Utilização de FTA (*Fault Tree Analysis*) em Segurança de Processo em Equipamentos Industriais

Irias, Luiz Gonzaga Caminhas

Magalhães, Thiago Souza

Romanha, Camilo

Silva, Guilherme Tavares de Melo

CREA/MG - Conselho Regional de Engenharia e Agronomia de Minas Gerais

1. INTRODUÇÃO

Com o desafio crescente de garantir a integridade dos ativos industriais e com uma visão voltada para o futuro a fim de comprometer-se com a segurança do processo, há necessidade de criar e implementar metodologias para conhecer e identificar as falhas que levam aos eventos indesejáveis durante o ciclo de vida do ativo.

Devido à complexidade dos equipamentos industriais, sejam eles de mineração, petrolífera ou etc. torna-se indispensável o entendimento do seu funcionamento, sistemas e seus principais componentes como também inferir como esses grupos atribuídos ao equipamento podem vir a falhar, seja por seleção inadequada de componente, instalação crítica sem devidos procedimentos, degradação e avarias durante a operação e manutenção ou seu desativamento ao final de sua vida útil, sem atentar-se de todos os cuidados para proteger a segurança das pessoas em geral, e ao mesmo tempo o meio ambiente.

De uma forma abrangente o risco é considerado como efeito da incerteza nos objetivos. E a sua a avaliação para um equipamento ou processo, como também as falhas associadas à esses equipamentos ou processos possibilita a compreenção da natureza do risco e suas características, que consequentemente proporciona a identificação das medidas para prevenir ou reduzi-los [1].

O principal objetivo desta metodologia aqui apresentada é utilizar a técnica de análise de árvore de falhas, FTA (Fault Tree Analysis), comumente conhecida, que é uma representação lógica de fatores em diagramas de árvore com as interações das causas básicas que podem resultar em um evento indesejável (chamado “evento de topo”) com uma avaliação histórica e técnica de especialista para uma análise qualitativa, e com isso evitar possíveis catástrofes com avaliações nas fases de projeto, construção, instalação, comssionamento, operação, manutenção e descomissionamento do ativo.

2. DESCRIÇÃO

O grau de detalhamento considerado para esta análise de risco é baseado através de duas fases, e que se considera uma combinação técnica qualitativa:

- A **primeira fase** é considerada as probabilidades de falhas através do levantamento prévio de eventos conhecidos e coletados, sejam eles incidentes ou acidentes desses equipamentos ou comum aos principais components na industria;
- Na **segunda fase** as informações coletadas são unidas com a expertise e *benchmarking* de especialistas dos equipamentos, e em workshops com grupos técnico especializado que por sua vez possuem o conhecimento necessário do equipamento e de seus componentes para uma análise e interpretação considerando os possíveis eventos, probabilidade de ocorrência e suas consequências, caracterísitcas temporáis, eficácia dos controles que possam interromper a falha / minimizar suas consequências,

1 Engenheiro Mecânico e Consultor – HATCH
2 Engenheiro Mecânico e Consultor – HATCH
3 Engenheiro de controle e automação e Consultor – HATCH
4 Engenheiro Civil e de Meio Ambiente e Consultor – HATCH

contexto operacional onde o ativo está inserido, limites definidos e características do processo adicionais.

Sabe-se que essa técnica pode ser utilizada quantitativamente para calcular a probabilidade do evento topo, ou qualitativamente para identificar potenciais causas e os caminhos para uma falha e por consequência o evento topo.

2.1 Associação das falhas

A abordagem aqui considera uma análise qualitativa, e que para a identificação dos fatores causais utiliza-se das informações obtidas das duas fases apresentadas acima para o desenvolvimento da árvore, assim como também a relação lógica das causas com o evento indesejável.

Uma compreensão técnica do sitema e de como ele pode falhar são requeridas para uma análise qualitativa. Os fatores causais são eventos associados as falhas como:

- Falha mecânica do componente/equipamento;
- Erro humano associados a procedimentos críticos, fator associado como (PRC);
- Falha de qualidade durante o processo que possam desencadear os eventos causais, seja elas, fabricação, recuperação, recebimento e armazenamento, fator associado como (QA);
- Falhas decorrentes a fase do ciclo de vida: Construção, montagem e instalação dos componentes, fator associado como (CO), (MO) e (IN) respectivamente aos ciclos;
- Eventos adjacentes, fator associado como (AD).

Os níveis mais baixos da árvore de um sistema analisado, conhecidos como eventos de base, ou modos de falha são desenvolvidos até que uma análise adicional se torne improdutiva, ou seja, não útil, podendo parar em um componente ou equipamento adjacente ou a partir da observância do controle ou quesito atribuído com base na matriz de criticidade da empresa, ou seja, na consideração da condionante de uso de um ou mais controles/quesitos que possam prevenir ou mitigar os eventos.

2.2 Classificação dos tipos de controles

Os controles podem prevenir os eventos indesejáveis, aqui chamados de controles preventivos (CP) ou mitigar as consequências, aqui chamado controle mitigatório (CM).

A avaliação dos controles/barreiras obtidas durante as duas fases acima são analisadas conforme a classificação da tabela 1 abaixo [2].

Tabela 1 – Tipos de Barreira e elementos de ligação “Detectar-Decidir-Atuar” (*Barrier Types and Linkage to ‘Detect-Decide-Act” elements)*

1 Engenheiro Mecânico e Consultor – HATCH
2 Engenheiro Mecânico e Consultor – HATCH
3 Engenheiro de controle e automação e Consultor – HATCH
4 Engenheiro Civil e de Meio Ambiente e Consultor – HATCH

Short Name	Barrier Type †	Description	Detect	Decide	Act	Examples
Passive	**Passive Hardware**	The barrier works by virtue of its presence.	N/A	N/A	N/A	Dike, blast wall, crash barrier, anti-corrosion paint
Active	**Active Hardware**	All elements of the barrier are executed by technology.	Technology (e.g., pressure sensor)	Technology (e.g., logic controller)	Technology (e.g., emergency shutdown valve)	Process control systems and Safety Instrumented Systems
Human ††	**Active Hardware + Human** (predominately hardware)	The barrier is a combination of human behavior and technological execution.	Technology (e.g., high-high level indicator and alarm)	Human (e.g., operator hears and responds to alarm)	Technology (e.g., emergency shutdown valve) OR Human (e.g., operator manually shuts valve)	Operator-activated ESD valve Gas alarm and decision by human to evacuate
	Active Human (predominantly human)	The barrier consists of human actions, often interacting with technology.	Human observation (e.g., operator walk around detects leak)	Human evaluation (e.g., decides to shut-down and isolate the equipment)	Human – but acting on technology (e.g., operator presses stop button or manually shuts a valve)	Operator detection and response (e.g., during structured walk arounds)
Continuous	**Continuous Hardware**	The barrier is always operating.	N/A	N/A	Technological	Ventilation system, impressed current cathodic protection

2.3 Identificação dos controles

Durante o desenvolvimento para a definição dos controles na árvore de falhas, é de extrema importância verificar se os controles apropriados foram identificados. Saber identificar se é ou não um controle faz a diferença. A identificação deve seguir a árvore de decisão conforme figura 1 abaixo [3].

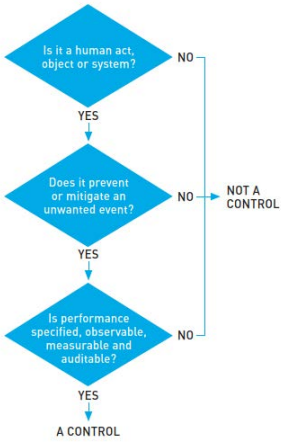

Figura 1 – Árvore de Decisão de Identificação de Controles (Control identification decision tree)

Após a identificação dos controles, faz se necessário a avaliação de criticidade para se determinar se são controles críticos ou não. Porque a partir desse ponto pode se assegurar as medidas necessárias para garantir que esses controles sejam eficázes durante o ciclo de vida do equipamento. Essa identificação deve ser feita através da ávore de decisão de controle crítico conforme figura 2 abaixo [3].

1 Engenheiro Mecânico e Consultor – HATCH
2 Engenheiro Mecânico e Consultor – HATCH
3 Engenheiro de controle e automação e Consultor – HATCH
4 Engenheiro Civil e de Meio Ambiente e Consultor – HATCH

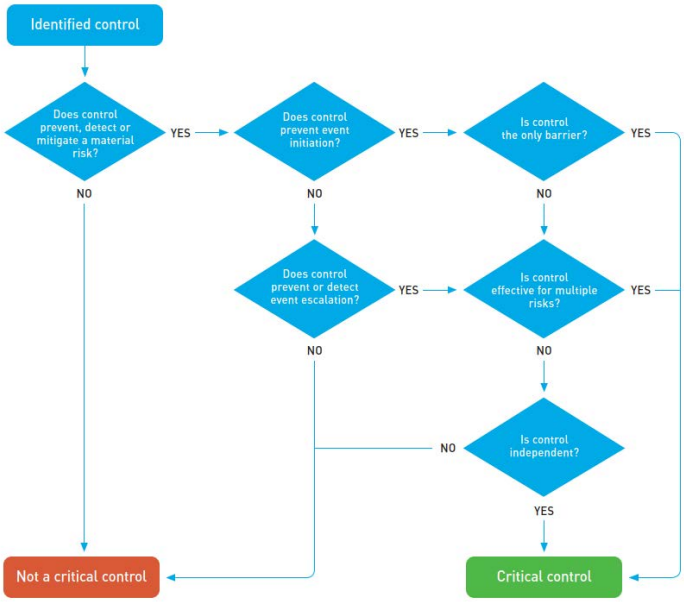

Figura 2 – Árvore de Decisão de Controle Crítico (Critical control decision tree)

De posse das potenciais causas e controles críticos tem-se uma visão clara dos caminhos de uma falha que irá desencadeiar eventos até o evento indesejável.

1. RESULTADO E DISCUSSÃO

Para exemplificar todo o processo acima descrito, na figura 3 é apresentado uma análise de árvore de falhas de simplificada de uma correia transportadora, considerando que o evento indesejável seja incêndio na correia.

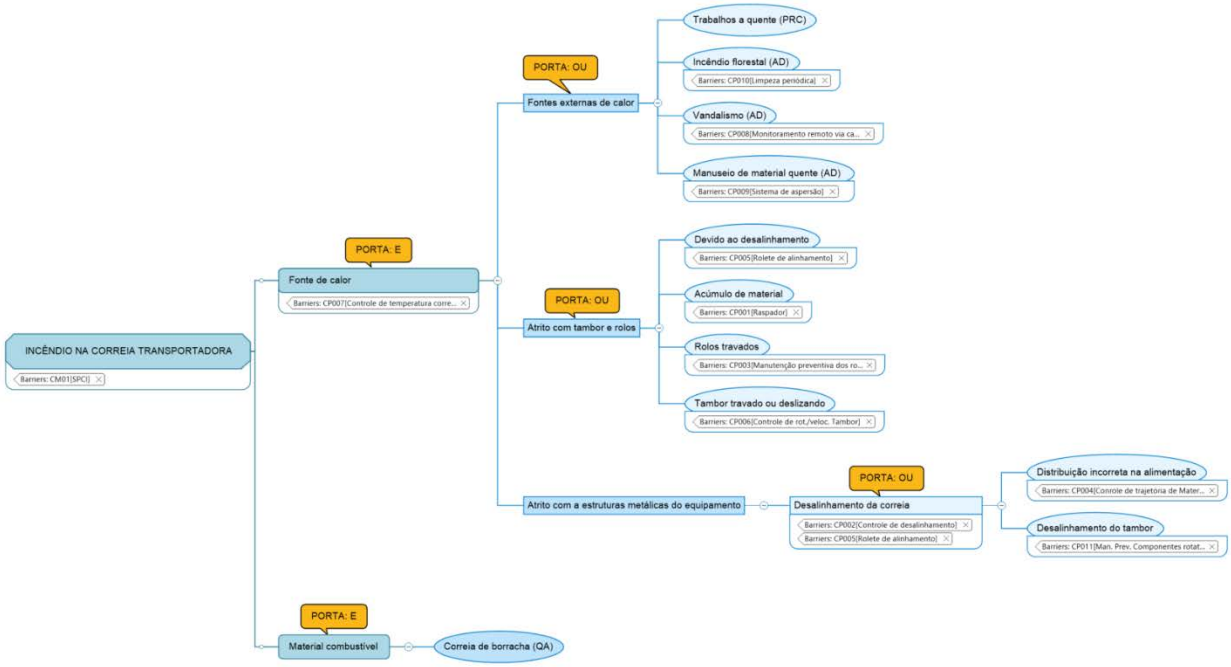

Figura 3 – Exemplo simplicado de uma ávore de falha

1 Engenheiro Mecânico e Consultor – HATCH
2 Engenheiro Mecânico e Consultor – HATCH
3 Engenheiro de controle e automação e Consultor – HATCH
4 Engenheiro Civil e de Meio Ambiente e Consultor – HATCH

2. COMENTÁRIOS FINAIS

A abordagem apresentada aplica o conceito "*top-down*", onde relaciona as falhas diretamente ao evento indesejável de uma forma multidisciplinar, sistemática e flexível. Ela uni a praticidade da observância dos fatores causais, pois apresenta uma facilidade no entendimento do sistemas com muitas interações e interfações através de representações gráficas, com a avalição crítica dos especialista e boas práticas da industria.

3. REFERENCES:

[1] *ISO 31000 – Risk Management – Guidelines*, (2018).

[2] *CCPS – Center for Chemical Process safety, Bow Ties in Risk Management. A Concept Book for Process Safety*, NY and UK (2018).

[3] *ICMM – International Council on Mining & Metals, Health and Safety Critical Control Management - Good Practice Guide*, UK (2015).

1 Engenheiro Mecânico e Consultor – HATCH
2 Engenheiro Mecânico e Consultor – HATCH
3 Engenheiro de controle e automação e Consultor – HATCH
4 Engenheiro Civil e de Meio Ambiente e Consultor – HATCH