se dedicam ao aprimoramento da metodologia de projeto como um todo, salientam em diferentes fases do processo de projeto o atributo segurança, porém as metodologias não priorizam a segurança em relação a outros requisitos como desempenho, custo, estética etc. Também se pode observar nessas metodologias que existe uma clara deficiência nas orientações de como tratar o atributo segurança e de como relacioná-lo com os demais requisitos de projeto. Entende-se que o procedimento está correto, dado que o projeto é desenvolvido para obter-se um determinado desempenho. No entanto, relegar a segurança a um segundo plano ou não considerá-la pode criar uma bomba de efeito retardado que ao "explodir" gera reflexos negativos para o produto, nome da empresa e até sua falência em face dos custos relacionados com os danos advindos da negligência ou ignorância em relação à segurança. São exemplos de *recall* recentes:

- Eletrodomésticos – Carrier EUA efetuou chamada para *recall* de 185.000 produtos comercializados de Janeiro de 2002 a dezembro de 2006. Causa: superaquecimento dos terminais elétricos podendo causar risco de chama externa ao produto (*U.S. Consumer Product Safety Commission*, 2008).
- Eletrodomésticos – Whirlpool EUA efetuou chamada para *recall* de 1.400.000 produtos. Causa: união deficiente do terminal ao fio causando superaquecimento e queima total do produto (*U.S. Consumer Product Safety Commission*, 2008).

- Automotiva – Fiat Brasil convocou para reparo na direção hidráulica e mangueira de combustível do modelo Tipo fabricado entre 1993 e 1995. (http://www.estradas.com.br/, 2008)
- Automotiva – GM EUA condenada a pagar US$ 4,9 bilhões a consumidor que sofreu graves queimaduras, devido à explosão de um tanque de combustível de um modelo da GM. (*U.S. Consumer Product Safety Commission*, 2008)
- Automotiva – Firestone EUA anuncia substituição de 6,5 milhões de pneus. Falha no pneu pode ter sido responsável por 46 mortes e centenas de acidentes. Custo aproximado do *recall* de 1 bilhão de dólares. (*U.S. Consumer Product Safety Commission*, 2008)

Neste capítulo serão concentrados esforços no sentido de evidenciar os aspectos de segurança nos modelos e metodologias encontrados na literatura a fim de propiciar maior facilidade de acesso às informações referentes ao assunto de forma a serem consideradas pelo time de projeto no tratamento do atributo segurança.

## 3.2 Processo atual de desenvolvimento de produto

Em geral os modelos de processo de projeto de produto orientam o time de projeto sobre as etapas a serem cumpridas e recursos a serem utilizados para a execução de um projeto de produto. Esses modelos, na sua maioria, são modelos genéricos e expressam "o que" o time de projeto deve fazer, desde a identificação do problema até a documentação final.

Particularmente, considerando-se os modelos de procedimentos de projeto, não se encontram evidências claras sobre os caminhos ou as diretrizes para o processo de como capturar e utilizar as informações e experiências existentes, principalmente nas fases iniciais do projeto. Esses modelos também não definem, de forma consistente quando transportados para um segmento específico da indústria, quais ferramentas são mais adequadas e qual o momento ideal para sua aplicação. Como comentado anteriormente são modelos genéricos que tratam mais sobre "o que" fazer e pouco sobre o "como" e "quando" fazer.

Para uma análise mais detalhada será utilizado o modelo de processo de desenvolvimento de produto desenvolvido pelo NeDIP (Figura 3.1), que por ser um modelo onde a segurança não é o foco principal pode evidenciar mais claramente as deficiências no tratamento do atributo segurança. Esse modelo compreende três macro-fases do processo desenvolvimento, planejamento, projetação e implementação, que, por sua vez são

desdobradas em fases constituídas de diversas tarefas, cuja execução irá gerar uma série de conhecimentos na forma de documentação e registros definidos como “saídas”.

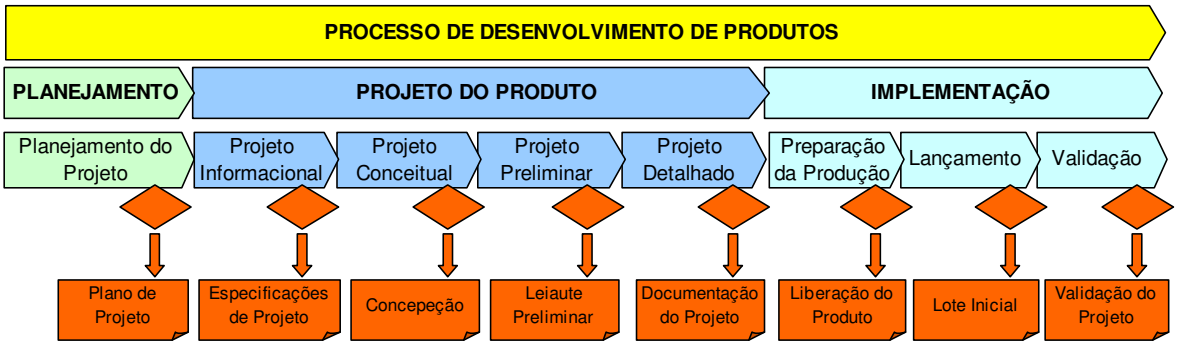



Figura 3.1 - Modelo Processo de Desenvolvimento de Produto (adaptado de ROMANO, 2003)

A macro-fase planejamento define o início formal do projeto e nela é elaborado o planejamento de *marketing*, o plano de projeto, o plano de qualidade e a definição da política de segurança e são estabelecidas as metas de segurança a serem atendidas com o novo projeto. O modelo em análise prevê nessa fase o estabelecimento da política de segurança do produto, porém não fica claro onde devem ser buscadas as informações para elaboração de tal política. Projetos de novos produtos em um determinado segmento da indústria tendem a ser muito similares a projetos anteriores, portanto, na definição da política, a segurança deve ser incorporada a todo o aprendizado obtido com projetos similares. Esse aprendizado pode ser originado de boas práticas implementadas em projetos anteriores ou ainda devido a incidentes vivenciados com produtos similares.

Entre as três macro-fases da Figura 3.1, a fase do projeto do produto é, sem dúvida, a que atua no tratamento e análise dos requisitos de segurança. Nessa etapa do projeto os requisitos de segurança são relacionados aos modos de falha que possam ocasionar incidentes mapeados e soluções de projetos são adotadas para endereçar os problemas identificados.

Quadro 3.1 – Desdobramento das fases do projeto (Adaptado de ROMANO, 2003)

**Projeto Informacional**

| Entradas | Atividades | Tarefas | Domínios | Mecanismos | Controles | Saídas |
|---|---|---|---|---|---|---|
| Política de segurança | Levantar informações sobre segurança no ciclo de vida | Revisar histórico de segurança dos produtos disponíveis no mercado ou similares | SE | Banco de dados sobre segurança | Avaliação dos disponíveis no mercado "I" e "II" | Informações sobre segurança |
| | | Avaliar risco de acidente e/ou possibilidade de mau uso ao longo do ciclo de vida | SE | Análise de risco | Ciclo de vida do prod. | |
| | | Identificar as especificações de projeto que se relacionam com as metas de segurança | SE | Análise de especialista | Especificações de projeto | |
| | | Anexar informações sobre segurança ao sistema de documentação do projeto | GP | Sistema de documentação do projeto | Plano de gerenciamento da qualidade<br>Plano de gerenciamento das comunicações | |

**Projeto Conceitual**

| Entradas | Atividades | Tarefas | Domínios | Mecanismos | Controles | Saídas |
|---|---|---|---|---|---|---|
| Informações sobre segurança do produto<br>Concepção/conceito do produto | Realizar estudo inicial de segurança sobre a concepção do produto | Revisar e incorporar as normas de segurança existentes no desenvolvimento da concepção | SE | Análise de risco<br>Normas de segurança<br>Banco de dados sobre segurança | Política de segurança do produto | Informações sobre segurança do produto |
| | | Anexar informações sobre segurança ao sistema de documentação do projeto | GP | Sistema de documentação do projeto | Plano de gerenciamento da qualidade<br>Plano de gerenciamento das comunicações | |

**Projeto Preliminar**

| Entradas | Atividades | Tarefas | Domínios | Mecanismos | Controles | Saídas |
|---|---|---|---|---|---|---|
| Informações sobre segurança do produto | Realizar análise de segurança sobre o leiaute final do produto | Revisar o atendimento às metas de segurança | SE | Análise de especialista | Política da segurança | Informações sobre segurança do produto |
| | | Anexar informações sobre segurança ao sistema de documentação do projeto | GP | Sistema de documentação do projeto | Plano de gerenciamento das comunicações<br>Plano de gerenciamento da qualidade | |

**Projeto Detalhado**

| Entradas | Atividades | Tarefas | Domínios | Mecanismos | Controles | Saídas |
|---|---|---|---|---|---|---|
| Informações sobre segurança do produto<br>Requisição de protótipo | Realizar análise de segurança do protótipo e/ou componentes | Analisar protótipo | SE | Análise de especialista | Política de segurança | Relatório de segurança do protótipo |
| | | Verificar o atendimento do protótipo às metas de segurança durante os testes de laboratório e de campo | SE | Observação<br>Normas de segurança | | |
| | | Elaborar e emitir relatório de segurança do protótipo com ações corretivas caso necessário | SE | Relatório de segurança do protótipo | Plano de gerenciamento das comunicações | |
| | | Anexar o relatório de segurança do protótipo ao sistema de documentação do projeto | GP | Sistema de documentação do projeto | Plano de gerenciamento das comunicações<br>Plano de gerenciamento da qualidade | |

Em síntese a macro-fase de projeto do produto inicia-se com as informações de mercado, incluindo-se os interesses ou as manifestações dos clientes do projeto os quais abrangem toda cadeia do ciclo de vida tais como: manufatura, logística, revenda, assistência técnica, utilização pelo consumidor final e outros. Tais informações são transformadas em especificações de projeto, ou seja, informações genéricas são transformadas em requisitos quantificados constituindo os principais problemas técnicos a serem resolvidos. Esse processo de transformação é denominado de projeto informacional do produto. Nessa etapa o processo proposto se limita a definir algumas tarefas como: identificar as normas técnicas que se relacionam com o projeto; avaliar as expectativas dos usuários sobre as características de segurança; levantar informações sobre segurança ao longo o ciclo de vida.

No que tange à tarefa avaliar as expectativas dos usuários entende-se que tal atividade é de baixa eficácia, visto que os usuários raramente possuem conhecimento técnico de forma que possam identificar algo diferente do avaliado pelo corpo técnico do time de projeto.

A fase seguinte denomina-se projeto conceitual, e como o nome sugere define o conceito que melhor atende as especificações de projeto, ainda em forma qualitativa representa as principais funções e princípios de solução esboçados para o projeto.

A partir do conceito selecionado o projeto é desenvolvido de acordo com critérios técnicos e econômicos e a luz de informações adicionais, até o ponto de configurar o leiaute do produto, que é de natureza quantitativa com o arranjo geral dos elementos que caracterizam as formas e geometria do produto. Essa fase denomina-se projeto preliminar do produto.

Por último, desenvolve-se o projeto detalhado e nessa fase o objetivo é desenvolver e finalizar o projeto, no sentido de serem concluídos desenhos, documentações e o planejamento para a produção, para então ser encaminhado à manufatura.

O Quadro 3.1 apresenta o desdobramento das tarefas relativas à segurança para as etapas do projeto informacional, conceitual, preliminar e detalhado. Existe certo grau de detalhamento em “o que” deve ser feito sem, entretanto, definir o “como” e de que forma essas informações serão integradas efetivamente e eficazmente ao processo de projeto e traduzidas em ações para mitigação dos problemas relativos à segurança. Ao mesmo tempo algumas tarefas aparecem de forma repetitiva nas diversas fases do projeto sem, no entanto, ficar evidenciada a conexão entre essas e outras atividades relacionadas à inserção do atributo segurança ao projeto do produto.

### 3.3 Teoria em projeto para a segurança

Alonço (2004) resume de forma concisa os resultados de trabalhos e proposições de metodologias desenvolvidas por diversos autores como Lima (1985), Carpes Junior (2001), Barone *et al.* (2000), Pahl & Beitz (1996), Pighini (2000), entre outros. A partir daí fez-se novas proposições e pretende-se agregar alguns novos conceitos e abordagens sobre o atributo segurança no processo de projeto.

O foco natural da engenharia simultânea é no projeto do produto. Uma decisão relativa ao projeto do produto tende a ter um número significativo de impactos sobre o ciclo de vida do produto. A figura a seguir evidencia a interação da segurança.

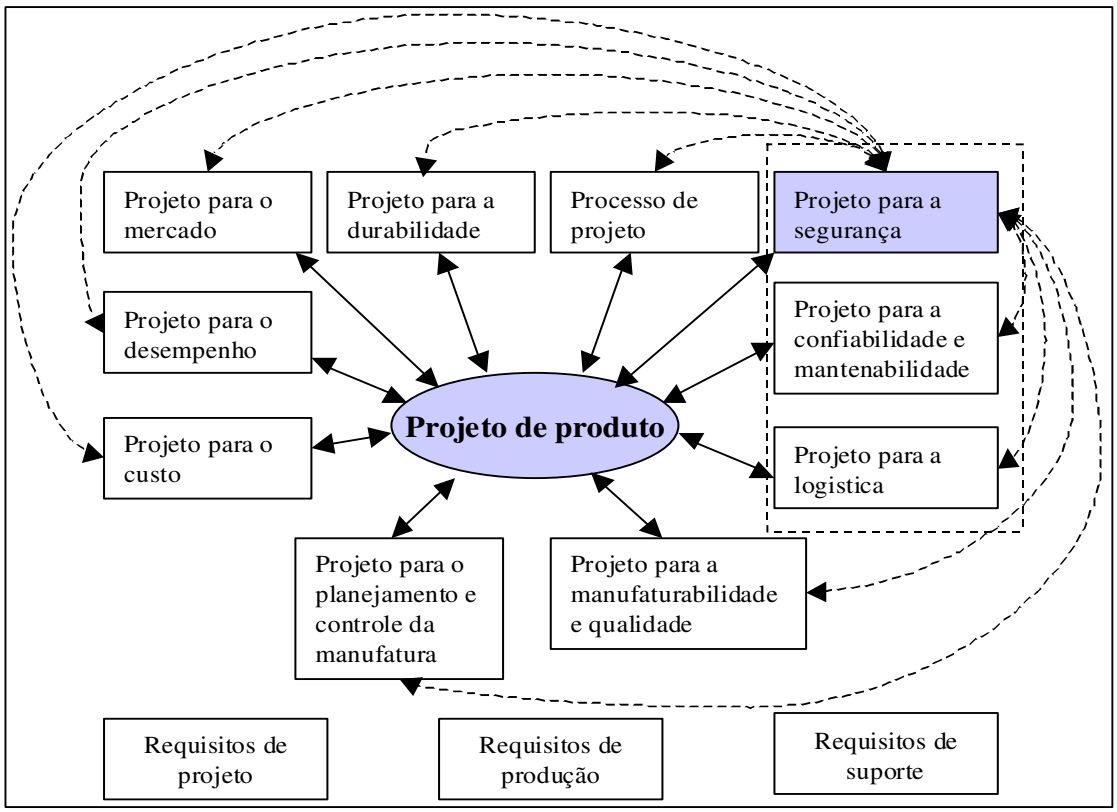



Figura 3.2 – Interação da segurança com as diversas áreas de foco no processo de projeto de produto (Adaptado de DOWLATSHAHI, 2001)

Dowlatshahi (2001) propõe que produtos projetados em um ambiente de engenharia simultânea empregam uma abordagem interdisciplinar que utiliza métodos, procedimentos e regras para planejar, analisar, selecionar e otimizar o projeto do produto. A Figura 3.2 estabelece uma estrutura conceitual onde a interação entre as várias áreas funcionais em um ambiente de engenharia simultânea pode ser explorada e analisada. As áreas funcionais

apresentadas na Figura 3.2 têm relação com todas as etapas do ciclo de vida do produto desde a conceituação até o descarte.

O processo de projeto de produto tradicional considera fatores tais como custo, durabilidade, mercado, desempenho, manufaturabilidade e outros como apresentado na Figura 3.2. Entretanto, poderiam ser incluídos fatores adicionais tais como: estética, capacidade, ergonomia, intercambiabilidade, mantenabilidade, confiabilidade, testabilidade, entre outros. Cada um destes relacionamentos poderia ser explorado, analisado individualmente. Algumas das áreas relacionadas na Figura 3.2 mesmo não tendo como foco principal a segurança, de uma ou de outra forma interagem com ela. Portanto, qualquer análise focada no projeto para a segurança deve considerar a interação com os outros atributos presentes na Figura 3.2. Essa interação adiciona certa complexidade ao processo de engenharia simultânea, porém ao mesmo tempo oportuniza a simultaneidade. O foco no projeto para segurança na interação com outras áreas pode gerar um diferencial competitivo pela otimização de soluções evitando custos adicionais para garantir a segurança do produto.

Para Dowlatshahi (2001) existem quatro distintas, porém inter-relacionadas, áreas de entrada que formam a percepção do que é um produto seguro. Elas são classificadas em termos de entradas forçadas e voluntárias, sendo as mesmas respectivamente; processos civis, regulamentação governamental, políticas internas de segurança e *marketing*, conforme apresentado na Figura 3.3.

Em termos de processos civis as experiências negativas vivenciadas pelas empresas ou por concorrentes do segmento tendem a alterar a percepção dos fabricantes sobre o conceito de produto seguro direcionando ações para evitar que tais experiências se repitam no futuro.

Regulamentação governamental é outra importante entrada. Essas regulamentações fornecem o direcionamento para que um determinado projeto seja desenvolvido de forma a garantir as condições mínimas de segurança ao produto.

Políticas internas de segurança são normalmente programas voluntários iniciados pelas empresas para o desenvolvimento e produção de produtos seguros. De forma geral, essas políticas internas de segurança são as mais efetivas para garantir a segurança dos produtos, pois são feitas de forma voluntária e possivelmente internalizadas na cultura da empresa.

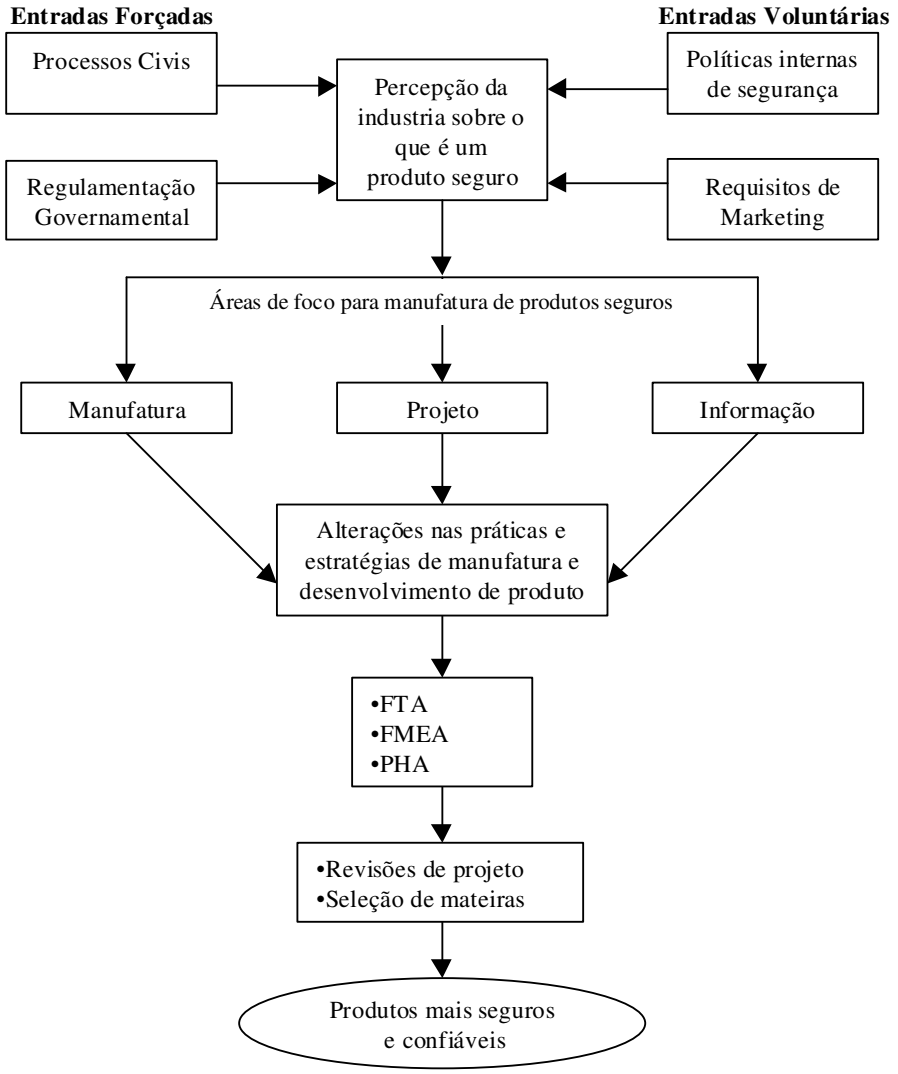



Figura 3.3 - Estrutura conceitual de projeto para a segurança (DOWLATSHAHI, 2001)

A percepção de produto seguro é também afetada pelos requisitos de mercados, ou seja, pelo o que o consumidor entende como produto seguro. Essa percepção do consumidor muitas vezes leva as empresas a introduzirem acessórios e/ou funções em seus produtos de forma a transmitir a idéia de segurança ao consumidor. *Air bags* introduzidos pela indústria automobilística é um típico exemplo de um requisito do mercado.

Conforme Dowlatshahi (2001) a combinação desses dados de entrada proporciona as bases para a criação de um programa para desenvolvimento de produtos seguros. Esse programa deve estar focado em três etapas do desenvolvimento de produto visando eliminar três fontes de problemas distintas, porém diretamente relacionadas: projeto, manufatura e informação ao usuário sobre condições não seguras durante o uso do produto. Detalhamento das três etapas é apresentado no Quadro 3.2.

Quadro 3.2 – Etapas de desenvolvimento de produto (DOWLATSHAHI, 2001)

| **Foco no Projeto** | **Foco na Manufatura** | **Foco na Informação** |
|---|---|---|
| Projeto é o fator de maior importância para garantir a segurança do produto. O projeto de um produto seguro pode ser obtido efetiva e economicamente se três etapas forem seguidas:<br>• *Projeto dos sistemas* – esta é uma atividade que envolve a seleção das arquiteturas e tecnologias para atingir a função desejada no produto.<br>• *Projeto dos parâmetros* – este é um estágio onde a segurança pode ser incorporada aos sistemas sem qualquer incremento de custo.<br>• *Projeto das tolerâncias* – se o produto demanda segurança adicional além do que é possível no projeto dos parâmetros, então isto pode possivelmente ser feito com acréscimo de custo. Nesse estágio, materiais mais especificados podem ser utilizados para melhorar a performance, qualidade ou segurança do produto. | Não importa quão cuidadosamente um produto é projetado se não for manufaturado corretamente pode não resultar num produto seguro. Se um produto ou produção não atende a especificação de projeto e de algum modo não é detectado e atinge o mercado então o defeito resultante é um defeito de manufatura. Problemas podem também ser verificados quando algum material não atende a especificação ou mesmo quando o material incorreto é utilizado. | Um produto mesmo que livre de defeitos de projeto ou manufatura pode ainda assim ser perigoso para o consumidor, quando advertências ou outras instruções não são fornecidas. O produto deve vir com instruções sobre como evitar riscos potenciais. Avisos de advertência ou instruções de uso inadequadas são considerados defeitos e sujeitos a processos civis. Smith e Talbot (1991) sugerem que um defeito devido a uma informação inadequada existe quando:<br>• Falha em prover qualquer advertência do perigo e risco envolvido com o uso do produto<br>• Falha em prover advertência adequada do perigo e risco envolvido com o uso do produto<br>• Falha em prover intrusões adequadas para o uso seguro do produto |

De La Garza e Fadier (2006) abordam a questão da segurança nos projetos considerando que apesar da introdução de novas tecnologias e abundância de novas regulamentações e normas técnicas, as margens de segurança permanecem insuficientes e os riscos residuais ainda são significantes. Essa situação pode ser explicada por três fenômenos:

a) Migração na fronteira dos sistemas

Nesse contexto, Rasmussen (1997) desenvolveu a idéia de que existe uma migração natural em direção às fronteiras de performance aceitável. Para o autor, a causa principal dos acidentes está relacionada ao comportamento das organizações sob forte pressão competitiva em busca de maior eficiência.

A margem para ação pode ser representada por um “envelope”. Dentro dos limites representados as ações e decisões permanecem aceitáveis de acordo com os diferentes critérios (Figura 3.4).

Quando a pressão é colocada em um dos eixos, por exemplo, a produtividade a ação irá aproximar a fronteira oposta do “envelope”. O espaço no interior das fronteiras pode ser definido como espaço de possibilidades, ou seja, define a amplitude das ações e decisões para

que não ocorra ruptura das fronteiras do projeto. A interação entre os limites das fronteiras é única para cada projeto e dependente de diversos fatores ao longo do ciclo de vida do produto. Também há de se considerar uma migração natural dos limites ao longo do ciclo de vida do produto, principalmente referente às fronteiras de performance e segurança.

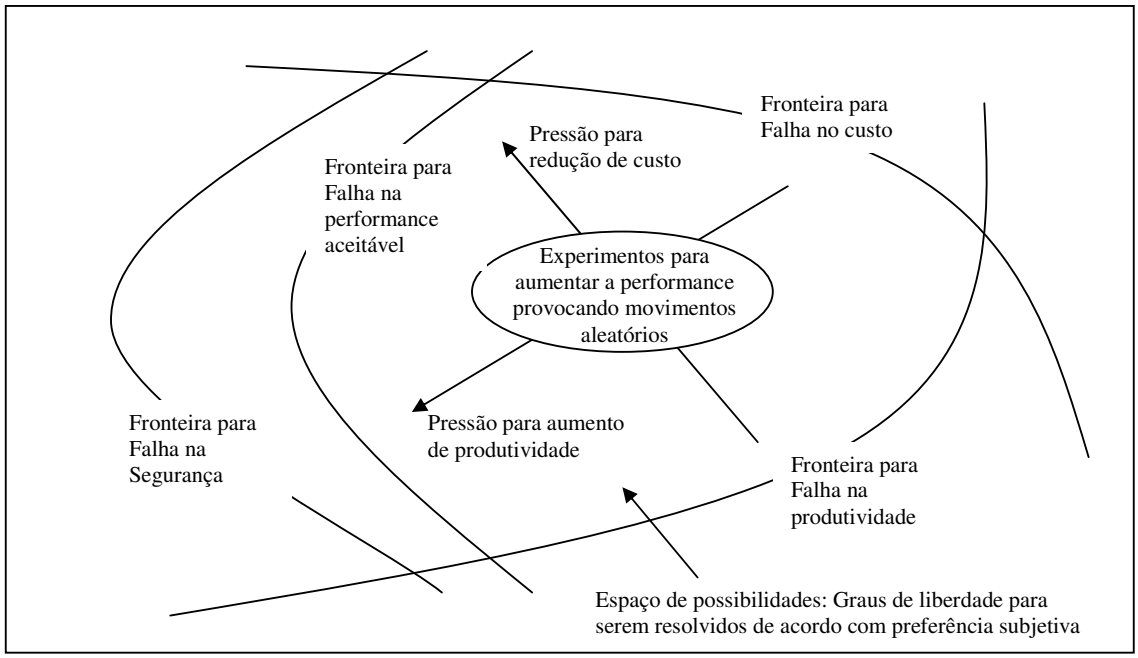



Figura 3.4 - Modelo de gerenciamento de risco
(RASMUSSEN, 1997)

b) Abordagem seqüencial para segurança no processo de projeto

Os modelos e ferramentas de projeto estão em constante evolução, porém permanecem limitados pela capacidade de integrar a prevenção no processo normal de projeto. Didelot (2001) ressalta que a incorporação da segurança nos projetos segue uma abordagem seqüencial e não integrada, devido principalmente à aderência a normas e regulamentações, as quais normalmente são consideradas tardiamente no processo normal de projeto. O crescente número de normas e a dificuldade que os usuários encontram em traduzir as especificações em requisitos de projeto tornam o esforço para integrar esses requisitos pouco produtivos. Nesse cenário, a segurança passa a ser considerada seqüencialmente nos diferentes estágios do processo de projeto. Isso significa que primeiramente o projeto proposto é feito utilizando outros critérios e então checado quanto às considerações e critérios de segurança.

Uma análise das atividades de projeto (DE LA GARZA, 2004) confirma que os requisitos de segurança de forma geral são anexados ao longo do projeto. Segurança não é um requisito inicial específico ou evidente para o projeto. Conforme o autor, existem apenas duas

situações em que a segurança está integrada ao processo de projeto. A primeira é baseada no conhecimento explícito compartilhado pelo coletivo (normas, regras internas de projeto). O segundo é baseado no conhecimento tácito individual que um projetista pode ter oriundo de experimentações ou experiências pessoais. O estudo também mostra as limitações dessas duas situações por causa da falta de sistematização dos objetivos e requisitos iniciais de projeto e da dificuldade de gerar e disseminar o conhecimento necessário para integrar a segurança ao processo de projeto.

c) Experiências passadas são muito pouco exploradas pelos projetistas

Um exame nas práticas industriais mostra que existem muito poucos projetos totalmente novos. Normalmente os novos projetos são processos de reutilização de velhas soluções. Assim sendo, é de vital importância a coleta de informações para identificar as conseqüências de qualquer solução de projeto que venha a ser reutilizada. De forma geral, as empresas não estão estruturadas para coletar as informações sobre o comportamento das diversas soluções de projeto já implementadas. Isso significa que os projetistas terão dificuldades em avaliar e antecipar o comportamento das soluções adotadas no contexto dos novos projetos.

Com base nos três fenômenos descritos, De La Garza e Fadier (2006) propõem uma nova filosofia em projetos para segurança baseada no usuário final levando em consideração as características do usuário e interações com meio ambiente e com o equipamento. Conforme o autor um dos pontos-chave para implementação da filosofia proposta é o uso do conhecimento e experiência passada, porém estruturado e devidamente analisado para gerar conhecimento efetivo aos projetistas. A literatura em geral enfatiza que o conhecimento de experiências passadas não é um processo usado sistematicamente. Existem poucos dados disponíveis principalmente relacionados a relatórios de acidentes os quais, apesar de significativos, não são suficientes para suportar processo de projeto com informações relevantes.

Como forma de estruturar estas informações propõe-se o uso da ferramenta desenvolvida por Didelot e Fadier (2002) como forma de estruturar dados de experiências passadas para finalidades de projeto. A ferramenta é denominada árvore lógica. A forma de representação da árvore lógica contém elementos nos quais o projetista pode atuar para incrementar a segurança do projeto. A Figura 3.5 apresenta um exemplo da ferramenta proposta por Didelot e Fadier (2002) adaptada a uma ocorrência evidenciada em um condicionador de ar. O modo de representação é centrado no evento principal que define a necessidade de construção da árvore lógica. O evento principal é posicionado no centro da

figura, mas não como um evento de topo como seria na construção de uma árvore de falha tradicional. A partir desse ponto tenta-se determinar os eventos anteriores e posteriores, como sendo:

- Eventos anteriores - causas que propiciaram o evento principal: circunstâncias especiais, elementos introduzidos pelo projeto, elementos introduzidos pelo processo de manufatura, interação equipamento usuário etc.
- Eventos posteriores - eventos que originaram a falha e suas respectivas conseqüências na forma de acidentes ou incidentes, como por exemplo, deficiência de procedimentos e suas conseqüências etc.

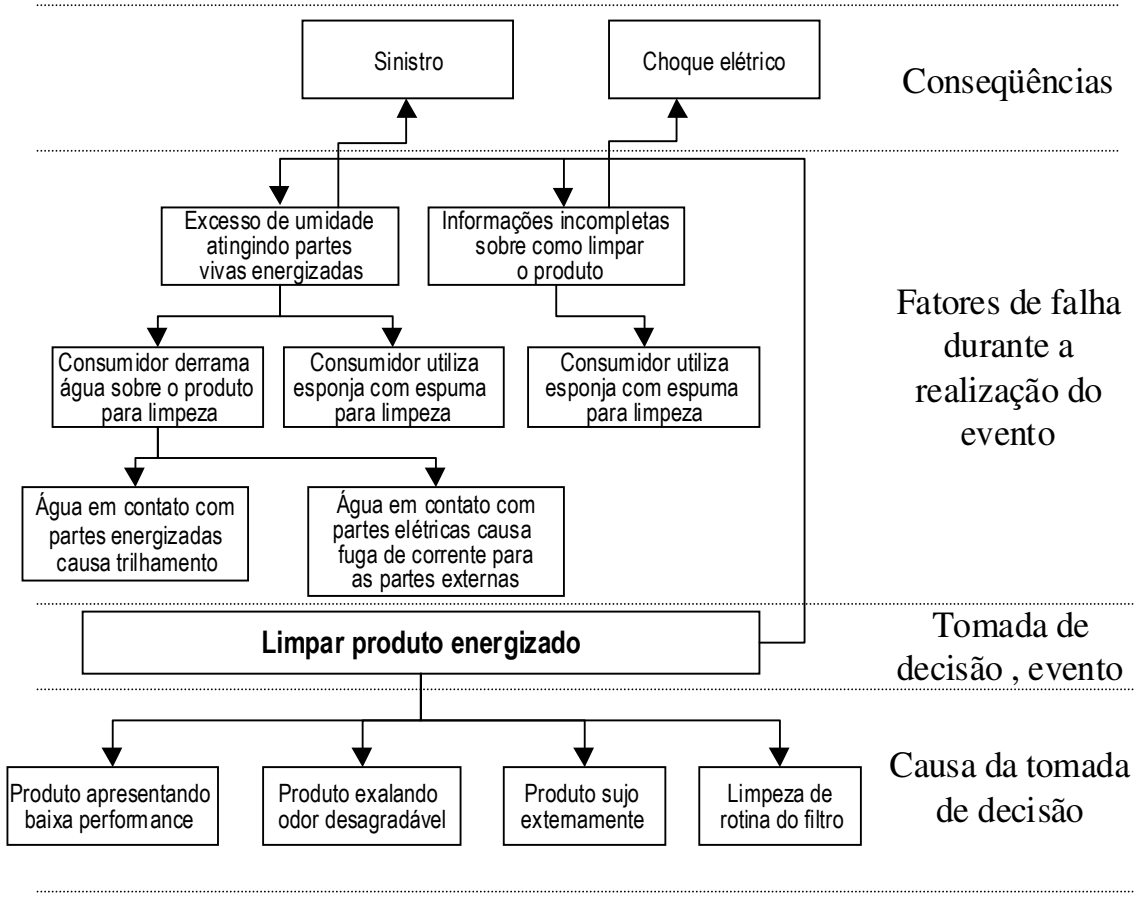



Figura 3.5 - Árvore lógica (Adaptado de DIDELOT e FADIER (2002)

Hammer (1993), ao discutir os programas de segurança, sugere que nenhum programa é suficientemente robusto se não considerar todas as fases de desenvolvimento do projeto. Para tal sugere uma lista de tarefa que se estende ao longo de todas as etapas do ciclo de vida do produto. O Quadro 3.3 apresenta as tarefas definidas por Hammer (1993) durante o ciclo de vida do produto.

Hammer (1993) sugere também que essa lista de tarefa deva ser parte integrante dos itens a serem discutidos ao longo das revisões de projeto, que devem ser conduzidas por times multidisciplinares ao término de cada etapa do projeto. Cabe salientar que a lista de tarefas proposta pelo autor é genérica e que deve ser adaptada em função do tipo de produto e em função do modelo de processo de projeto utilizado.

Quadro 3.3 – Programa de tarefas para Segurança de Produtos (HAMMER, 1993)

| **Fase de conceito** | |
|---|---|
| 1. Revisar produtos similares sobre aspectos de segurança.<br>2. Determinar problemas anteriores com produtos similares.<br>3. Determinais perigos potenciais existentes no produto proposto:<br>• Para usuários<br>• Para técnicos<br>• Para outros equipamentos e instalações<br>• Para o meio ambiente<br>4. Ajudar os projetistas no planejamento preliminar.<br>5. Ajudar e participar de estudos de comércio.<br>6. Preparar uma análise de perigo preliminar para o conceito aceito. | 7. Preparar critério para a segurança do projeto.<br>• Revisar e incorporar as normas existentes e exigências de certificação.<br>• Determinar requisitos adicionais onde os requisitos existentes são inadequados.<br>8. Determinar testes de segurança que podem ser necessários para materiais, componentes, dispositivos de segurança e operação.<br>9. Fazer a determinação preliminar de dispositivos de segurança que podem ser necessários.<br>10. Estabelecer exigências de confiabilidade a serem impostas aos fornecedores.<br>11. Estimar o impacto do programa de segurança<br>12. Fazer uma avaliação do risco. |
| **Desenvolvimento do processo de avaliação** | |
| 1. Coletar informações sobre perigos e proteções.<br>2. Avaliar os aspectos de segurança das alterações propostas.<br>3. Conduzir testes de segurança em materiais, componentes e dispositivos.<br>4. Avaliar os testes para determinar a viabilidade do projeto.<br>5. Preparar plano de aquisição para a fase de desenvolvimento do Produto.<br>6. Preparar orçamento para os custos do programa de segurança e equipamentos.<br>7. Determinar interface e informações exigidas para as atividades entre os projetistas da equipe e os fabricantes/fornecedores. | 8. Preparar as regras iniciais do programa de segurança do produto.<br>9. Instruir a equipe da companhia sobre os objetivos e metodologia de segurança do produto.<br>10. Monitorar o programa de segurança durante as fases seguintes.<br>11. Atualizar os critérios de projeto seguro através da incorporação de chances e achados adicionais.<br>12. Estabelecer conexões intra-companhia, com fornecedores e outras partes interessadas. |
| **Desenvolvimento do produto** | |
| 1. Administra reuniões do Comitê Segurança de Produto.<br>2. Assegurar que todas as equipes estejam familiarizadas com a segurança do produto, com as regra do programa e as responsabilidades de todas as equipes.<br>3. Continuar ajudando os projetistas nos assuntos de segurança.<br>4. Participar dos estudos sobre comercialização, proposta para o projeto detalhado e mudanças de segurança.<br>5. Preparar análises de segurança. | 9. Administrar as revisões formais de segurança do projeto.<br>10. Revisar o protótipo e o plano de teste.<br>11. Estabelecer procedimento de revisão para assegurar que as relações homem-máquina são ideais.<br>12. Revisar as operações e procedimentos de manutenção antes da publicação para assegurar que eles são necessários, não envolvam nenhuma tarefa de risco, e contenham as advertências necessárias.<br>13. Estabelecer meios pelos quais possam ser |

| | |
|---|---|
| 6. Manter os gerentes informados para qualquer problema de segurança em potencial ou existente.<br>7. Determinar se os projetistas estão observando os critérios de projeto seguro. Notificar sobre qualquer deficiência para que a ação corretiva seja tomada.<br>8. Determinar quais montagens, componentes, materiais ou procedimentos são críticos em segurança para que procedimentos especiais possam ser definidos durante montagem, manipulação e operação. | informados os problemas de projeto.<br>14. Analisar documentos, estudos, resultados de testes e outras informações relacionadas à segurança.<br>15. Assegurar que todas as tarefas e testes requeridos por agências do governo são respeitados e observados.<br>16. Identificar que tipos de dispositivos protetores e advertências devem ser providenciados.<br>17. Assegurar, com a equipe jurídica, que as advertências estejam adequadas. |
| **Avaliação da produção** | |
| 1. Atualizar análises do protótipo como projetado e construído.<br>2. Avaliar desempenho do protótipo para conotações de segurança.<br>3. Avaliar as mudanças recomendadas.<br>4. Preparar plano de aquisição para atender a produção e fases de operação.<br>5. Meios institucionais para:<br>• Informar produção e gerentes de controle de qualidade sobre quais itens são considerados de segurança críticos.<br>• Assegurar que o pessoal da produção esteja instruído para não realizar modificações no projeto, de materiais ou de itens críticos de segurança.<br>• Assegurar que as inspeções, testes de segurança ou itens críticos sejam informados.<br>6. Continuar o trabalho de campo sobre a segurança do equipamento. | 7. Completar a análise de segurança do projeto.<br>8. Procedimentos institucionais para revisões de segurança e para criar pedidos de mudança.<br>9. Revisar advertências para o produto novo<br>10. Prever treinamento para vendedores, distribuidores e técnicos de serviço.<br>11. Instituir procedimento para receber e processar reclamações, problemas e reivindicações.<br>12. Instituir procedimentos para registro de garantia.<br>13. Instituir procedimentos para garantir que o trabalho em partes de segurança crítica é inspecionado e que eles incluem advertências que também devem estar presentes nas partes originais.<br>14. Assegurar que as informações sobre os itens que são de segurança crítica são conhecidos pela produção e departamentos de controle da qualidade. |
| **Produção** | |
| 1. Assegurar que os gerentes produção e qualidade e as respectivas equipes estão dando a atenção necessária aos itens críticos de segurança.<br>2. Assegurar que a produção não esteja efetuando alterações de projeto de itens críticos sem a prévia avaliação da equipe de segurança.<br>3. Assegurar que a inspeção e testes de falha sobre itens críticos está informando a equipe de segurança.<br>4. Assegurar que as advertências de segurança estão adequadamente posicionadas no equipamento.<br>5. Analisar reclamações dos clientes e informações sobre problemas de campo. Recomendar ações onde a segurança possa ser melhorada. Assegurar que ações corretivas são implementadas onde existir deficiências. Assegurar que são efetuados os registros das ações implementadas. | 6. Assegurar a inspeção de cada lote e que sejam efetuados os registros da qualidade.<br>7. Assegurar que os revendedores e fornecedores conheçam os aspectos de segurança para partes e montagens.<br>8. Manter o pessoal de serviço (e consumidores quando for o caso) informado com boletins que:<br>• Faça-os lembrar de perigos potenciais e precauções a serem observadas.<br>• Alerte-os sobre problemas potenciais recentemente determinados e medidas corretivas.<br>• Oriente-os sobre a disponibilidade de novos e melhores dispositivos de segurança. |
| **Operação e suporte** | |
| 1. Assegurar que cópias dos relatórios de | 3. Realizar visitas de campo a consumidores e |

| | |
|---|---|
| problemas de campo e de reclamações dos clientes estejam disponíveis para avaliação da equipe de segurança.<br>2. Providenciar assistência para o pessoal de serviço da companhia em problemas potenciais de segurança, falha de itens críticos ou investigação de acidentes. | representantes para assegurar que as operações estejam sendo executadas conforme estipulado em manuais e procedimentos.<br>4. Visitar o cliente para verificar se ele alterou o produto ou se tem utilizado o mesmo de forma incorreta. |

## 3.4 Fatores de influência na segurança de produtos

Inicialmente as teorias monocausais procuraram identificar uma causa única e fundamental para ocorrência do evento, no caso do incidente, o qual poderia ter origem no meio no indivíduo ou no equipamento.

A fragilidade e inconsistência na explicação dos acidentes pela teoria mono causal conforme Carpes Júnior (2001) levou, na década de 60, à consolidação das teorias multicausais. As teorias multicausais, de forma geral, apresentam a coexistência de várias causas na ocorrência de acidentes que podem ter origem em três fontes principais, (ambiente, máquina e homem) ou ainda da interação entre elas. As causas, por sua vez, formam uma cadeia de eventos que pode culminar na ocorrência de um acidente.

Condicionadores de ar de uso domésticos são classificados pela IEC 60335-1 como equipamentos “não atendidos”, ou seja, equipamentos que operam em grande parte do tempo sem a presença de um operador, no caso o usuário do produto. Essa característica induz a uma condição de uso onde a interação do usuário com o produto aconteça de forma pontual.

Nesse contexto, ambiente e homem são fontes que podem apenas ser estimadas, porém nunca efetivamente controladas, conseqüentemente a máquina como fonte de perigo potencial e a interação dela com as demais fontes assume grande relevância.

Característica insegura das máquinas e sua interação com o homem e o ambiente são informações que devem ser determinadas, analisadas, tratadas e convertidas em soluções durante as diversas etapas do processo de projeto. Erros na condução dessa análise durante as diversas etapas do processo de projeto constituem um dos principais fatores de influência na segurança dos produtos.

### 3.4.1 Erros de projeto

Conforme Alonço (2004), as atividades de projeto podem estar sujeitas a equívocos, serem incorretas ou ainda impróprias aos fins a que se destinam. Esses erros durante a

condução do processo de projeto podem ter como conseqüência atrasos, custo adicional, qualidade ou ainda segurança.

Alonço (2004) classifica em três grupos as fontes de erros em projetos a citar:

- Erro de informação;
- Erro em atividades de projeto;
- Erro de comunicação;

Erros de informação são potencializados nas fases iniciais do projeto, em especial durante o projeto informacional onde serão levantadas as informações de mercado, incluindo-se os interesses ou as manifestações dos clientes do projeto os quais abrangem toda cadeia do ciclo de vida tais como: manufatura, logística, revenda, assistência técnica, utilização pelo consumidor final e outros. Erros nessa etapa do projeto podem resultar em produtos inadequados para o fim a que se destinam. O Quadro 3.4 apresenta uma relação de erros de informação que podem acontecer durante a execução de projetos.

Quadro 3.4 – Erros de informação em projetos (MCMAHON *et al*., 1997)

| **ERROS DE INFORMAÇÃO** | **EXEMPLOS DE ERROS** |
|---|---|
| Exigência funcional. | Exigências de clientes incorretamente interpretadas/modificadas; Referências incorretas em normas técnicas ou códigos. |
| Influências externas no produto. | Entendimento incorreto sobre a aplicação do cliente. |
| Atributos explícitos, como, parâmetros dimensionais, propriedades dos materiais etc. | Erro dimensional, material não adequado ou impropriamente especificado. |
| Atributos implícitos, como características e comportamentos do produto sujeitos às influências externas. | Estimativas de desempenho incorretas.<br>Transcrição incorreta de valores de normas técnicas.<br>Requisitos dos clientes incorretamente traduzidos ou interpretados. |
| Restrições nos valores de parâmetros explícitos. | Parâmetros especificados não possíveis de reproduzir na manufatura. |

Pela característica de estarem desenvolvendo algo novo, os projetos são sempre executados sob certo grau de incerteza. Pode, porém, ocorrer incerteza na interpretação dos requisitos dos clientes, na interpretação de requisitos de normas e interpretação de resultados de testes, ou ainda imprecisão nos métodos de avaliação utilizados.

Incerteza e imprecisão também podem ser observadas nos métodos e ferramentas utilizados para a execução do projeto. Pode ocorrer devido à definição de métodos e ferramentas inadequados, pela aplicação incorreta de ferramentas, execução incompleta de

alguma atividade e outras falhas na condução do processo de desenvolvimento de produtos. No Quadro 3.5 são apresentadas algumas fontes de erro evidenciadas ao longo das atividades de projeto.

Quadro 3.5 – Fontes de erros em atividades de projeto (Adaptado de GIBBINGS, 1986)

| FONTE DE ERRO | EXEMPLOS DE ERROS |
|---|---|
| Técnica inadequada. | Método não possui precisão adequada;<br>Método não permite obter respostas desejadas. |
| Atividade não concluída. | Análise incompleta. |
| Erro de método. | Erro de limitação na técnica utilizada. |
| Atividade executada incorretamente. | Erro na transcrição de dados. |
| Falha no processo. | Falha na interação de diversas atividades; resultados não disponíveis no tempo requerido. |
| Erro deliberado. | Falsificação de resultados. |
| Perda de tempo. | Análise tão longa que os resultados não estão disponíveis no tempo necessário. |

Não menos importante, a comunicação é uma parte do processo de projeto que pode ser uma das principais fontes de erro. Conforme Gibbings (1986) a comunicação pode ser modelada em três fases: codificação, transmissão e decodificação, nas quais podem ser introduzidos diversos modos de erros, como os relatados no Quadro 3.6.

Quadro 3.6 – Fontes de erros em comunicação (Adaptado de GIBBINGS, 1986)

| FONTE DE ERRO | EXEMPLOS DE ERROS |
|---|---|
| Codificação do erro. | Comunicação incorreta no uso de normas técnicas ou erro no uso de normas técnicas. |
| Perda de sinal. | Projeto reproduzido pobremente; arquivo apagado inadvertidamente. |
| Ruído de sinal. | Perda de informações devido à deficiência no domínio do idioma utilizado; times com membros de diversos países. |
| Erro na decodificação. | Uso incorreto ou comunicação incorreta sobre o teor de normas técnicas. Unidades em diferente base ou convertidas incorretamente. |
| Comunicação incompleta. | Sistemas incompatíveis, por exemplo, comunicação entre sistemas de CAD. |

### 3.4.2 Erro humano

No que tange ao uso, instalação ou ainda operação de um determinado equipamento a NBR5462, Confiabilidade e Mantenabilidade enquadra erro humano como falha por uso incorreto.

Conforme Carpes Júnior (2001), a política de "zero incidente" com base na supressão do erro foi buscada exaustivamente ao mesmo tempo em que tem sido questionada por diversos pesquisadores. Mesmo em sistemas tecnologicamente avançados o funcionamento inadequado de sistemas de segurança tem provocado sérios incidentes. Além disso, é sempre previsto que os operadores atuem com eficiência em situações inesperadas revertendo situações potencialmente perigosas, o que nem sempre é uma certeza.

Kumamoto (1996) classifica os erros humanos como falha ativa ou latente. A probabilidade de ocorrência dessas falhas é determinada por fatores relacionados com treinamento, capacitação, procedimentos, definição de responsabilidades, demanda, produção etc. Esses fatores, por sua vez, são influenciados por outros fatores tais como gerenciamento de risco, projeto, sistema de comunicação etc.

Há de se considerar que sistemas do tipo dos condicionadores de ar são passíveis de ser manuseados, instalados e operados por indivíduos sem qualquer conhecimento ou informação sobre o produto.

Nesse contexto, a possibilidade de uma falha por uso incorreto ser o fator deflagrador de um evento que cause um incidente deve ser investigado pelos projetistas e minimizado ao máximo quando da elaboração do projeto. O uso indevido, instalação inadequada ou ainda o não seguimento de rotinas de manutenção são exemplos de falhas por uso incorreto que, mesmo quando combinadas, não devem ser a causa de incidentes com o produto. Portanto, o impacto sobre a segurança devido à falta de conhecimento do usuário deve ser previsto e as devidas ações para minimizar qualquer incidente devem ser adotadas.

## 3.5 Comentários finais

A aplicação de metodologias de projeto, de forma geral, garante a funcionalidade do produto pelo atendimento da função principal. Sobre a função principal são elaboradas as soluções do projeto e, nesse contexto, os requisitos de segurança ficam em um plano secundário.

As metodologias atuais, mesmo as que se dedicam à segurança, não abordam como integrar de forma efetiva as ações e ferramentas aplicadas nas diversas etapas do processo de

projeto para tratamento do atributo segurança. Sob esse aspecto, segundo Carpes Júnior (2001, p. 72), “existe uma contradição nas metodologias de projeto: dizem que é importante a segurança, durante determinada fase ou durante todo o projeto, mas não dizem como inseri-la de fato”.

Listas de verificação, como a elaborada por Hammer (1993), são de grande utilidade para estabelecimento de um processo de projeto, tais questionamentos ajudam o time de projeto na verificação se todas as etapas foram cumpridas, sem, no entanto, garantir que os aspectos de segurança tenham sido eficazmente inseridos no projeto.

Dados de experiências passadas, conforme Didelot e Fadier (2002), podem ser estruturados de forma efetiva por meio da aplicação da árvore lógica proposta pelos autores, porém esses dados em nada contribuirão para a segurança de um novo produto se eles não forem inseridos de forma eficaz nos novos projetos.

Dias *et al*. (2007) colocam a segurança como um atributo básico de produtos industriais. Nos projetos para a segurança os autores descrevem a postura a ser assumida pelos projetistas e os princípios de projetos a serem adotados sem, no entanto, detalhar como o atributo segurança será efetivamente introduzido no processo de projeto.

A metodologia proposta neste trabalho visa suprir essa deficiência, gerando condições para que todas as informações relacionadas à segurança sejam inseridas no projeto do produto de forma efetiva nas diversas etapas do processo de projeto.