

INTEGRIDADE DE POÇOS OFFSHORE: ANÁLISE DE SEGURANÇA DA ÁRVORE DE NATAL MOLHADA USANDO STPA

Lucas Ribeiro de Almeida, lucas.ribeiro.almeida@usp.br¹

Marco Aurélio Pestana, marco.pestana@usp.br¹

Joaquim Rocha dos Santos, jrsantos@usp.br¹

Marcelo Ramos Martins, mrmartin@usp.br¹

RESUMO

Apesar de ter uma das matrizes energéticas mais limpas do mundo, o setor energético brasileiro ainda é fortemente dependente do petróleo e gás natural, que muitos consideram como elemento fundamental para a transição energética para a economia de baixo carbono. No Brasil, a exploração de petróleo em operações offshore se reveste de vital importância, uma vez que grande parte do petróleo produzido no país tem origem no mar, sendo que boa parte de camadas muito profundas no pré-sal. Dada a complexidade e os riscos da fase de produção, é fundamental garantir a segurança do sistema durante sua operação. Partindo do pressuposto de que os métodos tradicionais de análise de segurança podem carecer de uma forma estruturada para abordar o problema à medida que a complexidade dos sistemas e ambientes aumenta, esse trabalho apresenta uma análise usando o STAMP (*System-Theoretic Accident Model and Process*) - e mais especificamente, sua ferramenta de análise de perigos STPA (*System Theoretic Process Analysis*) - com o propósito de demonstrar seu potencial como alternativa para conduzir análises de segurança. Esse trabalho apresenta uma análise STPA de uma Árvore de Natal Molhada (ANM), seguindo toda metodologia proposta pelos seus criadores: definição do propósito da análise; modelagem da estrutura hierárquica de controle, identificação das ações de controle não seguras; e identificação dos cenários de perdas. Como poderia ser esperado, pode-se identificar potenciais perigos que não estão relacionados a eventos de falha de componentes, mas às ações de operadores, combinações de eventos não triviais, entre outros. Os resultados encontrados reforçaram a ideia de que o uso do Pensamento Sistêmico na Análise de Segurança poderá ser uma ferramenta de grande auxílio na identificação de perigos importantes e não facilmente identificados por meio das técnicas tradicionais de análise.

1. INTRODUÇÃO

A exploração, desenvolvimento e produção de petróleo e gás natural envolve importantes desafios, aos quais são inerentes riscos tecnológicos, gerenciais, sociais, ambientais e econômicos [1]. Entre os principais riscos, encontra-se: a) o de liberação descontrolada de hidrocarbonetos do reservatório para o meio ambiente, o qual pode se dar, entre outros meios, pela perda de integridade dos poços produtores; e b) focando na fase de produção, sua paralisação inesperada causa diversos impactos negativos no poço, inclusive na sua integridade e potencial monetário. Neste sentido, a ANP (Agência Nacional do Petróleo, Gás Natural e Biocombustíveis) já prevê no seu SGIP (Sistema de Gerenciamento de Integridade de Poços) práticas gerenciais e medidas de diversas naturezas com o propósito de manter a integridade dos poços [2]. As práticas de gestão cobrem áreas tais como: treinamento, operação, auditorias etc. Os métodos tradicionais de análise de risco e confiabilidade nem sempre tem se mostrado a ferramenta mais adequada a análises envolvendo decisões nessas diversas áreas de conhecimento [3], que contém sistemas com forte acoplamento entre suas partes, complexa interação e requisitos normalmente conflitantes, além da inerente complexidade técnica que envolve a exploração de recursos minerais em operações offshore.

Com o propósito de aperfeiçoar e contribuir com a técnicas existentes, o STAMP foi idealizado como uma metodologia que parte de paradigmas diferentes dos métodos tradicionais [3]. De acordo com Leveson, os métodos mais tradicionais de análise foram idealizados a partir de uma visão de mundo com sistemas

¹ Laboratório de Análise, Avaliação e Gerenciamento de Riscos (LabRisco) – Escola Politécnica da Universidade de São Paulo

predominantemente analógicos, e hoje em dia poucos sistemas são construídos sem a inclusão de componentes digitais, os quais operam de modo diferente dos componentes analógicos que substituem. Ao mesmo tempo, a complexidade dos sistemas e dos ambientes onde operam tem aumentado cada vez mais. Com isso, métodos como a FTA (*Fault Tree Analysis*) e FMEA (*Failure modes and effects analysis*) podem acabar perdendo um pouco de sua efetividade, justamente por terem sido criados para sistemas com outras tecnologias.

A análise de segurança conduzida usando-se o STAMP aborda a questão como um problema de controle [3], onde o sistema é decomposto em várias malhas. Nesse método, os acidentes acontecem quando essas malhas não existem ou falham em cumprir sua função. É um método ainda em desenvolvimento, criado nos Estados Unidos e, atualmente, pouco usado no Brasil.

Seguindo a metodologia do STAMP, foi criado o STPA como uma ferramenta para a análise de perigos que, de acordo com sua própria criadora, “investiga um acidente antes que esse ocorra” [4]. O STPA é uma técnica de que, em adição às falhas de componentes, assume que acidentes também podem ser causados pela interação não segura dos níveis de controle do sistema, incluindo seus operadores e outros atores. Sendo capaz de detectar cenários de acidentes em casos em que não existem falhas físicas de componentes, seguindo uma metodologia estruturada

2. A ANÁLISE STPA

A análise STPA é dividida em 4 passos conforme a Figura 1. No primeiro passo é definido o alvo de estudo da análise, reunindo informações básicas como as fronteiras do sistema, stakeholders, perdas consideradas pelos stakeholders, perigos ligados à essas perdas e as restrições de atuação que o sistema deve cumprir para evitar os perigos. No segundo passo é modelada a Estrutura de controle (SCS) do sistema, indicando todos os níveis de controle, suas responsabilidades para com a segurança do sistema, e a natureza da interação entre os níveis. No terceiro passo são identificadas as Ações de Controle Não Seguras (UCA's), ou seja, as ações de controle de cada controlador que podem afetar a segurança do sistema. E no quarto passo é estudado como a interação entre os componentes do sistema pode induzir os controladores a executarem UCA's, criando cenários de perdas.

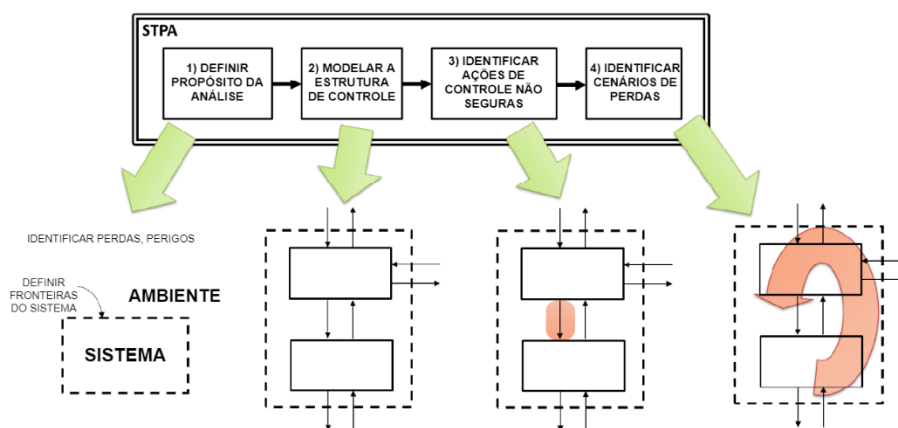


Figura 1: Passos do STPA [4]

É interessante notar que todos os passos da análise STPA fornecem informações sobre o sistema que podem ser utilizadas na prevenção de acidentes. Isso pois a análise visa estudar como um acidente pode vir a acontecer, sempre se relacionando com a SCS do sistema. Na Figura 2 estão apresentados dois elementos que resumem as saídas do STPA. As perdas acontecem se o sistema estiver num estado de perigo e isto se combinar com um determinado cenário de condições ambientais (chamado de cenário de pior caso). E o sistema pode entrar num estado de perigo quando um controlador executa uma ação de controle não segura. Então, para evitar as perdas tem-se que: a) impor restrições sobre a atuação do sistema (que geralmente negam os perigos em nível de sistema), das quais são retiradas as responsabilidades para que o controlador mantenha o sistema num estado seguro; e b). impor restrições sobre a atuação do controlador (que, em geral, negam as UCA's), para evitar a execução de ações de controle não seguras. Por fim, todas as informações obtidas com o STPA

podem ser utilizadas para desenvolver programas de prevenção de acidentes adicionais de modo a reforçar as restrições e responsabilidades. Como gerar novas restrições, programas de mitigação, e programas de *leading indicators* [5], [6]

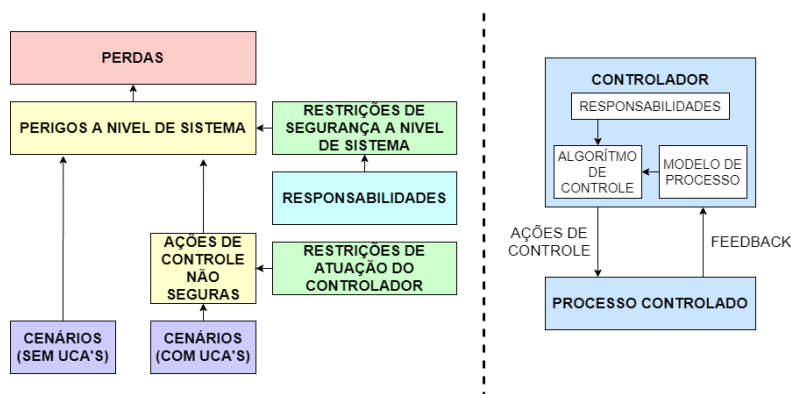


Figura 2: Resumo dos resultados do STPA e Bloco básico para construção da SCS [4]

3. ALGUNS RESULTADOS OBTIDOS

Durante a execução do STPA, é reunida uma grande quantidade de dados, sendo que todos são considerados como resultados da análise. Portanto a apresentação na totalidade dos resultados é inviável em um espaço reduzido, então nesta seção serão apresentadas apenas duas pontuações consideradas como as de maior interesse.

3.1 Anomalia na SCS da ANM

Ao finalizar a modelagem da SCS do sistema em questão, foi possível notar uma anomalia na mesma conforme apresentado na Figura 3: O operador não possui indicadores para saber o estado das válvulas que ele controla. Possui apenas um indicativo do histórico de comandos que ele acionou, porém esta informação quebra o loop de controle e feedback, é uma informação de feedback que independe do processo controlado (Sai direto do painel de switches para o display). Assim, se apenas o histórico de comandos for utilizado para aferir o estado das válvulas, o operador pode ser facilmente induzido a executar diversas ações não seguras, afetando a segurança do sistema.

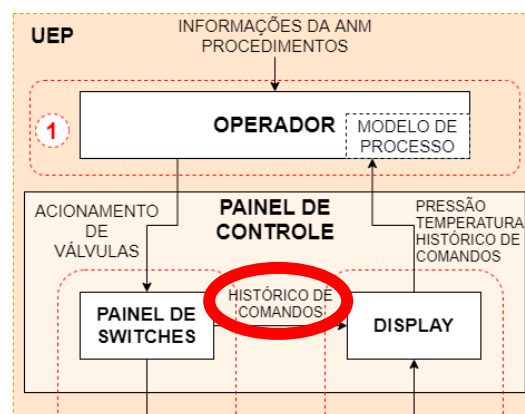


Figura 3: Recorte com anomalia da SCS modelada para a ANM

3.2 Cenários de acidentes sem falhas físicas

Ao final do processo, foram identificados 541 cenários de perdas. Em seguida, foi realizada uma classificação desses cenários de acordo com a natureza do fator causal, dividindo-o nas três categorias apresentadas na Figura 4 e nas proporções com que foram identificados. Pode-se perceber que os cenários que contém falhas físicas de equipamentos são apresentados numa proporção muito semelhante aos cenários onde não ocorre nenhuma falha de componentes (Falhas de modelo de processo ou falha humana). Diante de tais dados já fica mais clara a contribuição que o STPA pode trazer para a segurança de sistemas ao abordar o problema de uma perspectiva diferente.

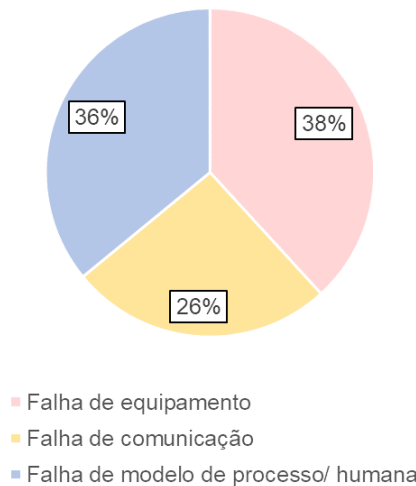


Figura 4: Distribuição dos cenários identificados de acordo com sua natureza

4. CONCLUSÃO

O objetivo principal deste trabalho foi apresentar brevemente uma análise STPA para demonstrar a aplicabilidade do STAMP em sistemas com forte acoplamento entre suas partes; mais especificamente, a aplicação da ferramenta na análise de segurança de um poço fase de produção. Neste trabalho, optou-se por apresentar a análise de um único equipamento – as ANM, que são usadas durante a fase de produção dos poços; entretanto, mesmo com a fronteira do sistema tão reduzida, já foi possível demonstrar como o STAMP pode contribuir para o aprimoramento da análise de segurança, contribuindo com os demais métodos mais tradicionais. Abordar um problema partindo de uma perspectiva diferente pode contribuir para a identificação de fatores que antes passariam despercebidos. E esta é a proposição fundamental do STAMP: Abordar o problema da segurança partindo das interações de ações de controle e feedback no sistema, ao invés de procurar combinações lógicas de eventos.

Como sugestão de trabalhos futuros, entende-se que o tema abordado é extenso com diversas possibilidades para o prosseguimento dos estudos apresentados. Dentre elas a aplicação da técnica às demais fases de vida do poço, a inclusão de outros fatores que influenciam na produção de petróleo, como por exemplo: as unidades estacionárias de produção, sistemas de armazenamento e transporte, e outros.

5. AGRADECIMENTOS

O presente trabalho foi realizado com apoio financeiro do Programa de Recursos Humanos da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis – PRH-ANP, suportado com recursos provenientes do investimento de empresas petrolíferas qualificadas na Cláusula de PD& I da Resolução ANP nº 50/2015.

6. REFERÊNCIAS

- [1] MORAIS, J. M., *Petróleo Em Águas Profundas*, IPEA , Brasil (2013);
- [2] ANP, Resolução Anp No 46, De 1o.11.2016, Brasil (2016).
- [3] LEVESON, N. G., *Engineering a Safer World: Systems Thinking Applied to Safety*, The MIT Press, EUA (2016).
- [4] LEVESON, N. G., & THOMAS, J. P., *STPA Handbook*, EUA (2018).
- [5] LEVESON, N. G., “A systems approach to risk management through leading safety indicators”, *Reliab. Eng. Syst. Saf.*, vol. 136, pp. 17–34, (2015).
- [6] TAMIM et al., “A framework for developing leading indicators for offshore drillwell blowout incidents”, *Process Saf. Environ. Prot.*, vol. 106, pp. 256–262, (2017).