METODOLOGIA PARA ANÁLISE DE RISCO / CONFIABILIDADE DA INTERAÇÃO ENTRE OS SISTEMAS DE POTÊNCIA ELÉTRICA E DE AUTOMAÇÃO EM PLATAFORMAS DE PRODUÇÃO

Monteiro, Gilsa[1]; Fernandez, Margareth[2]; Contarini, Maria[3]; Oliveira; Luiz Fernando Seichas[4]; Diniz, Flávio Luiz Barros[5]; Vieira, Tobias Alvarenga[6]; Filho, Mário Aguiar[7]; Galvão, João Carlos[8].

[1,2,3] PETROBRAS / UN-RIO / ST / SPO; Rua. Gal Canabarro, nº500 / 5º andar – CEP: 20.271-900 – Rio de Janeiro / R.J, gilsa.utc@petrobras.com.br; margarethlima.utc@petrobras.com.br; mcontarini.utc@petrobras.com.br;
[4,5,6,7,8] DNV Principia; Rua. Sete de Setembro, 111 – 12º andar – CEP: 20.050-006– Rio de Janeiro / R.J, luiz.oliveira@dnv.com; flavio.diniz@dnv.com; tobias.vieira@dnv.com; mario.filho@dnv.com; joão.carlos.galvao@dnv.com.

Resumo:
Em 2002, a Unidade Petrobras P-34 sofreu uma seqüência de eventos envolvendo interações entre os sistemas de potência elétrica e de automação, que acabaram por afetar de forma adversa a estabilidade deste FPSO (*Floating Production and Offloading*). A unidade chegou a alcançar uma banda de 34º que quase culminou com seu afundamento. Após a recuperação da unidade, buscou-se desenvolver uma metodologia de análise que pudesse investigar interações entre esses sistemas, ou seja, eventos que afetassem silmultânea ou sequencialmente a estabilidade da plataforma, provocando situações críticas de adernamento ou afundamento.

O presente trabalho consiste numa nova abordagem de análise de risco e confiabilidade com foco na interação dos sistemas de potência elétrica e automação, além dos sistemas de potência hidráulica e de lastro, que sejam capazes de levar uma unidade flutuante à situações de adernamento ou afundamento. A técnica considera a aplicação de duas metodologias clássicas de análise de risco e confiabilidade (FMECA – *Failure Mode and Effect Analysis* e Árvore de Falhas), onde o fator humano também é considerado, tendo sido aplicada à uma unidade do tipo semi-submersível (SS) da Petrobras.

Palavras-Chave: adernamento; árvore de falhas; confiabilidade; risco.

Abstract:
In 2002, Petrobras P-34 had a sequence of events involving interactions between electrical and automation systems that adversely affected the ballast, leading the platform to a heel of 34º and almost causing the FPSO capsize. Since that, an increased focus was placed on the development of a methodology that could investigate possible interactions between these systems, which could cause heeling or even sinking of floating platforms.

This paper considers a new approach to analyse interactions between automation, electrical, ballast and hydraulic power systems that can lead the floating platform to a loss of stability. It comprises the following steps:

A) Functional FMECA (Failure Mode, Effects and Criticality Analysis), which has been applied to obtain knowledge of how systems work and how they interact;

B) FT (Fault Trees), developed to investigate the sequence of events that could lead the platform to one of the final states considered. Considerations about human responses, like human errors as well as failure recovery, permeated this analysis.

These traditional reliability methods are being applied in a new approach, where the human factor is also considered and the focus is the interactions between these systems and not their individual functioning. The methodology was applied in a Petrobras SS (Semi-Submersible) Platform.

Keywords: Heeling; reliability, fault trees, risk.

1. Introdução

As complexas instalações de produção da atualidade que lidam com produtos perigosos são projetadas de modo a prover barreiras múltiplas contra os vários tipos de acidentes capazes de ocorrer durante a operação das mesmas. Em particular, naquelas que dependem de sistemas automatizados para a garantia da segurança dos seus processos produtivos, os efeitos decorrentes de interações imprevistas entre os vários sistemas podem ser altamente deletérios para a manutenção da segurança operacional da instalação. Inúmeros acidentes em diversos setores industriais foram causados por eventos que se originam em um dos sistemas e que afetam outros, chegando a comprometer completamente a segurança e resultando em sérios danos para a instalação envolvida. Tais eventos são denominados "interações entre sistemas".

Interações entre sistemas são, portanto, aqueles eventos que afetam simultânea ou seqüencialmente vários sistemas de uma instalação de uma forma não prevista no projeto, causando uma grave deterioração das condições de segurança operacional da instalação. Isto normalmente decorre de uma interação entre componentes ou subsistemas, podendo ou não envolver atividades humanas, resultando em uma redução do grau de redundância do projeto, ou ainda mais geralmente, em um decréscimo da probabilidade de que uma ou mais funções de segurança operem com sucesso (redução da confiabilidade do sistema). De um modo geral, pode-se dizer que as interações entre sistemas são uma forma de dependência (probabilística ou determinística) entre os sistemas, as quais podem contribuir significativamente para o aumento do nível de risco das instalações.

Portanto, a definição de interação entre sistemas inclui tanto as interações aleatórias como aquelas denominadas não-aleatórias (ou seja, determinísticas). Neste último caso, a falha de um dado sistema ou a ocorrência de um evento externo resultaria com certeza absoluta na perda imediata da função (total ou parcial) de outro(s) sistema(s). Ambos os tipos de interação são de grande importância para a confiabilidade dos sistemas e para a segurança operacional da instalação.

Na área *offshore*, o recente acidente na P-34, ilustrado na Figura 1, foi um exemplo típico de uma situação onde aconteceram interações entre sistemas que chegaram a comprometer a segurança do FPSO, neste caso envolvendo, particularmente, os sistemas: de automação, de potência elétrica, de potência hidráulica, de lastro e carregamento da plataforma. A partir desse acidente, a Petrobras direcionou esforços para o desenvolvimento de uma metodologia de análise capaz de avaliar as possíveis interações entre esses sistemas que pudessem levar as unidades flutuantes de produção à perda de estabilidade, considerando também o fator humano nestas possíveis seqüências de eventos.

Figura 1. Acidente da P-34 em Outubro de 2002

2. Objetivos do Trabalho

Este trabalho objetivou fundamentalmente desenvolver uma metodologia para análise dos impactos sobre a estabilidade de unidades flutuantes de produção, decorrentes de eventos de falha envolvendo interações entre os sistemas de suprimento de potência elétrica (SPE), de automação e intertravamento de segurança (SAIS), de potência hidráulica (SPH) e de lastro (SLA). As considerações sobre as respostas humanas, tanto negativas (erros humanos) como positivas (recuperação de falhas durante uma seqüência de eventos acidentais) permearam a análise como um todo. A metodologia foi aplicada numa unidade Petrobras tipo semi-submersível (SS).

Vale ressaltar que o sistema de potência elétrica envolve tanto a geração (principal e de emergência), como os sistemas de distribuição em corrente alternada e contínua. Já no sistema de automação, são considerados: sensores (iniciadores de sinais), os painéis das remotas, os controladores lógicos programáveis (CLPs), o sistema supervisório (ECOS) e os atuadores (válvulas, motores, etc.).

3. Metodologia de Análise

A metodologia desenvolvida consiste em uma combinação entre duas técnicas de risco e confiabilidade tradicionais: FMECA (*Failure Mode and Effect Analysis*) e AF (Árvore de Falhas). Trata-se de um estudo pioneiro na área *offshore*, onde ambas as metodologias possibilitaram a análise das interações entre os sistemas.

A utilização conjunta das técnicas analíticas referidas acima certamente oferece um nível adequado de detalhamento para este trabalho, ou seja, propicia um grau de certeza adequado de que, pelo menos, as interações mais críticas sejam identificadas e avaliadas. É importante frisar que **nenhuma metodologia é capaz de garantir que sejam identificadas todas as possíveis interações** entre os vários sistemas de uma instalação complexa, tal qual uma plataforma *offshore* de produção. O que se busca é a identificação e avaliação do maior número possível de interações, cujo resultado certamente inclui as interações mais críticas para a segurança.

3.1. Aplicação da FMECA:

A realização da FMECA possibilitou o entendimento do funcionamento dos sistemas e de como eles interagem, explicitando principalmente as maiores dependências existentes. Por outro lado, a utilização desta técnica também proporcionou uma abordagem qualitativa de classificação de risco das funções estudadas. Esta classificação foi extremamente útil durante o processo de hierarquização de ações e de proposição de melhorias para os sistemas estudados, possibilitando identificar as funções com alta criticidade, que podem vir a motivar estados finais críticos para a plataforma.

Nesta fase, as funções de cada sistema foram listadas de forma a se avaliar:

a) os componentes responsáveis pelo cumprimento da função;

b) os modos de falha desses componentes;

c) a freqüência esperada de ocorrência do modo de falha, conforme ilustrado na Figura 2;

d) os efeitos da perda da função;

e) a severidade dos efeitos, conforme ilustrado na Figura 3;

f) a categoria de risco de cada cenário analisado, através da combinação dos valores de freqüência e severidade, conforme matriz de risco ilustrada na Figura 4.

Figura 2. Categorias de Frequência Utilizadas na FMECA

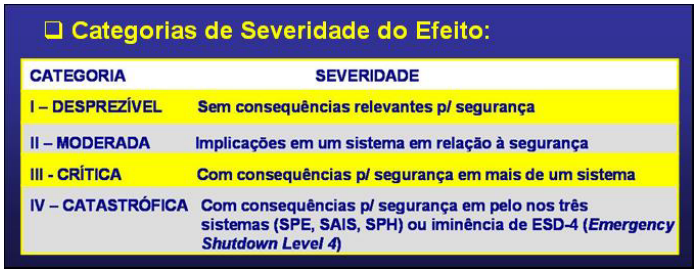

Figura 3. Categorias de Severidade Utilizadas na FMECA

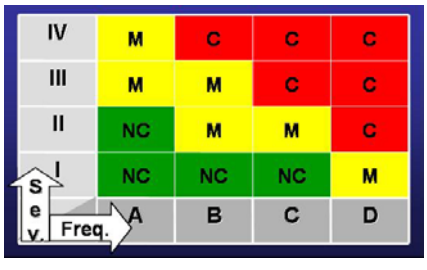

Figura 4. Matriz de Risco Utilizada na FMECA

3.2. Árvores de Falha

3.2.1. Detalhamento dos Estados Finais Considerados:

O desenvolvimento das árvores de falhas foi feito de modo a se identificar as combinações lógicas dos eventos básicos (falhas de componentes) que pudessem levar a unidade SS a estados finais críticos para a sua estabilidade, os quais foram detalhados conforme ilustrado na Figura 5:

Figura 5. Estados Finais CríticosConsiderados na Análise

3.2.2. Definição dos Eventos Topo das Árvores de Falha:

A definição dos eventos topo indesejados das árvores de falha foi feita de forma a identificar os eventos que pudessem levar a unidade a um dos estados finais apresentados na Figura 5. A Tabela 1 apresenta alguns eventos indesejados considerados como eventos topo das árvores de falha e o estado final ao qual estão associados:

Tabela 1. Listagem de eventos indesejados considerados como eventos topo nas árvores de falha.

Eventos Indesejados (Eventos Topo das Árvores de Falha)	Estado Final da Plataforma
Alagamento da Couna PC1	Adernamento Moderado
Alagamento da Couna PC4	Adernamento Moderado
Perda do Sistema de Lastro	Adernamento Leve
Perda do Sistema de Deslastro	Adernamento Leve

3.2.3. Construção das Árvores de Falha

A partir do conhecimento a cerca do funcionamento dos sistemas considerados e de suas interações, foi construída uma árvore de falhas para cada um dos eventos topo definidos. Para exemplificar, a Figura 7 ilustra parte da árvore de falhas construída para o evento “Alagamento da Coluna PC4”. O alagamento dessa coluna, a qual é ilustrada na Figura 6, gera um adernamento de 15,92º, considerado moderado, conforme categorias definidas na subseção 3.2.1.

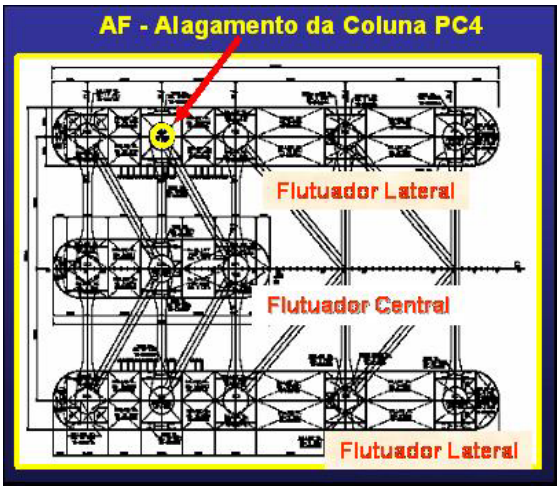

Figura 6. Alagamento da Coluna PC4

Como premissa para construção dessa árvore, foi considerado que a operação de lastro ou deslastro do *pontoon* correspondente à coluna PC4 está sendo realizada quando ocorre ruptura de uma linha do sistema de lastro que passa pela sala de bombas existente na coluna. Quatro diferentes casos de ruptura nessa linha foram considerados. A Figura 7 ilustra parte do caso que envolve ruptura num flange de 14”.

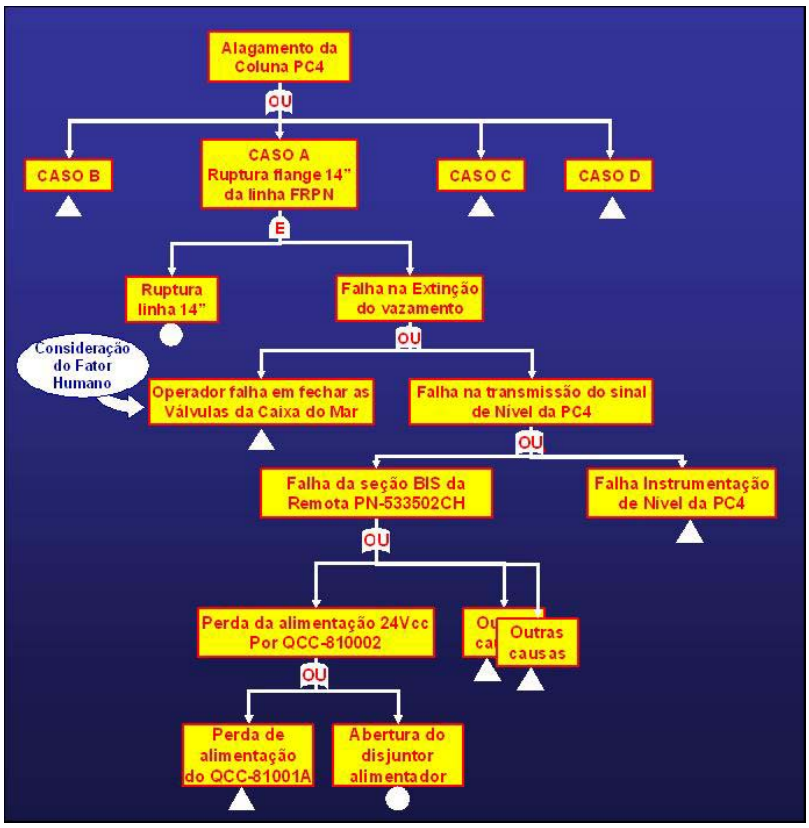

Figura 7. AF do Alagamento da Coluna PC4

3.2.4. Análise dos Cortes Mínimos das Árvores de Falha

Uma vez construída a árvore de falhas para cada um dos eventos topo definidos, procedeu-se a avaliação qualitativa das combinações dos eventos básicos ou não desenvolvidos que causam a ocorrência desse evento topo. Ou seja, procedeu-se à identificação dos cortes mínimos da árvore.

Denomina-se corte de uma árvore de falhas qualquer conjunto de eventos básicos ou não desenvolvidos cuja ocorrência ou existência simultânea implica na ocorrência do evento topo, ou seja, na falha do sistema. Desta forma, um corte pode ser definido como uma combinação de eventos básicos (como por exemplo: falhas dos componentes) que ao ocorrerem levam necessariamente à falha do sistema (ocorrência do evento topo da AF).

Um corte é denominado corte mínimo quando for constituído pelo menor número possível de eventos básicos cujas ocorrências simultâneas permitem observar o evento topo da árvore de falha. Em outras palavras, um corte mínimo é um conjunto de eventos cuja ocorrência é necessária e suficiente para causar a ocorrência do evento topo, não podendo ser reduzido sem perder a sua condição de corte.

Outro conceito importante é o de ordem de um corte mínimo, que pode ser definido como o número de eventos pelos quais o corte é formado. Assim, por exemplo, um corte composto de apenas um evento é denominado um corte mínimo de primeira ordem, ou seja, basta apenas que um evento ocorra para que o evento topo venha a ocorrer. Já um corte composto de dois eventos é um corte de segunda ordem. Em um sistema complexo, a existência de cortes de primeira ordem pode ser um indicador de baixa confiabilidade do sistema, pois significa que há falhas únicas capazes de causar a falha do sistema. Obviamente que isto nem sempre é verdadeiro, pois mesmo cortes de primeira ordem podem ter baixas probabilidades de falhas, o que não necessariamente compromete a confiabilidade do sistema.

Os critérios utilizados para a identificação e seleção dos cortes mínimos analisados no estudo foram baseados nas condições listadas abaixo:

a) Número de cortes na ordem de milhar. Ou seja, são analisados quantas ordens de corte foram necessárias até que o evento indesejado esteja representado por milhares de cortes;

b) São analisados todos os eventos básicos da menor ordem encontrada e os vinte eventos básicos com maior grau de ocorrência da ordem subsequente.

Esse critério permitiu detalhada análise dos cortes mínimos. Vale ressaltar que para que um corte seja analisado, basta que ao menos um de seus eventos básicos o sejam.

4. Conclusões:

As árvores de falhas qualitativas evidenciaram problemas de interações entre os sistemas, permitindo a identificação dos "pontos fracos" e a elaboração de propostas de melhorias. A metodologia desenvolvida permitiu avaliar, de forma estruturada e sistemática, as falhas decorrentes das interações entre sistemas, as quais poderiam levar à unidade à situações de adernamento ou afundamento.

Tendo como melhor fase para aplicação a de projeto de detalhamento e com uma duração estimada de seis meses, já se avalia a possibilidade de implementar essa metodologia de análise de forma sistemática nos novos projetos das unidades flutuantes de produção de petróleo e gás.

5. Referências

OLIVEIRA, LUIZ FERNANDO S. DE, O Estágio Atual da Aplicação de Confiabilidade na Indústria Brasileira de Processos Químicos, IV Encontro Técnico Sobre Engenharia da Confiabilidade, ETEC IV, PETROBRAS, Rio de Janeiro, 8 a 10 de agosto de 1995.

VESELY, W.E., "A Time Dependant Methodology for Fault Tree Evaluation", Nuclear Engineering Desing 13, p. 337 (1970).

PES, Programmable Electronic Systems in Safety Related Applications, 2.General Technical Guidelines, HSE - Health and Safety Executive, 1987.

AICHE, Guidelines for Preveting Human Error in Process Safety (1994).

HSE, Reducing Error and Influencing Behaviour (2000).

P. F. MELO, J. E. LIMA, I. L. STAL e L. F. OLIVEIRA, "ETAP1: A Code for Performing Event Tree Analysis", ANS Transactions 46, Jun/1984, p.521.

P. F. MELO,V. FLEMING, J. E. LIMA, I. L. STAL E L. F. OLIVEIRA, "Computer-Aided Event Tree Analysis with Uncertainty Propagation", Proceedings of the International Seminar on Implications of Probabilistic Risk Assessment, Blackpool, U.K., Mar/1985.

L. F. OLIVEIRA, P. F. MELO, J. E. LIMA E I. L. STAl, "An Application of the Explicit Method for Analysing Intersystem Dependencies in the Evaluation of Event Trees", Nuclear Engineering and Design 90, 1985, p.25.

P. F. MELO, J. E. LIMA, L F. OLIVEIRA, "Some Insights on the Event Tree Methodology Used for the Ongoing Angra 1 PRA", Proceedings of the 8th International Conference on Structural Mechanics in Reactor Technology (SMIRT 8), Bruxelas, Belgica, Ago/1985.

ROBERTS, N. H., VESELY, W.E., HAASL, D.F., and GOLBERG, F.F.(1981), fault Tree Handbook, U.S. Nuclear Regulatory Comission, NUREG-0492. Washigton, D.C.

SHAFAGHI, A.,ANDOW, P.K., AND LEES, F.P.(1984). "Fault Tree Synthesis Based on Control Loop Structure." Chemical Engineering Ressearch and Design 62,101-110;

SWAIN, A.D., and GUTMANN, H.E.(1983) Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Aplications. Sandia National Laboratories. NUREG/CR-1278 Washington, DC:U.S. Nuclear Regulatory Comission.