ANÁLISE DE CAMADAS DE PROTEÇÃO: UM MEIO EFICAZ NA REDUÇÃO DE ACIDENTES

**Autor: Elisio Carvalho Silva**

Data: 30/03/2012

## INTRODUÇÃO

O perigo está relacionado a qualquer atividade que fazemos. Enquanto ele estiver contido por camadas de proteção, não há o risco de se transformar num acidente. O risco pode variar de intensidade, depende da frequência de ocorrência e a severidade da consequência do evento. Por exemplo, um produto inflamável armazenado em grande quantidade num tanque, possui perigo inerente devido ao valor expressivo de energia intrínseca ao produto. O risco é a perda de contenção desse produto e liberação de sua energia provocada por uma fonte de ignição. Para evitar um acidente, é preciso identificar as formas de liberação de energia, determinar o evento iniciador e empreender esforços na redução da frequência de ocorrência do acidente ao adicionar camadas de proteção para que o evento iniciador não se propague e cause consequências indesejadas. Outro modo para mitigar a liberação dessa energia é minimizar a severidade da consequência resultante. Portanto, é possível determinar ações tanto para reduzir a freqüência como também a conseqüência de um evento acidental e, por conseguinte, minimizar o risco.

Acidentes custam caro às empresas. Por isso, é fundamental que elas definam meios para evitar situações que concorram negativamente com a sua imagem, o bem-estar dos seus funcionários, o meio ambiente e os seus ativos.

Este artigo tem como objetivo mostrar como elaborar uma análise de camadas independentes de proteção e definir se o processo operacional está num nível adequado de risco. Caso não esteja, definir quais ações serão implementadas para manter o processo seguro.

## TOLERABILIDADE DO RISCO

Dependendo de alguns fatores, toleramos ou não um determinado risco. Embora a severidade de um acidente aéreo seja muito alta, a sociedade aceita o avião como meio de locomoção porque a viagem é rápida, portanto facilita a nossa vida, e é um meio seguro de transporte já que a freqüência de fatalidade devido a queda de um avião é muito baixa, conforme cita David J. Smith, é de 2 fatalidades em cem milhões de ano.

Cada empresa deve definir a sua tolerabilidade de risco baseada em boas práticas ou conforme a legislação do país ou estado. No Brasil, alguns estados já definiram uma matriz de tolerabilidade de risco no seu programa de gerenciamento de risco aplicada às empresas que

manuseiam produtos perigosos. A Tabela 1 apresenta um exemplo de matriz de tolerabilidade de risco.

| Matriz de Tolerabilidade do Risco | | FREQUÊNCIA | | | | |
|---|---|---|---|---|---|---|
| | | IMPROVÁVEL | REMOTO | OCASIONAL | PROVÁVEL | FREQUENTE |
| Tempo médio entre falhas (MTTF)<br>Falhas por ano=1/MTTF | | $f>10^6$ anos | $10^4<f\leq10^6$ | $10^2< f \leq10^4$ | $1<f\leq10^2$ | $f\leq1$ano |
| SEVERIDADE | CATASTRÓFICA (múltiplas fatalidades) | MODERADO | NÃO ACEITO | NÃO ACEITO | NÃO ACEITO | NÃO ACEITO |
| | EXTREMAMENTE CRÍTICA (uma fatalidade) | ACEITO | MODERADO | NÃO ACEITO | NÃO ACEITO | NÃO ACEITO |
| | CRÍTICA (danos permanentes) | ACEITO | ACEITO | MODERADO | NÃO ACEITO | NÃO ACEITO |
| | MODERADA (danos temporários) | ACEITO | ACEITO | ACEITO | MODERADO | NÃO ACEITO |
| | BAIXA (pequenos danos) | ACEITO | ACEITO | ACEITO | ACEITO | MODERADO |

Tabela 1 – Matriz de Tolerabilidade de Risco
Adaptada de Dennis Nolan

Na Tabela 1, no eixo horizontal está a frequência do evento, ou seja, qual a expectativa que o evento ocorra. Para melhor entendimento da frequência veja a Tabela 2.

| Categoria | Faixa de Frequência Associada | Exemplos |
|---|---|---|
| Frequente | Mais que uma vez por ano. ($f \leq 1$ano) | **Em plantas existentes:**<br>- Histórico de uma ou mais ocorrência por ano e nenhuma alteração feita no sistema.<br>**Em projetos:**<br>- Histórico de uma ou mais ocorrências por ano em empreendimentos similares.<br>**Erro humano:**<br>- Atividade frequente com inexistência de treinamento e procedimento, em presença de condições de trabalho adversas. |
| Provável | Esperado na vida útil do empreendimento. ($1<f\leq100$ anos) | **Em plantas existentes:**<br>- Histórico de ocorrência menor que 1 por ano ou situação que já esteve próxima de ocorrer e nenhuma alteração feita no sistema.<br>- Ruptura ou quebra de equipamentos reconhecidamente degradados ou com inspeção deficiente. |

| | | |
|---|---|---|
| | | **Em projetos:**<br>- Histórico de ocorrência menor que 1 por ano ou situação que já esteve próxima de ocorrer em empreendimentos similares.<br>**Erro humano:**<br>Erro humano por inexistência de treinamento e procedimento, em presença de condições de trabalho adequadas. |
| Ocasional | (100<f≤10.000 anos) | **Em plantas existentes ou projetos:**<br>- Falha única de equipamento em bom estado de operação e manutenção.<br>**Erro Humano:**<br>- Cenários que dependem de falha única, humana em condições adequadas de ergonomia, com treinamento e procedimento. |
| Remoto | (10.000<f≤1.000.000 anos) | **Em plantas existentes ou projetos:**<br>- Falha dupla de equipamentos.<br>- Ruptura de equipamentos estáticos, linhas e acessórios sujeitos a inspeção.<br>- Falha de componente eletrônico.<br>**Erro Humano:**<br>- Dupla falha humana em condições adequadas de ergonomia com treinamento e procedimento. |
| Improvável | (f>1.000.000 anos) | **Em plantas existentes ou projetos:**<br>- Ruptura por falha mecânica de vasos de pressão com inspeção e testes periódicos nos sistemas de proteção. Sem histórico de sobrecarga de pressão, temperatura ou vibração, sem histórico de comprometimento por trincas ou perda de espessura.<br>- Falha de vários sistemas de proteção.<br>**Erro Humano:**<br>- Múltiplas falhas humanas em condições adequadas, com treinamento e procedimento. |

Tabela 2 – Definição das diversas faixas de frequência
Adaptada da Resolução CEPRAM nº 3.965 de 30 de junho de 2009.

No eixo vertical está definida a severidade do evento que é a consequência resultante caso ocorra o acidente. Se houver uma fatalidade, é extremamente crítica e mais de uma morte é considerada catastrófica.

Ao classificar o cenário, serão determinados três tipos de categorização do risco: não aceito, moderado e aceito. O risco "não aceito" obrigará a adoção de ações para reduzir a frequência ou a severidade do evento.

O "moderado" recomenda-se fazer uma avaliação das camadas de proteção existentes a fim de definir ações para reduzir a um risco aceito, porém deve-se avaliar custos e benefícios obtidos com as novas recomendações. Se os custos forem altos e não traduzirem em benefícios evidentes para a redução de acidente, o cenário poderá ser mantido como risco médio. Contudo, deverão ser instituídas ações para assegurar que o risco nunca ultrapassará a classificação "moderada".

No risco "aceito" nada precisará ser feito, apenas serão mantidos os programas de gestão para garantir a integridade do sistema.

## EVENTO INICIADOR E CAMADAS INDEPENDENTES DE PROTEÇÃO

As camadas de proteção são controles efetuados para prevenir ou mitigar um acidente. Quando esses controles falham, os acidentes ocorrem (Figura 1). Daí a necessidade de uma avaliação detalhada para definir a adoção das camadas adequadas para cada cenário de acidente, assim como garantir que elas funcionarão íntegras por toda a vida do processo.

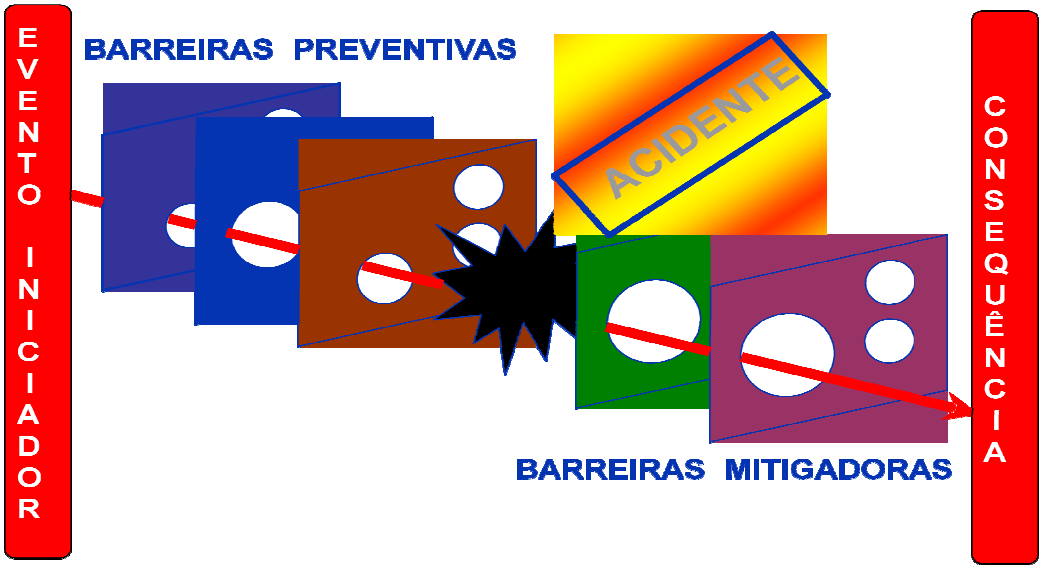


Figura 1- Representação das falhas das camadas de proteção

Um evento iniciador é aquele que dá início às causas de um acidente e que se não for bloqueado levará a consequências indesejadas. As camadas independentes de proteção (CIP) são os mecanismos mais eficazes para interromper uma cadeia de eventos acidental. Estando elas íntegras, reduzirão a frequência da ocorrência do evento (camadas preventivas) para valores tão baixos que possivelmente nunca ocorrerá durante a vida útil do sistema operacional, ou reduzirão a consequência do evento (camadas mitigadoras). Graficamente as camadas de proteção agirão conforme mostra a Figura 2.

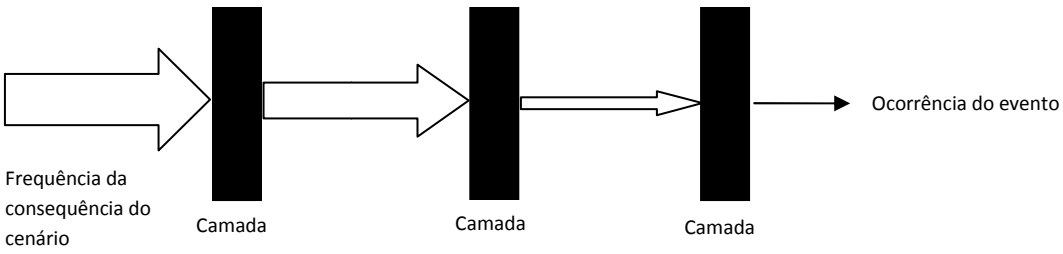


Figura 2 - Camada de Proteção (a largura das setas representa a frequência do evento)
Adaptado do livro Layer of Protection Analysis (CCPs, 2001)

São vários os tipos de camadas de proteção que podem ser aplicadas para evitar um cenário de acidente. Dependendo da severidade do evento e da complexidade do processo, podem ser necessárias mais de uma camada de proteção para atingir a tolerabilidade do risco. Alguns exemplos de camadas de proteção:

- Preventivas – projeto inerentemente seguro, sistema instrumentado de segurança, alarme e ação humana, válvula de alívio, sistema básico de controle de processo;
- Mitigadoras – diques de contenção, parede contra explosão, porta corta fogo, plano e resposta a emergência, sistema de detecção e combate a incêndio, isolamento de área.

As camadas de proteção preventivas são as mais importantes porque agirão para evitar o acidente, enquanto que as camadas mitigadoras não evitarão o acidente, no entanto reduzirão as suas consequências.

Camadas independentes de proteção e salvaguardas possuem funções parecidas, porém é preciso obter o entendimento entre suas diferenças. Uma salvaguarda protege o sistema de um acidente, mas não terá a mesma eficácia de uma camada independente de proteção por não possuir as seguintes características, conforme menciona a IEC 61511-3:

a) Especificidade – uma camada independente de proteção deve ser especificamente projetada para ser capaz de prevenir as consequências consideradas no projeto;
b) Independência – deve operar completamente independente de todas as outras camadas e do evento iniciador;
c) Confiabilidade – as camadas de proteção devem ser capazes de prevenir as consequências de um evento. Por isso, todas as possíveis falhas devem ser consideradas quando projetar uma camada de proteção;
d) Auditabilidade - as camadas de proteção devem ser testadas e mantidas adequadamente. As auditorias são necessárias para assegurar que o nível de redução de risco especificado foi atingido e está sendo mantido.

## ANÁLISE DE RISCO

A análise de risco será o ponto de partida para avaliar as camadas de proteção para um determinado cenário. Ela definirá o grau de risco de cada cenário e identificará as suas salvaguardas que poderão ser ou não camadas independentes de proteção. O cenário para análise da camada de proteção será representado pelo par causa-consequência e a causa será o evento iniciador. A categorização do risco definirá se o cenário será “não aceito”, “moderado” ou “aceito”. Sendo “não aceito” ou “moderado”, será aplicada a análise de camadas de proteção. A Tabela 3 mostra um modelo de análise de risco.

| DESVIO | CAUSA | CONSEQUÊNCIA | SALVAGUARDA | CAT. FREQ | CAT. SEVER | CAT. RISCO | RECOMENDAÇÕES |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

Tabela 3 – Modelo de análise de risco

## ANÁLISE DAS CAMADAS DE PROTEÇÃO

A análise de camadas de proteção é uma abordagem sistemática e semiquantitativa que permitirá avaliar as camadas existentes e propor novas, caso o evento resultante esteja numa frequência que leve o cenário a uma categorização de risco diferente da tolerável conforme a Tabela 1 ou outra matriz subscrita pela empresa. Deve ser realizada por um grupo multidisciplinar com participação indispensável de uma pessoa que conheça a metodologia de análise e outra que domine o conhecimento sobre o processo analisado. Essa análise poderá ser feita na mesma reunião em que estiver sendo realizada a análise de risco e no mesmo formulário. Dessa maneira poupará tempo, porém existe a desvantagem de prolongar a reunião e torná-la cansativa. Por isso, muitas empresas decidem fazer a análise de camadas de proteção em outro momento.

O primeiro passo é identificar a freqüência do evento iniciador, que é a causa conforme identificada na análise de risco. Essa frequência pode ser obtida por histórico da empresa (mais adequado) ou bancos de dados genéricos tais como, SINTEF - *Reliability Data for Control and Safety Systems*, OREDA - *Offshore Reliability Data*, CCPS - *Guidelines for Process Equipment Reliability Data*, CCPS - *Layer of Protection Analysis*, quando aplicável. Sempre terá como unidade de medição falhas/unidade de tempo, usualmente para cálculo utiliza-se falhas/ano.

Em continuação à análise, o grupo identificará quais as camadas de proteção existentes que previnem ou mitiguem o evento iniciador a se transformar num acidente. A partir desse momento deverá ser associada uma probabilidade de falha em demanda (PFD), que é adimensional e varia de 0 a 1, para cada camada existente. A PFD para uma camada de proteção é a probabilidade dela não agir de forma segura quando demandada. Por exemplo, se houver um cenário de alta pressão devido a falhas de uma válvula de controle de pressão, o dispositivo de alívio de pressão instalado no sistema será uma camada de proteção e terá uma PFD de $1x10^{-2}$.

Serão identificadas todas as camadas existentes e o cálculo adequado para encontrar a freqüência dos cenários com as camadas preventivas e as mitigadoras existentes. O cálculo da frequência resultante deverá ser feito da seguinte forma:

$$f_i^C = f_i^I \cdot \prod_{j=1}^{J} PFD_{ij}$$

Onde:

$f_i^C$ = Frequência da consequência associada ao cenário

$f_i^I$ = Frequência do evento iniciador i que dá origem a consequência C

$PFD_{ij}$ = Probabilidade da falha em demanda para a jenésima camada de proteção que protege contra a conseqüência C para o evento iniciador i

Uma vez feito o cálculo com todas as camadas existentes, a frequência resultante será comparada com a matriz de tolerabilidade dos riscos no intuito de verificar se o risco do cenário é aceito. Se for "não aceito" ou "moderado", serão sugeridas novas camadas de proteção, repetido o cálculo e comparado mais uma vez, até ter camadas suficientes para que o cenário seja aceito.

## ESTUDO DE CASO

Um produto gasoso altamente inflamável é enviado para um tanque a uma pressão de 150 psig, no entanto o tanque foi projetado para uma pressão máxima permitida de trabalho de 50 psig. Os seguintes dispositivos estão instalados para evitar ruptura do tanque por alta pressão:

1. Válvula de controle de redução de pressão controlada diretamente pelo sistema básico de controle de processo (PIC – *Pressure Indicator Controller*);
2. Alarme de alta pressão do mesmo sinal do sistema de controle de pressão com ação do operador para interromper o fluxo do produto;
3. Uma válvula de alívio com o set de abertura em 50 psig.

Num raio de 100 metros, tendo o vaso como ponto central, existem pessoas trabalhando 24 horas por dia. Um rompimento do vaso com o produto altamente inflamável haverá ignição imediata e consequente bola de fogo com potencial de causar 100% de fatalidade das pessoas presentes num raio de 100 metros.

Verificar se as camadas de proteção existentes mantêm o risco numa região tolerável.

| DESVIO | CAUSA | CONSEQUÊNCIA | SALVAGUARDA | CAT. FREQ | CAT. SEVER | CAT. RISCO | RECOMENDAÇÕES |
|---|---|---|---|---|---|---|---|
| Mais pressão | Falha no sistema de controle de pressão | Rompimento do vaso com posterior geração de uma bola de fogo. | • Válvula de alívio.<br>• Alarme de pressão alta e ação do operador. | Improvável | Catastrófica | Moderada | Confirmar a categoria do risco por meio de LOPA |

Tabela 4 – Análise de risco do estudo de caso

**Cálculo para as camadas independentes de proteção**

A análise das camadas independentes de proteção permitirá avaliar se a categorização de risco identificada na análise de risco, que é uma análise qualitativa, será confirmada ou não como tolerável (Tabela 4).

O primeiro passo é definir qual a frequência tolerável, na matriz de tolerabilidade de risco, para o cenário em discussão. Pela análise de risco o cenário é "moderado", pois tem uma categoria de frequência de "Improvável" e de severidade "Catastrófica". Revisitando a matriz de tolerabilidade de risco, percebe-se que esse cenário será tolerável se a frequência ficar menor que $1x10^{-6}$/ano. Mesmo nessa baixa frequência o cenário se manterá na categoria de moderado, porque para severidade catastrófica essa é a mínima categoria na matriz de tolerabilidade.

**Cálculo da frequência do evento iniciador, considerando as camadas de proteção existentes**

O evento iniciador é a falha no sistema de controle de pressão que pelo valor de literatura é de $1x10^{-1}$ falhas/ano ($F_{Ei}$). Como mencionado anteriormente, a frequência aceita para cenário de acidente com severidade catastrófica é $1x10^{-6}$ falhas/ano ($F_{Ac}$). Ao comparar a frequência do evento iniciador com a frequência aceita, nota-se que ela está bem acima. A PFD total necessária para que o cenário seja aceito deverá ser menor que $F_{Ac}/F_{Ei}$, ou seja, menor que $1x10^{-5}$. Portanto, deve-se buscar camadas de proteção, existentes e recomendadas, para atingir esse valor.

**Cálculo considerando as camadas de proteção existentes:** a análise de risco destaca que existem duas salvaguardas, porém uma delas não será considerada camada independente de proteção (CIP) porque ela não é independente do evento iniciador. Contudo, a válvula de alívio será uma CIP com uma PFD de $1x10^{-2}$ (valor de literatura). A frequência do evento não será mais $1x10^{-1}$ e sim $1x10^{-3}$ falhas/ano.

Como não foi atingido o valor de tolerabilidade do risco, serão necessárias implementar novas camadas independentes de proteção. Como na análise de risco não houve recomendação, o grupo de análise fará a recomendação para que o sistema analisado atinja o nível de tolerabilidade de risco subscrito pela empresa que é $< 1x10^{-6}$ falhas/ano. Uma recomendação plausível seria instalar um sistema de proteção para pressão com alta integridade (HIPPS - *High Integrity Pressure Protection Systems*) que poderá ser um sistema instrumentado de segurança (SIS) com nível de integridade de segurança 3 (SIL 3 – *Safety Integrity Level*) composto de transmissores de pressão, um sistema de lógica de controle de segurança e uma ou mais válvula possivelmente com teste parcial ou total de *stroke* (PST ou FST). A PFD desse sistema pode variar de $<1x10^{-3}$ a $\geq 1x10^{-4}$ (IEC 61511). Portanto, ao escolher o HIPPS deve-se ter em mente que a sua confiabilidade será alta. Nesse momento ainda não precisa fazer o cálculo detalhado da PFD do SIL, referente ao SIS em questão, e nem definir a arquitetura de redundância. Considerando que o sistema a ser instalado tenha uma PFD de $6x10^{-4}$ a frequência do evento passará a $6x10^{-7}$ falhas/ano que comparada com a frequência da tolerabilidade de risco para severidade catastrófica passa a ser um cenário tolerável.

Outra maneira de desenvolver o cálculo é elaborar uma árvore dos eventos com as camadas independentes de proteção existentes e recomendadas. Dessa maneira será possível visualizar as frequências de falhas e de sucesso do sistema (Figura 3).

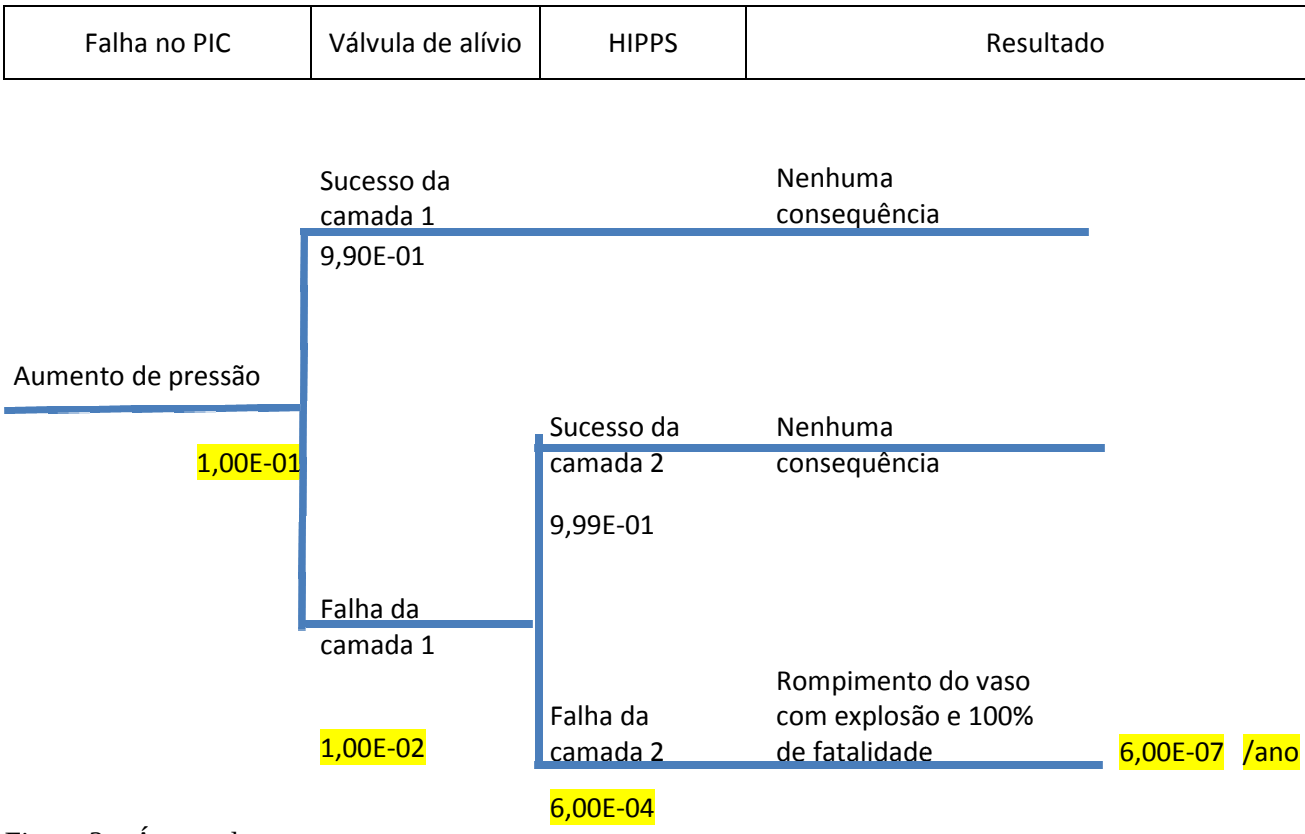


Figura 3 – Árvore dos eventos

## CONCLUSÃO

A análise de camadas independentes de proteção já vem sendo utilizada com sucesso nas indústrias química, petroquímica e de óleo e gás. Como demonstra este artigo, nem sempre a análise de risco qualitativa será suficiente para garantir um bom nível de segurança para empresas que trabalham com produtos perigosos. A análise de risco mostrou que com as duas salvaguardas o sistema era seguro. No entanto, ao fazer a análise de CIP verificou-se que necessitaria de mais camada de proteção para permitir que o sistema atingisse o nível de tolerabilidade de risco exigido. Além da válvula de alívio de pressão existente foi necessário adicionar mais uma camada de proteção. A razão disso é que a análise de camada de proteção permite obter resultados mais acurados, porque é uma análise semiquantitativa o que leva a resultados mais reais.

Concluída a análise, é fundamental promover o acompanhamento da implantação das recomendações para que todo o processo de análise de risco seja eficaz e evite eventos de

acidentes. Uma vez as recomendações sejam implantadas, serão implementadas auditorias para identificar deficiências em relação aos padrões (IEC 61511 ou ISA 84.00.01 para caso específico de SIS), à documentação gerada em relação às especificações de segurança (SRS – *safety requirement specification*), competências, instalação, validação e teste de manutenção. Esse conjunto de ações aumentará o padrão de segurança dos processos ao assegurar que serão implantadas camadas de proteção proporcionais ao risco e irão funcionar adequadamente quando demandadas. Dessa forma, os eventos indesejados serão evitados, vidas serão salvas e outros custos consideráveis serão eliminados.

## Referências


CCPS - **Layer of Protection Analysis.** New York: American Institute Of Chemical Engineers, 2001. 270 p.

CCPS- **Guidelines for Safe and reliable Instrumented Protective Systems.** New Jersey: John Wiley &Sons Inc., 2007.405p

IEC 61511-3. **Functional safety –Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels**. International Electrotechnical Commission, 2004.

IEC 61511-1 **Functional safety –Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements.** International Electrotechnical Commission, 2004.

MANNAN, S. **Lee's Loss Prevention in the Process Industries – Hazard Identification, Assessment and Control**. 3th Elsevier Inc, 2005. 3708 p.

NOLAN, Dennis P.. **Aplication of HAZOP and What-if Safety Reviews to the Petroleum, Petrochemical and Chemical Industries.** 1st New Jersey: Noyes Publications, 1994. 128 p.

**Norma Técnica NT-01/2009. Gerenciamento de Risco no Estado da Bahia, 2009**. Disponível em: http://www.semarh.ba.gov.br/legislacao/resolucao_cepram/resolucao_3965.pdf. Acesso em 2 set. 2009.

SMITH, David J. **Reliability Maintainability and Risk.** 8th Elsevier Ltd, 2011. 436 p.