UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM ENGENHARIA DE PRODUÇÃO

Juliano Couto Portela

ABORDAGENS DE SEGURANÇA OPERACIONAL DA USINA HIDRELÉTRICA ITAIPU BINACIONAL SOB A PERSPECTIVA DA ENGENHARIA DE RESILIÊNCIA

Porto Alegre
2016

Juliano Couto Portela

ABORDAGENS DE SEGURANÇA OPERACIONAL DA USINA HIDRELÉTRICA ITAIPU BINACIONAL SOB A PERSPECTIVA DA ENGENHARIA DE RESILIÊNCIA

Dissertação submetida ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal do Rio Grande do Sul como requisito parcial à obtenção do título de Mestre em Engenharia de Produção, modalidade Profissional, na área de concentração em Sistemas de Produção.

Orientador: Lia Buarque de Macedo Guimarães, PhD.

Porto Alegre

2016

Juliano Couto Portela

ABORDAGENS DE SEGURANÇA OPERACIONAL DA USINA HIDRELÉTRICA ITAIPU BINACIONAL SOB A PERSPECTIVA DA ENGENHARIA DE RESILIÊNCIA

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia de Produção na modalidade Profissional e aprovada em sua forma final pelo Orientador e pela Banca Examinadora designada pelo Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal do Rio Grande do Sul.

_____

Profa. Lia Buarque de Macedo Guimarães, PhD
Orientador PPGEP/UFRGS

_____

Prof. Jose Luis Duarte Ribeiro, Dr.
Coordenador PPGEP/UFRGS

Banca Examinadora:

Professor Éder Henriqson, Dr. (PUC-RS)

Professor Marcelo Fabiano Costella, Dr. (UNOCHAPECÓ)

Professor Tarcísio Abreu Saurin, Dr. (UFRGS)

A Bianca, Andrei, Julia Victoria, Bruna:
o verdadeiro significado de “riqueza”.
A meus mestres, professor Couto e Joanna,
que leem este trabalho de onde estiverem:
obrigado.

AGRADECIMENTOS

À minha família, sem a qual jamais estaria onde estou.

À professora Lia, sempre com a palavra adequada na hora certa.

Aos colegas da Itaipu Binacional, que com suas observações permitiram que este trabalho evoluísse de maneira tão fluida.

À Itaipu Binacional, por investir na formação de seus profissionais, em especial àqueles que tornaram possível este importante passo.

A luz, o sol, o ar livre
envolvem o sonho do engenheiro.
O engenheiro sonha coisas claras:
superfícies, tênis, um copo de água.

O lápis, o esquadro, o papel;
o desenho, o projeto, o número:
o engenheiro pensa o mundo justo,
mundo que nenhum véu encobre.

(Em certas tardes nós subíamos
ao edifício. A cidade diária,
como um jornal que todos liam,
ganhava um pulmão de cimento e vidro).

A água, o vento, a claridade
de um lado o rio, no alto as nuvens,
situavam na natureza o edifício
crescendo de suas forças simples.

João Cabral de Melo Neto, em *O Engenheiro* (1945)

"Don't keep forever on the public road, going only where others have gone. Leave the beaten track behind occasionally and dive into the woods. You will be certain to find something you have never seen before, and something worth thinking about to occupy your mind. All really big discoveries are the result of thought.

Alexander Graham Bell, citado por Ralph Whiteside (1947)

RESUMO

Acidentes graves em organizações com infraestruturas críticas, como a Usina Hidrelétrica Itaipu Binacional, embora raros, causam importantes impactos sociais e econômicos em sua área de influência. Portanto, eles devem ser evitados mesmo que, seja esperada uma taxa "normal" de acidentes por conta dos fatores de risco e complexidade da sua operação. Essa dissertação apresenta uma investigação das condições que levam a acidentes em casos específicos da operação da Itaipu Binacional sob o enfoque proativo da gestão da Segurança II de acordo com a Engenharia de Resiliência (ER). Ela se baseia na variabilidade da operação normal e, portanto, "no muito que dá certo", em contraponto à visão tradicional da Segurança I, reativa, baseada na análise retrospectiva de acidentes e "no pouco que dá errado". Com base em uma revisão da literatura quanto os requisitos, princípios e temas da ER e da Segurança-II e nas opiniões estruturadas de operadores foram desenvolvidos dois estudos: o primeiro traçou preocupações destes operadores em relação ao risco de incêndio em um transformador da Itaipu Binacional para desenvolver indicadores e planos de ação aderentes aos princípios da ER. O objetivo foi suplementar, com elementos de ER, uma análise de risco convencional baseada em árvore de falhas e árvore de eventos, e otimizar o plano de ação de emergência em caso de incêndio em transformador da unidade geradora. Os resultados mostraram a oportunidade de melhoria para o desenvolvimento de indicadores proativos para a análise de risco. O segundo estudou, com base no método FRAM, a operação normal e a variabilidade de quatro manobras operacionais típicas selecionadas pelos operadores dentro dos quadrantes da matriz periodicidade-complexidade. Os resultados indicaram que as mesmas variabilidades influenciam nos passos operacionais, não importando a complexidade tampouco a periodicidade da manobra. Um comparativo entre a análise das variabilidades em situação normal e os relatórios das quatro falhas ocorridas entre 2006 e 2015 apontou que o sucesso e a falha advêm da mesma fonte, e que algumas variabilidades como "ambiente de manobra", a "necessidade de confirmar os passos das manobras" e situações que tiram a atenção do operador atuam de forma decisiva em praticamente todas as manobras. Os resultados foram discutidos com os integrantes da equipe que propuseram adaptações necessárias para aumento da segurança operacional do trabalho normal sob a perspectiva de ER.

Palavras-chave: Engenharia de Resiliência, Segurança-II, Análise de Risco, Segurança Operacional

ABSTRACT

Serious accidents in organizations with critical infrastructures, such as the Itaipu Binacional Hydroelectric Power Plant, although rare, cause important social and economic impacts in their area of influence. Therefore, they must be avoided even if a "normal" rate of accidents is expected because of the risk factors and complexity of the operation. This dissertation presents an investigation on the conditions that lead to accidents in the operation of Itaipu Binacional under the proactive approach of Security II management according to Resilience Engineering (RE). It is based on the variability of the normal operation and, therefore, "in the many things that goes right", in contrast to the traditional and reactive view of Safety-I, based on the retrospective analysis of accidents and "the few things that went wrong". After a review of the literature on the requirements, principles and themes of RE and Security-II and on the structured opinions of the operational staff, two studies were developed: the first one brings the concerns of these operators in regard of the risk of fire in a transformer in order to develop indicators and action plans adherent to the RE principles. The objective was to supplement a conventional risk analysis based on fault tree and event trees with RE elements, optimizing the emergency action plan. The results showed the opportunity for improvement of proactive indicators for risk analysis. The second one, inspired by the FRAM method, deals with the normal operation and variability of four typical operational maneuvers selected by operators within four quadrants of a periodicity-complexity matrix. The results indicated that the same variabilities influence the operational steps, regardless of the complexity or the periodicity of the maneuver. A comparison between the analysis of the variabilities in normal situation and the reports of the four operational failures occurred between 2006 and 2015 indicated that success and failure come from the same source, and that some variabilities such as “maneuver environment”, “necessity to confirm the maneuver steps” and “situations that take the attention of the operator” act decisively in virtually all maneuvers. The results were discussed with the team members who proposed the necessary adaptations to increase the operational safety of normal work from the RE perspective.

Keywords: Resilience Engineering, Safety-II, Risk Analysis, Operational Safety.

LISTA DE FIGURAS

Figura 1 Modelo gravata borboleta 24
Figura 2 Árvore de falhas simplificada para explosão de transformador 34
Figura 3 Árvore de eventos simplificada para explosão do transformador 35
Figura 4 Variação de valores de R_t para diferentes Ir_n e p_n 36
Figura 5 Probabilidade de as coisas darem certo (acertos) e de darem errado (erros/falhas) ... 45
Figura 6 Manobras bem-sucedidas x falhas na Itaipu Binacional, período 2006 a 2015 50

LISTA DE TABELAS

Tabela 1 Resumo de princípios e temas de ER 29
Tabela 2 Categorização de profissionais ouvidos nas entrevistas 29
Tabela 3 Exemplo do tratamento das citações e formação do banco de dados 30
Tabela 4 Exemplos de repetições dos fatores de resiliência por cargo 31
Tabela 10 Pesos dos fatores de resiliência 32
Tabela 11 Ações e indicadores de resiliência propostos 33
Tabela 7 Perfil dos profissionais envolvidos no estudo 49
Tabela 8 Manobras contempladas no estudo no período de 2006 a 2015 51
Tabela 9 Variabilidades que influenciam a operação 52
Tabela 10 Exemplo de manobra e variabilidades 53
Tabela 11 Número de passos das manobras estudadas: total e "caminho crítico" 53
Tabela 12 Frequência das variabilidades nos passos "caminho crítico", cômputo geral 54
Tabela 13 Frequência das variabilidades nos passos "caminho crítico", estratificado 55
Tabela 14 Ações propostas 57
Tabela 15 Variabilidades na falha operacional de 2010 59
Tabela 16 Variabilidades na falha operacional de 2008 60
Tabela 17 Variabilidades na primeira falha operacional de 2014 61
Tabela 18 Variabilidades na segunda falha operacional de 2014 62
Tabela 19 Resumo das variabilidades nas quatro falhas 63

SUMÁRIO

1 INTRODUÇÃO 12
1.1 COMENTÁRIOS INICIAIS 12
1.2 TEMA E OBJETIVOS 14
1.3 JUSTIFICATIVA 14
1.4 MÉTODO 15
1.5 ESTRUTURA DO TRABALHO 17
1.6 DELIMITAÇÕES DO TRABALHO 18

2 SUPLEMENTAÇÃO DA ANÁLISE DE RISCO COM ELEMENTOS DE ENGENHARIA DE RESILIÊNCIA PARA INCÊNDIO DOS TRANSFORMADORES PRINCIPAIS DA USINA HIDRELÉTRICA ITAIPU BINACIONAL 19
2.1 INTRODUÇÃO 19
2.2 REFERENCIAL TEÓRICO 21
2.2.1 Indicadores de segurança 21
2.2.2 Princípios da resiliência 22
2.2.3 Método da gravata borboleta 23
2.3 MÉTODO 25
2.4 RESULTADOS E DISCUSSÃO 28
2.4.1 O Plano de Ações de Emergência 28
2.4.2 Formação dos requisitos de ER 29
2.4.3 Percepções colhidas nas entrevistas e aderência aos princípios de resiliência 29
2.4.4 Repetições e pesos aplicados aos Fatores de Resiliência 31
2.4.5 Aplicações dos fatores de resiliência às árvores de falhas e de eventos 34
2.5 CONCLUSÃO 37
2.6 REFERÊNCIAS 38

3 FOCO NO SUCESSO: ABORDAGEM DE SEGURANÇA-II PARA MANOBRAS OPERACIONAIS DA USINA HIDRELÉTRICA ITAIPU BINACIONAL 41
3.1 INTRODUÇÃO 41
3.2 REFERENCIAL TEÓRICO 43
3.2.1 Abordagem reativa da Segurança-I 43
3.2.2 Abordagem proativa da Segurança-II 45
3.3 MÉTODO 47
3.4 RESULTADOS E DISCUSSÃO 50
3.5 CONCLUSÃO 64
3.6 REFERÊNCIAS 66

4 COMENTÁRIOS FINAIS 67
4.1 CONCLUSÃO 67
4.2 SUGESTÕES PARA TRABALHOS FUTUROS 68

REFERÊNCIAS 70

1 INTRODUÇÃO

1.1 COMENTÁRIOS INICIAIS

Infraestruturas críticas (IC) são sistemas, serviços e bens vitais para o bem-estar da sociedade cuja perturbação ou destruição causa impactos graves sobre a saúde, segurança e bem-estar econômico dos cidadãos (LABAKA; HERNANTES; SARRIEGI, 2015). Qualquer destas infraestruturas, para serem bem-sucedidas em sua operação, devem possuir pelo menos algumas das características das Organizações de Alta Confiabilidade (OACs), aquelas que, mesmo inseridas em um ambiente no qual uma taxa "normal" de acidentes seria esperada por conta dos altos fatores de risco e complexidade inerentes a sua operação, são bem-sucedidas em evitá-los ao longo de seu ciclo operacional (SÆTREN; LAUMANN, 2014).

Um exemplo de OAC é a Usina Hidrelétrica Itaipu Binacional que fornece aproximadamente 17% da energia consumida pelo mercado brasileiro e 80% da consumida pelo mercado paraguaio. É a maior geradora de energia do mundo, já tendo produzido mais de 2,4 bilhões de MWh em seus 32 anos de operação (ITAIPU BINACIONAL, 2016a), e possui potencial de causar perda de produção e estabilidade dos sistemas nela interconectados. Apesar de jamais ter sido a causa primária de um blecaute no sistema elétrico brasileiro (PORTELA et al., 2011), os riscos associados à falta de esquemas específicos de proteção para todas as situações previstas (e, obviamente, as imprevistas) e à complexidade de seu sistema de operação exigem reflexão contínua sobre a capacidade de seu *staff* de garantir a segurança das instalações e da produção de energia, e portanto da estabilidade dos sistemas a ela conectados, em situações previstas e imprevistas.

No entanto, o modo de operação e manutenção (O&M) de instalações elétricas em geral vem sendo fortemente afetado pelas acentuadas mudanças tecnológicas de seus equipamentos e sistemas. Tais mudanças, por um lado, aumentam a capacidade de supervisão e monitoramento das condições ambientais das organizações. Onde antes existiam relés de proteção eletromecânicos, robustos, porém limitados na capacidade de fornecer análise e diagnóstico do sistema, hoje *Intelligent Electronic Devices* (IEDs) proveem uma série de variáveis e sinais de monitoramento que permitem a predição de defeitos através de gráficos de tendências das mais diversas variáveis. É inegável o intuito de garantir o alto nível de confiabilidade e segurança em seus serviços, mas ao fazê-lo também viu-se aumentada a vulnerabilidade operacional, o número de agentes envolvidos em uma situação de crise em

infraestruturas críticas e, por consequência, a complexidade da gestão de crises (LABAKA; HERNANTES; SARRIEGI, 2015). Neste ponto, as vulnerabilidades sociais associadas à mudança tecnológica de estruturas críticas devem considerar suas características: no caso do setor elétrico, os riscos associados à mudança da tecnologia são altos e a velocidade das mudanças é alta (KRÖGER, 2008). Isto é corroborado pelos acidentes graves em instalações com estas características (Sayano-Shushenskaya, 2009; Deepwater Horizon, 2010; Fukushima, 2011) onde situações não vivenciadas até o momento do acidente passaram despercebidas em algum momento da operação e foram determinantes para a falha catastrófica.

Para que estas infraestruturas continuem sua operação bem-sucedida neste novo contexto, é importante evoluir a gestão da segurança: de reativa, baseada na análise retrospectiva de acidentes e "no que dá errado", para proativa, baseada na operação normal e "no que dá certo". Essa nova abordagem suplementa as técnicas de análise de acidentes/incidentes, que normalmente apontam as causas-raiz destas ocorrências para falhas humanas, em componentes, equipamentos ou sistemas (HASSAN; KHAN, 2012).

Para prover novo rumo à investigação das condições que levam aos acidentes e não somente ao estudo das causas que levaram a eles, a abordagem de gestão de segurança denominada Engenharia de Resiliência (ER) vem sendo utilizada em ambientes de alto risco (AZADEH et al., 2014). Resiliência, termo tomado de outros ramos do conhecimento, é seminalmente definida como "uma medida da habilidade dos sistemas em absorver mudanças em variáveis de decisão e em seus parâmetros, continuando a existir" (HOLLING, 1973). Quando aplicada a organizações, a resiliência apresenta outras capacidades que permitem gerenciar as atividades da organização para antecipar e evitar ameaças à sua existência e a seus objetivos (HALE; HEIJER, 2006). Para a ER, a gestão de segurança tradicional – denominada "Segurança-I" (HOLLNAGEL, 2014) – foca em manter a taxa de acidentes em um nível o mais baixo possível, enquanto a nova gestão – "Segurança-II" (HOLLNAGEL, 2014) – foca a probabilidade de sucesso levando em consideração a maior parte da operação normal, ou "o que normalmente dá certo", tornando a gestão mais proativa do que reativa (HOLLNAGEL; WEARS; BRAITHWAITE, 2015).

1.2 TEMA E OBJETIVOS

O tema dessa dissertação é a Engenharia de Resiliência e sua visão de segurança, ou Segurança-II, aplicada na Usina Hidrelétrica Itaipu Binacional, pois uma nova visão de segurança operacional faz-se necessária à luz das mudanças tecnológicas da organização e do impacto que eventuais acidentes de grandes proporções em tal estrutura pode causar às sociedades brasileira e paraguaia.

O objetivo maior é utilizar a abordagem não tradicional da segurança, ou Segurança-II, derivada da Engenharia de Resiliência (ER), na investigação das condições de operação das manobras da Usina Hidrelétrica Itaipu Binacional. Entre os objetivos específicos, podem ser citados: (i) apresentar os relativamente novos princípios, conceitos e heurísticas de ER, aplicando-os ao estudo de caso; (ii) por meio do processo participativo dos executantes, mostrar a aderência de suas preocupações com os princípios de ER e de Segurança-II; (iii) adicionar à análise de risco tradicional elementos não técnicos para suplementá-la; (iv) fornecer subsídios para a formação de indicador capaz de medir quantitativamente a capacidade da organização de antecipar, monitorar, prever, resistir e responder a uma disrupção; (iv) verificar, com base em resultados históricos, as relações entre sucessos e falhas operacionais e a aderência da teoria de Segurança-II às falhas operacionais havidas nos últimos dez anos na Itaipu Binacional; (v) propor ações para dirimir os riscos às falhas; (vi) estabelecer primeiros passos de nova cultura de segurança na Itaipu Binacional, organização de referência em muitos ramos do conhecimento.

A dissertação apresenta dois estudos: 1) a aplicação de princípios, conceitos e heurísticas da ER como suplementar na análise tradicional de risco de incêndio de transformadores principais da usina hidrelétrica Itaipu Binacional, e 2) a aplicação de princípios e conceitos de Segurança-II – derivada da ER – na análise da operação de quatro manobras típicas executadas pelos operadores da usina, classificadas por periodicidade e complexidade, a fim de analisar a operação normal e o impacto das variabilidades presentes quando da execução destas.

1.3 JUSTIFICATIVA

A principal justificativa para o tema proposto está associada com as constantes mudanças tecnológicas das instalações da Usina Hidrelétrica Itaipu Binacional. Avizinha-se

um processo de atualização tecnológica de todos os sistemas de controle, supervisão e monitoramento de suas 20 (vinte) unidades geradoras e das subestações sob sua responsabilidade.

Alia-se a isso uma característica da força de trabalho de O&M da organização: há, no momento, duas gerações compartilhando experiências e suplementando seus conhecimentos. Uma delas é menos afeita a mudanças tecnológicas, porém conhece a instalação desde a montagem e comissionamento. Outra é adaptada às novas tecnologias, porém possui pouca experiência sobre as peculiaridades dos equipamentos e instalações.

Do ponto de vista empresarial, a Itaipu Binacional é internacionalmente reconhecida como líder de produção de energia e sustentabilidade. Na sua visão organizacional

> "até 2020, (...) se consolidará como a geradora de energia limpa e renovável com o melhor desempenho operativo e as melhores práticas de sustentabilidade do mundo, impulsionando o desenvolvimento sustentável e a integração regional" (ITAIPU BINACIONAL, 2016b).

Adotar práticas de resiliência para delinear a segurança operacional de seus ativos vai ao encontro dessa visão de produção sustentável e alto desempenho operativo, balanceando adequadamente o *trade-off* entre produção e segurança.

1.4 MÉTODO

A dissertação é composta de dois artigos principais; os métodos de pesquisa específicos de cada um estão detalhados no próprio corpo do texto dos artigos. No entanto, muitos aspectos são comuns: por conta do envolvimento do pesquisador (que atuou como operador indireto) com o tema e com as pessoas investigadas (todos fazem parte da equipe de técnicos, engenheiros e gerentes da operação da Itaipu Binacional) ambas as pesquisas que dão base a essa dissertação são caracterizadas como aplicadas, participantes, qualitativas e exploratórias.

O primeiro artigo aborda o plano de Ação de Emergência em Caso de Incêndio em Transformador da Unidade Geradora, que dentre o Plano de Ação de Emergências (PAE) da Itaipu Binacional (um conjunto de procedimentos estabelecidos para eventuais contingências críticas) é o plano mais estabelecido e de maior frequência em simulados. Isso favorece que

os operadores tenham opiniões mais consolidadas a respeito do plano e, portanto, os indicadores produzidos com base em tais opiniões sejam mais robustos. Para a consecução dos objetivos do primeiro artigo, foi feita uma revisão da literatura quanto aos requisitos, princípios e temas da ER e de Segurança-II que pudessem suplementar a análise de risco tradicional que utiliza requisitos de confiabilidade de componentes, equipamentos e sistemas. A ER aborda proativamente "o que dá certo" no sistema sociotécnico, sendo uma alternativa às abordagens tradicionais reativas que estudam "o que deu errado". Esta suplementação teve também como base as opiniões da equipe de operadores da Itaipu Binacional, organizada pela ferramenta *Design* Macroergonômico (DM) (FOGLIATTO; GUIMARÃES, 1999), que é detalhada no próprio artigo. As entrevistas com os grupos de operadores, observadores e gerentes foram decupadas, verificada sua aderência às quatro habilidades de um sistema resiliente [15], e categorizadas em "Fatores de resiliência" para formar indicadores aderentes aos princípios de ER. O DM auxiliou na formação destes indicadores de resiliência que servem como fatores amplificadores da probabilidade de falha tradicional do componente ou sistema que sofre o impacto. Desta forma, esses elementos aderentes à ER atuam como uma suplementação da análise de risco tradicional. Finalmente, é delineada uma árvore de falhas e de eventos (método "gravata borboleta") da contingência crítica, agregando os indicadores de resiliência aos elementos tradicionais de risco.

O segundo artigo trata do estudo de quatro manobras operacionais realizadas pela equipe de operadores da Itaipu Binacional e das variabilidades que incidem na operação normal, Inspirado no Método de Análise de Ressonância Funcional (*Functional Resonance Analysis Method* – FRAM), que reflete o pensamento de Segurança-II e da ER [13], avaliou também o impacto destas variabilidades nos quatro casos de falha ocorridos entre 2006 e 2015, O foco do FRAM é a natureza das atividades diárias com o objetivo de construir um modelo de como o sistema sociotécnico funciona, em vez de investigar, dentro de um modelo reativo predefinido, como um acidente ocorreu. Dentre as mais de quinhentas manobras realizadas pela operação da Itaipu Binacional, foram escolhidas quatro, por meio de entrevistas com os operadores e supervisores, e pesquisa no banco de dados interno de ocorrências. Estas quatro manobras são representativas dos quatro quadrantes de uma matriz de "complexidade" de manobra alta e baixa e "periodicidade" – ou "frequência" alta e baixa. A partir da eleição das manobras, foram feitas interações com os profissionais (em entrevistas e acompanhando as manobras) para identificar as variabilidades que afetam cada passo de cada uma das manobras contempladas no estudo e que de fato incidem na operação normal e

que podem afetar o resultado global da manobra. Entrevistas *in loco* também foram conduzidas, com o pesquisador acompanhando as manobras de rotina.

1.5 ESTRUTURA DO TRABALHO

Este trabalho está organizado em três capítulos além desta introdução ao tema, que justificou a importância de se abordar a segurança de instalações críticas, em especial a Usina Hidrelétrica Itaipu Binacional, sob os preceitos de Engenharia de Resiliência e Segurança-II. Este primeiro capítulo também apresentou os objetivos, o método de trabalho, a estrutura e as limitações do estudo.

O segundo capítulo apresenta o artigo contendo o estudo de caso da aplicação de princípios, conceitos e heurísticas da Engenharia de Resiliência a fim de suplementar a análise de risco de Incêndio de Transformadores Principais da Usina Hidrelétrica Itaipu Binacional. Para isso, estuda o *status* acadêmico atual da análise de risco que incorpora elementos de ER, propõe a formação de fatores e indicadores aderentes a ER, aplicando-os às árvores de falhas e de eventos desta ocorrência, baseada no método “gravata borboleta”.

O terceiro capítulo apresenta o segundo artigo que compõe essa dissertação. Neste, são aplicados princípios e conceitos de Segurança-II (que “focam o sucesso”) à operação da Usina Hidrelétrica Itaipu Binacional para o caso específico de quatro manobras típicas executadas pelos operadores da usina e subestações. Para isso, foram estudados os métodos disponíveis para a abordagem de Segurança-II, determinadas as variabilidades que incidem na operação normal e analisadas retroativamente as falhas já ocorridas para verificar a aderência do estudo.

O quarto capítulo apresenta as conclusões obtidas a partir do trabalho desenvolvido, esclarecendo as limitações da pesquisa. Também são feitas considerações que podem servir de sugestões para estudos futuros neste mesmo tema.

1.6 DELIMITAÇÕES DO TRABALHO

Conforme já abordado, aplicações práticas de ER e Segurança-II são incipientes e a literatura ainda debate os termos básicos de gestão de riscos operacionais sob essas perspectivas, tendo havido até o momento mais confusão do que clareza (AVEN, 2012). Neste contexto, não seria razoável supor que este trabalho forneça contribuições firmes nessa narrativa, sendo antes uma aplicação prática do que se tem disponível até o momento. Caso o futuro mostre novas abordagens que invalidem as aqui tratadas, exigir-se-ão adaptações.

Com relação às entrevistas, foram conduzidas somente com os executantes da operação, por serem da linha de frente do combate de acidentes e de resposta a perturbações. O estudo pode ser ampliado com a adição de opiniões estruturadas do *staff* de manutenção e da brigada de emergência.

O primeiro artigo é um estudo de caso específico da aplicação dos preceitos de ER a uma análise de risco de explosão de um transformador elevador da Itaipu Binacional; análises de risco de outros equipamentos e sistemas tão capazes de representar risco de disrupção quanto este, apesar de possíveis, não serão abordadas neste estudo.

O segundo artigo é um estudo de caso de quatro manobras operacionais representadas em quadrantes de complexidade e periodicidade e a visão de Segurança-II sobre elas. Apesar de terem sido escolhidas com base na opinião dos operadores e supervisores, é frágil afirmar que estas manobras representam o universo de mais de quinhentas manobras efetuadas pela operação da Itaipu Binacional.

2 SUPLEMENTAÇÃO DA ANÁLISE DE RISCO COM ELEMENTOS DE ENGENHARIA DE RESILIÊNCIA PARA INCÊNDIO DOS TRANSFORMADORES PRINCIPAIS DA USINA HIDRELÉTRICA ITAIPU BINACIONAL

2.1 INTRODUÇÃO

Organizações são continuamente desafiadas a manter altos níveis de produtividade sem que sejam descuidados aspectos referentes à segurança das pessoas, instalações e meio ambiente. Assim, a integridade de seus ativos, garantida através das estratégias e atividades que possuam a intenção de mantê-los disponíveis, seguros e confiáveis, deve ser uma de suas maiores preocupações [1].

Paradoxalmente, em organizações cujas consequências socioeconômicas de eventuais acidentes são elevadas, não raro o *trade-off* entre produção e segurança é relativamente pouco explorado, pois as características de seus sistemas de segurança física, normalmente sobredimensionados ou duplicados, diminuem consideravelmente a probabilidade de risco de catástrofes, sem, no entanto, diminuir o impacto socioeconômico caso barreiras não planejadas sejam rompidas ou situações imprevistas ocorram. Instalações geradoras de energia elétrica enquadram-se neste perfil de organizações de alta confiabilidade cujo risco operacional está, de alguma forma, fora de controle, o que as obrigam a constantemente revisitar sua capacidade de monitorar, antecipar e responder a eventos de risco à segurança de seus sistemas [2].

Os estudos das causas-raiz de alguns dos mais graves acidentes destas instalações (Chernobyl, 1986 [3]; Three Mile Island, 1979 [4]; Sayano-Shushenskaya, 2009[1]; Fukushima, 2011 [5]) concluíram que variáveis desconhecidas quando do projeto da instalação introduziram variabilidades que saíram do controle, levando a situações desestruturadas [6]. Na mesma linha, muitas das análises de acidentes que se têm registro apontam para causas fundamentais serem falhas humanas, em equipamentos ou a um problema técnico associado a um processo de controle [1]. Uma nova abordagem de gestão de segurança, denominada Engenharia de Resiliência (ER) surge como contraponto a esta visão reativa. A ER pondera que a gestão de segurança tradicional, denominada Segurança I, foca a manutenção de

[1] O relatório oficial do parlamento russo foi retirado do website

incidentes e acidentes no menor nível possível, considerando o número de casos de falhas sem considerar os de sucesso. Para a ER, a nova gestão, ou Segurança II, deve focar a probabilidade de sucesso sob as mais diversas circunstâncias, ou seja, considerar o que dá certo, para assegurar que o sistema sociotécnico funcione o mais acertadamente possível, tornando a gestão mais proativa do que reativa [7].

Taleb [8] manifesta sua preocupação em lidar com os eventos que nomeia "cisnes negros": imprevisíveis – nada no passado convincentemente aponta para a sua ocorrência –, causam enorme impacto e, posteriormente ao seu acontecimento, não raro conclui-se que ele não seria tão aleatório e improvável como era percebido. Por tais características, sua probabilidade é impossível de ser calculada. Avaliar a resiliência dos processos em torno das condições que podem levar a um evento destes surge como uma maneira de a sociedade lidar com tais eventos.

A segurança de uma organização resiliente não pode ser tratada somente com a adição de barreiras, procedimentos e salvaguardas. Requer monitoramento contínuo da performance do sistema e margens de desempenho que garantam um alto grau de segurança operacional com risco controlado. Resiliência, assim, é uma maneira de *lidar com a complexidade sistêmica* [9], monitorando o processo de decisão organizacional para avaliar o risco de a organização estar operando mais perto do que percebe de limites de segurança [10], complementando o gerenciamento tradicional de risco.

À Itaipu Binacional, tendo como visão organizacional ter o melhor desempenho operativo e as melhores práticas de sustentabilidade do mundo até 2020 [11], interessa adotar práticas de resiliência para delinear a segurança operacional de seus ativos.

A aproximação das disciplinas "Análise de Risco" e "Engenharia de Resiliência" conta aproximadamente uma década; uma aplicação possível para uma organização que se pretenda resiliente é a de revisar suas análises de risco tradicionais e inserir nestas os princípios e propriedades de ER, tornando a análise mais adequada aos preceitos da segurança proativa, ou Segurança-II. Neste contexto, este artigo objetiva apresentar um estudo de caso da aplicação de princípios, conceitos e heurísticas da Engenharia de Resiliência a fim de suplementar a análise de risco de Incêndio de Transformadores Principais da Usina Hidrelétrica Itaipu Binacional.

A primeira seção deste artigo apresenta uma visão global teórica do *status* acadêmico atual da disciplina ER, dos indicadores de segurança, dos princípios de resiliência e do método que será utilizado para desenvolver este estudo. A segunda seção mostra o método utilizado para levantar os princípios e temas de resiliência na avaliação do risco de incêndio

em um transformador. A terceira seção apresenta a formação dos fatores e indicadores aderentes a princípios de resiliência e baseados nas opiniões estruturadas do *staff* operacional da Itaipu Binacional, aplicando-os a uma análise de risco tradicional baseado no método "gravata borboleta" para explosão de transformador. A última seção oferece reflexões das contribuições do quadro e considerações para estudos futuros.

2.2 REFERENCIAL TEÓRICO

2.2.1 Indicadores de segurança

Uma quantidade significativa de indicadores proativos disponíveis na literatura foca na segurança ocupacional ao invés da segurança do sistema, e alguns representam somente uma lista de ameaças potenciais, como falta de treinamento de segurança, presença de instalações médicas no local, se há política normatizada para sistemas de segurança e bloqueio (cartões, cadeados, etc.); enfim, processos relacionados à promoção da segurança, mais pessoal do que patrimonial [12].

Praticamente todo o esforço acadêmico com relação a indicadores de segurança foi no sentido de desenvolver indicadores organizacionais; mesmo assim, um considerável trabalho de identificação de indicadores proativos tem sido desenvolvido nos últimos anos. Muitos destes padrões recomendam que a identificação de tais indicadores comece pela identificação do risco, mas assumem que acidentes são causados por uma cadeia linear de eventos, não considerando as interações indiretas e fatores complexos sistêmicos em tais acidentes [12].

Em vista de uma análise de risco fundada em indicadores para atender preceitos de ER, propõe-se estabelecer uma cadeia de ligação entre indicadores proativos, propostos por Leveson [12], análise de risco e resiliência dos processos, de forma que os princípios de ER estejam atendidos pelos indicadores e pelo método de análise de risco proposto.

A intenção deste trabalho vai ao encontro da linha de pensamento de verificar indicadores proativos de segurança para um risco específico e inserir neles preceitos/conceitos/princípios da ER, a exemplo do que produziu a *Electric Power and Research Institute*: uma série de indicadores gerenciais proativos de processos organizacionais relacionados à segurança a partir de seis "temas" relacionados ao desempenho e segurança organizacional, que mesmo não tendo sido identificados no relatório como temas de ER, são os mesmos utilizados pela academia como critérios de resiliência:

comprometimento da alta gerência; cultura de relatar; cultura do aprendizado; consciência situacional; prevenção; flexibilidade [13].

2.2.2 Princípios da resiliência

Dentre as definições de resiliência sob diferentes perspectivas disciplinares, optou-se como basilar para este trabalho aquela aplicada aos sistemas de gerenciamento de segurança, segundo o qual "resiliência refere-se à habilidade de uma organização de antecipar e envolver ameaças à sua existência e metas principais, recuperando-se rapidamente" [18]. A aplicação de ER é particularmente adequada a um sistema de alto risco com características complexas por causa do (a) alto grau de interconexões entre os componentes do sistema e (b) incertezas e variabilidades em tais condições de complexidade [15].

Há inequívoca relação entre os conceitos de cultura de segurança e de resiliência, para onde converge o objetivo deste trabalho: abordagens modernas de segurança não dispensam a melhoria contínua de procedimentos, o aprendizado contínuo e a consciência situacional de todos os níveis da organização para avaliação de riscos [14]. O conjunto de conceitos e princípios da ER estão ligados a processos (tais como treinamento, capacidade de resposta, capacidade de monitoramento) a serem avaliados sob cunho principalmente qualitativo [16] os quais, por mais que sejam importantes, não são os geralmente considerados nas análises de risco tradicionais, que são as utilizadas pela maioria dos técnicos e engenheiros de segurança. Além disso, indicadores quantitativos são os mais adequados para oferecer suporte à tomada de decisão [17]. Desta forma, assumindo que seria um passo muito grande para uma empresa adotar uma análise somente baseada nos princípios de ER, ignorando dados quantitativos e as formas mais tradicionais de avaliação como *checklists* e árvores de falhas uma solução proposta é adotar indicadores de risco aderentes aos princípios de ER, suplementando a análise tradicional de risco.

Exemplificando, indicadores "de resiliência" podem ser baseados em métricas vinculadas à mudança de tecnologia e aos impactos que tais mudanças causam na resiliência do sistema; caso tais métricas reflitam adequadamente o estado atual dos fatores vinculados a tais mudanças de tecnologia, é possível em um novo cenário mudar o valor da métrica para auferir o risco de determinado evento com base em tais mudanças sem que seja necessário refazer completamente a análise de risco.

Adicionalmente, uma abordagem de resiliência não deveria tratar somente dos eventos disruptivos e das probabilidades de falha de componentes que podem levar ao seu

acontecimento (do contrário, seria considerada uma análise de risco tradicional), mas também do restabelecimento do sistema após estes eventos. O aspecto dinâmico da análise de resiliência não se refere somente às condições que levaram ao evento disruptivo, mas também às ações subsequentes ao evento, supondo que ele efetivamente aconteceu – avaliação da habilidade de "responder". Uma análise de vulnerabilidade, portanto, ditaria a ação resiliente apropriada a ser tomada. Análises de vulnerabilidade em intervalos regulares são uma das chaves para conhecer os eventos disruptivos e continuamente aprender com os incidentes, um dos princípios da resiliência [17].

Com relação a princípios, métodos e heurísticas de resiliência, o fato de ser um conceito relativamente novo na academia faz com que ainda restem discordâncias e complementaridades; este trabalho deverá ainda selecionar os mais aplicáveis, e onde, na análise de risco proposta. As definições podem ser encontradas nos trabalhos referenciados. A revisão da literatura mostra que, apesar de não haver unanimidade entre as diferentes terminologias ligadas à ER [15], Hollnagel propôs as habilidades que um sistema deve aprimorar/manter para se considerar resiliente: *Responder* a ameaças regulares e irregulares de uma maneira robusta e, ao mesmo tempo, flexível; *Monitorar* o que pode ser ou vir a ser uma ameaça, incluindo seu próprio desempenho; *Antecipar* riscos (e eventos de risco) e oportunidades; *Aprender* pela experiência – tanto com o sucesso quanto com o fracasso [16], [19]–[21]. Estudos subsequentes convergem para definir estas habilidades como as principais (ou os quatro princípios básicos) que definem a resiliência de sistemas. Embora tais habilidades não estabeleçam sozinhas as métricas para medir a resiliência, servem de base para que, com o conhecimento do processo, o analista extraia dos elementos de risco ou das barreiras de segurança em quais elementos tais princípios são aplicáveis.

2.2.3 Método da gravata borboleta

A explicação detalhada de como uma abordagem gravata borboleta (GB) é aplicada em um contexto de risco foi encontrada em diversos ensaios; o aqui demonstrado é uma compilação destes [22]–[27].

A GB é uma ferramenta gráfica para ilustrar um cenário de acidente e que contempla praticamente todo o "ciclo de vida" de uma ameaça, desde os eventos primários que lhe dão origem até as consequências; no lado esquerdo, uma árvore de falhas identifica os possíveis eventos que causam o evento crítico; o centro mostra o ponto no qual o controle foi perdido, o perigo está prestes a se confirmar e medidas de mitigação e recuperação são necessárias; do

lado direito, as possíveis consequências do evento crítico baseado no desempenho das barreiras de segurança [26]. A Figura 1 mostra a representação gráfica do modelo.

Figura 1 Modelo gravata borboleta

Sistemas de prevenção são encontrados no lado da árvore de falhas, e sistemas de mitigação são encontrados no lado da árvore de eventos [22].

O método GB ajuda a revisar o perfil do acidente assim que nova informação relevante fica disponível para qualquer parte do modelo, causando a atualização do perfil de risco [26], especialmente necessário quando os parâmetros pouco mutáveis de resiliência forem inseridos na análise; um exemplo é a mudança tecnológica de um determinado processo, que pode não alterar significativamente os elementos estáticos das árvores mas influenciam muito nos princípios de resiliência aplicados no modelo (conhecimento, preparação, treinamento, etc.).

A importância das barreiras para o nível de segurança foi estudada por diversos autores, resumidos em [28]. A análise das barreiras é utilizada pelos elementos críticos de segurança, e indicadores de desempenho foram desenvolvidos para ilustrar o desempenho da barreira através de medidas quantificáveis [1].

Indicadores reativos podem, portanto, ser vistos como falhas nas medidas de recuperação ou as consequências imediatas, ou seja, falhas no lado direito da GB. Indicadores proativos, por sua vez, estarão localizados no lado esquerdo, antes do sistema atingir o evento de topo. A análise avança se forem adicionados fatores escalonáveis às barreiras, trazidos por análises não diretamente relacionadas ao risco [29]. Um exemplo seria uma barreira preventiva “conhecimento adequado dos operadores” que sofreria a influência de “baixo orçamento para treinamento”. Desta maneira, além de definir um indicador proativo, podem ser inseridos elementos que à primeira vista seriam estranhos à avaliação de risco; os princípios e indicadores de ER poderiam ser estes fatores escalonáveis.

Do ponto de vista da ER, o lado esquerdo fornece elementos do que “ainda não aconteceu”, avaliando as capacidades de *adaptação* e de *absorção* do processo e as

habilidades de *monitorar*, *aprender* e *antecipar*. O lado direito, por sua vez, fornece elementos para se medir capacidades de *absorção* e de *recuperação* e as habilidades de *responder* e *aprender*.

Desta forma, a resiliência suplementa o processo de avaliação de risco, na proporção que será definida a partir da metodologia a ser aplicada neste estudo. A este trabalho interessa mais evidenciar o método para a inserção de princípios de ER a uma análise de risco do que detalhá-la, por isso tanto a árvore de falhas quanto a árvore de eventos serão representadas de forma simplificada.

2.3 MÉTODO

A avaliação dos requisitos, princípios e temas da resiliência dispostos anteriormente para adequá-los ao estudo de caso pressupõe o uso de elementos subjetivos juntamente com os eminentemente técnicos para a avaliação de risco suplementar que os incorpora. A análise de risco tradicional utiliza requisitos de confiabilidade de componentes, equipamentos e sistemas. A análise suplementada com elementos de ER adicionará elementos baseados nas opiniões e percepções de vários níveis de interessados.

Outros trabalhos [30] já fizeram uso destes elementos com vistas à avaliação de processos sob a perspectiva da ER em empresas do setor elétrico. Segundo tal referência, o contexto organizacional e a capacitação dos indivíduos são requisitos fundamentais sob a perspectiva da ER.

O Plano de ações de Emergências da Itaipu Binacional é um conjunto de procedimentos estabelecidos para eventuais contingências consideradas críticas na usina. Tem o objetivo de minimizar os impactos de tais contingências ao abordar de forma sistematizada os procedimentos da Brigada de Emergência, Operação da Usina e Segurança Empresarial. Pressupõe a realização de treinamentos e simulados periódicos para as contingências críticas. Dentre estes planos, o mais completo é o deste estudo de caso – Incêndio em Transformador da Unidade Geradora, tendo em vista o potencial de danos às instalações, pessoas e/ou meio ambiente no caso de um sinistro. Por ser o plano mais completo, permite que funcionários da operação não envolvidos diretamente com a atividade possam opinar, de forma qualitativa, sobre um processo amadurecido. Estes funcionários não executam os procedimentos do PAE nem as manobras, e atuam nas atividades de pré e pós operação (estatística, normas, suporte técnico...). Neste estudo, eles serão denominados “operadores indiretos”.

A ferramenta utilizada para levantar os requisitos de ER aplicados ao estudo de caso foi o *Design* Macroergonômico [31] que promove "a participação de trabalhadores de diferentes setores da empresa, explicitando interações existentes entre estes profissionais". Considerou-se que o caráter participativo da macroergonomia é aderente aos princípios da ER na medida em que procura entender as demandas dos profissionais para que os sistemas sejam mais eficientes e seguros, refletindo a capacidade atual das habilidades de "monitorar", "antecipar", "responder" e "aprender" da organização por meio de quem efetivamente é responsável pelas ações que refletem as habilidades.

Por promover o processo participativo, algumas das etapas de aquisição de conhecimento do estudo macroergonômico foram escolhidas para nortear as ações estruturantes [31]:

(i) Identificação do usuário e coleta organizada de informações;

(ii) Priorização dos itens de demanda identificados pelo usuário, levando em consideração o conjunto de dados amostrais (frequências, ordem em que o item é mencionado, peso da opinião conforme a categorização do grupo ao qual o entrevistado faz parte);

(iii) Incorporação da opinião de especialista com vistas à correção de distorções apresentadas no *ranking* obtido em (ii), bem como a incorporação de itens pertinentes de demanda ergonômica não identificados pelo usuário.

O processo participativo visa obter, de maneira estruturada, as principais preocupações dos *stakeholders* do processo (no caso, supervisores e operadores executores do Plano de ações de Emergências, gerentes e operadores indiretos), identificar com base nestas preocupações os temas/princípios de ER citados pelos *stakeholders*, ranqueá-los e inseri-los na análise de risco. O pesquisador autor desta dissertação, que é um dos operadores indiretos deste estudo de caso, assumiu o papel do "especialista".

Os itens são levantados por meio de entrevistas não estruturadas e espontâneas, nas quais os indivíduos são instigados a discorrer livremente sobre "forças, fraquezas, ameaças e oportunidades no processo de combate às causas e consequências de incêndio em um dos transformadores principais". A amostra é de 65 (sessenta e cinco) funcionários, estratificados em operadores (41), supervisores (12), operadores indiretos (10) e gerentes (2). Por causa dos trabalhos em turno de revezamento, as entrevistas com os operadores foram conduzidas em grupo, nos próprios turnos. As entrevistas com os operadores indiretos, e gerentes, individuais. Com os supervisores, individuais para os que não participam do turno de operação, em conjunto com o grupo de operadores quando participam. Todas foram gravadas e decupadas, dando origem, assim, a um banco de dados com todas as citações dos

profissionais. De acordo com o *Design* Macroergonômico, as repetições – mais de um profissional cita a mesma preocupação – e a ordem na qual a preocupação é citada importam para a formação do(s) indicador(es).

Para entender se as citações são aderentes às habilidades de resiliência [15], após decupadas, para cada uma delas é verificada sua aderência às quatro habilidades de um sistema resiliente. Responder; Monitorar; Antecipar; Aprender. Assim, é criado um "índice de aderência" das citações às habilidades de um sistema resiliente. Ao mesmo tempo, as citações são categorizadas em "Fatores de resiliência" de forma a facilitar a formação de: a) um indicador aderente aos princípios de ER; ou b) uma solicitação de plano de ações vinculado à preocupação dos profissionais. Como vários profissionais citam as mesmas inquietudes com palavras diferentes, a categorização é necessária para avaliar a repetitividade e o ranqueamento destas.

À medida que as citações vão sendo agrupadas em fatores de resiliência, o método DM prevê que seja aplicado um peso inversamente proporcional à ordem da citação, de forma que à n-ésima citação seja aplicado um peso $1/p$, assim cada fator de resiliência segue a fórmula

$$Fr = \sum_{i=1}^{p} \frac{1}{p}, \quad (1)$$

onde *p* é o peso de cada uma das citações do mesmo fator e *Fr* o somatório destes.

No entanto, como há diferença significativa na quantidade de profissionais em cada categoria (exemplo: 41 operadores e 2 gerentes), depois de calculados os fatores é necessário normalizá-los a fim de equilibrar o fator para cada uma das quatro diferentes categorias.

Com base no somatório de todos os *Fr*, é feito um ranqueamento dos fatores de resiliência para priorização de planos de ação ou indicadores.

A formação dos pesos, portanto, possui a finalidade de:

a) Caso sejam propostas ações, ranqueá-las de acordo com a prioridade;
b) Caso seja proposto um indicador Ir_n, este indicador servirá como um fator amplificador da probabilidade de falha tradicional do componente ou sistema que sofre o impacto, de forma a quanto maior o peso p_n do item de resiliência, maior o impacto no indicador tradicional, segundo a fórmula

$$R_n = {Ir_n}^{p_n} \quad (2)$$

Onde R_n é o indicador de resiliência relativo ao índice Ir_n elevado ao peso p_n da citação devidamente categorizada conforme o DM. Como o indicador Ir_n é sempre menor que 1 (pois índice medido em valor percentual), um peso maior do fator de resiliência, que

representa uma maior preocupação dos profissionais, desfavorece o indicador. A formação dos índices Ir_n não faz parte do escopo deste trabalho.

A maneira proposta de se adicionar o peso do fator de resiliência à análise de risco convencional é "penalizar" o componente cujo cálculo da probabilidade de falha é tradicional com o indicador de resiliência; como este último sempre terá valor menor que 1 (pior quanto mais fraca a habilidade resiliente do sistema), a probabilidade de falha do componente é "agravada" ao dividi-la pelo indicador R_n.

A partir da priorização dos elementos e da correspondência destes com os princípios/temas de ER verificados na revisão bibliográfica, será delineada a "gravata borboleta" da contingência crítica com a inserção dos elementos de ER levantados e a demonstração dos exemplos matemáticos para validação do método.

O envolvimento do pesquisador com o tema e com as pessoas investigadas (todos fazem parte da equipe de operadores, engenheiros e gerentes da operação da Itaipu Binacional) caracteriza uma pesquisa participante, aplicada e exploratória.

2.4 RESULTADOS E DISCUSSÃO

2.4.1 O Plano de Ações de Emergência

O Plano de Ações de Emergência (PAE) de "Incêndio em Transformador Principal dos Geradores" é um conjunto de procedimentos estabelecidos para eventuais casos de incêndio nos transformadores elevadores das unidades geradoras, localizados em ambiente confinado (galeria de transformadores da casa de força da Itaipu Binacional) e considerados de importância crítica para a segurança físico-operacional da Usina Hidrelétrica Itaipu.

O PAE estrutura as ações a serem tomadas pelas equipes de Operação da Usina, Bombeiros, Segurança Empresarial e Brigada de Emergência para o combate às consequências de um eventual incêndio. Prevê a atuação das equipes de Operação da Usina na comunicação do sinistro a diversos órgãos, confirmação das atuações das linhas de ação automáticas de combate ao incêndio (extinção por água nebulizada), manobras de aplicação dos sistemas manuais (sistema suplementar de água para rescaldo, sistema de CO_2) e isolação elétrica dos painéis envolvidos.

Periodicamente, o PAE prevê a realização de simulados de incêndio no qual participam todas as equipes envolvidas e, ao final de cada, é realizado um *brainstorm* para avaliação SWOT dos resultados. Por se tratar do processo de mitigação das consequências do

evento, no qual a operação está mais diretamente envolvida, o material colhido nas entrevistas teve relação com as forças e fraquezas, oportunidades e ameaças do PAE.

2.4.2 Formação dos requisitos de ER

Com base no que foi apresentado no capítulo 2.2 – "Referencial Teórico", a Tabela 1 apresenta uma compilação dos princípios e temas de ER para que seja verificada a aderência dos fatores colhidos nas entrevistas a estes.

Tabela 1 Resumo de princípios e temas de ER

Referências que citam o princípio de ER:	***Princípio que avalie a capacidade de o sistema:***	***Descrição resumida***
[21], [18], [19], [20], [16], [32]	**Antecipar**	Qual a capacidade de prevenir-se, envolvendo ameaças potenciais, riscos, eventos de risco e oportunidades
[21], [18], [19], [20], [16], [32]	**Responder**	A ameaças regulares e irregulares, de maneira rápida, com excelente comunicação e mobilização otimizada de recursos
[21], [19], [15], [20], [16], [17], [33], [32], [28]	**Monitorar**	Em tempo real, o que pode ser ou vir a ser uma ameaça. Conhecer "o que está acontecendo" e ter e visão sistêmica. "Consciência situacional", neste contexto, será considerado também como "monitorar".
[21], [19], [15], [17], [20], [16], [33], [32]	**Aprender**	Tanto com o sucesso quanto com o fracasso

2.4.3 Percepções colhidas nas entrevistas e aderência aos princípios de resiliência

Os profissionais da Operação da Usina ouvidos nas entrevistas foram instados a falar livremente sobre o tema "forças, fraquezas, ameaças e oportunidades no processo de combate às causas e consequências de incêndio em um dos transformadores principais". Um banco de dados com 189 (cento e oitenta e nove) citações foi formado e, para cada citação, sua aderência aos princípios de resiliência (constantes da Tabela 1) foi verificada.

Ainda, os grupos entrevistados foram categorizados de acordo com suas responsabilidades no processo, transcritos na Tabela 2.

Tabela 2 Categorização de profissionais ouvidos nas entrevistas

Categoria	**Número de profissionais**	**Descrição**
Operador	41	Executor das manobras; confirma o incêndio, executa aplicações manuais de combate, interage com bombeiro e chefe da Brigada de Emergência, realiza isolações elétricas.
Supervisor	12	Supervisor da operação, comanda ações de combate
Observador	10	Não possui envolvimento direto com a ocorrência, mas é capaz de fornecer uma análise crítica das forças, fraquezas, oportunidades e ameaças. Pode participar da formação do PAE.
Gerente	2	Responsáveis pela condução do processo.

Posteriormente, as citações foram categorizadas em “Fatores de resiliência” de forma a facilitar a formação de: a) um indicador aderente aos princípios de ER; ou b) uma solicitação de plano de ações vinculado à preocupação dos profissionais. Como vários profissionais citam as mesmas inquietudes com palavras diferentes, a categorização é necessária para avaliar a repetitividade e o ranqueamento destas.

O banco de dados tem o formato exemplo das quatro citações transcritas na Tabela 3. Ela também ajuda a verificar se cada citação é aderente às habilidades de resiliência: Responder; Monitorar; Antecipar; Aprender. Um exemplo: a citação “Subir e descer escadas várias vezes com o cilindro da máscara autônoma nas costas: os operadores possuem capacidade física para isso?” afeta as habilidades de *Antecipar* – afinal, a situação está sendo levantada antes de ser um problema real – e *Responder* – uma vez que a capacidade física do operador pode influenciar a capacidade resiliente da organização em responder adequadamente a um eventual sinistro. Esta citação, por outro lado, pouco ou nada diz a respeito da habilidade de *Monitorar* ou *Aprender*.

Tabela 3 Exemplo do tratamento das citações e formação do banco de dados

Cargo	**Transcrição da fala**	**"Fator de resiliência"**	**Aderência aos princípios de ER:**
Observador	“As equipes de operação e bombeiros usam nomenclaturas diferentes para a localização dos equipamentos na planta”	**Comunicação entre bombeiros / operação / brigada**	Antecipar Responder Aprender
Operador	“Subir e descer escadas várias vezes com o cilindro da máscara autônoma nas costas: os operadores possuem capacidade física para isso?”	**Preparação física do operador**	Antecipar Responder
Gerente	“Houve muita renovação de pessoal, precisamos garantir que todos conheçam detalhadamente todos os planos, principalmente este, o mais importante de todos”	**Renovação do pessoal de execução**	Antecipar Responder Aprender
Supervisor	“Caso aconteça um sinistro desta natureza, temos de mandar 4 operadores para cumprir os objetivos do PAE e ainda tratar da perturbação que certamente ocorrerá. Me preocupam os recursos humanos disponíveis”	**Disponibilidade de recursos humanos da operação**	Antecipar Responder

Assim, é criado um “índice de aderência” das citações às habilidades de um sistema resiliente. Ao mesmo tempo, as citações são categorizadas em “Fatores de resiliência” de forma a facilitar a formação de: a) um indicador aderente aos princípios de ER; ou b) uma solicitação de plano de ações vinculado à preocupação dos profissionais. Como vários profissionais citam as mesmas inquietudes com palavras diferentes, a categorização é necessária para avaliar a repetitividade e o ranqueamento destas.

A habilidade de *Antecipar* foi considerada aderente a 91% das citações; a de *Responder*, a 92%; a de *Monitorar*, a 6%; a de *Aprender*, a 51%. Não é surpresa que profissionais da operação estejam, no caso específico deste sinistro, mais preocupados com as ações pós-evento, já que são eles os responsáveis pelas primeiras ações em caso de sinistro.

Note-se que 100% das citações são aderentes a pelo menos uma das habilidades de um sistema resiliente.

2.4.4 Repetições e pesos aplicados aos Fatores de Resiliência

A categorização em "fatores de resiliência" permitiu que se avaliassem as repetições; a Tabela 4 mostra um exemplo de como elas se processaram. Em diferentes palavras, porém com o mesmo intuito.

Tabela 4 Exemplos de repetições dos fatores de resiliência por cargo

Fator de resiliência	Observador	Gerente	Operador	Supervisor	Total de repetições
Comunicação entre bombeiros/operação/brigada	5	0	1	7	**13**
Segurança do operador na execução das manobras	5	2	11	7	**25**

A tabela mostra que, por exemplo, a "Segurança do operador na execução das manobras" foi citada 7 vezes pelos supervisores, 5 pelos observadores, 2 pelos gerentes e 11 pelos próprios operadores. Ainda, como previsto no método, a cada citação é aplicado um peso inversamente proporcional à ordem, de forma que à n-ésima citação fosse aplicado um peso $1/p$, de forma que o peso final de cada fator de resiliência seguiria a fórmula (3).

Depois de formado o somatório dos fatores, foram considerados no estudo somente os principais fatores de cada especialidade, e para avançar no estudo todos os que resultaram em números maiores do que 0,5 (exceto para a categoria "Gerente", onde foram considerados os fatores maiores que 0,25; como foram entrevistados dois gerentes, o fator é naturalmente menor que nos outros casos).

O método ainda prevê que a quantidade de profissionais que participaram das entrevistas é muito diferente de especialidade para especialidade, havendo diferença significativa na somatória dos fatores *Fr*, portanto houve a necessidade de trazê-los para a mesma base; assim, a coluna ao lado dos *Fr* relaciona o *Fr* de cada fator de resiliência ao máximo de cada especialidade. O peso final de cada fator é o somatório destas relações. A Tabela 5 mostra a formação destes pesos com base no que foi obtido do banco de dados.

Tabela 5 Pesos dos fatores de resiliência

Fator de resiliência	Observador		Gerente		Operador		Supervisor		Peso final
	Fr	$\frac{Fr_{esp}}{máx(Fr_{esp})}$	*Fr*	$\frac{Fr_{ger}}{máx(Fr_{ger})}$	*Fr*	$\frac{Fr_{ope}}{máx(Fr_{ope})}$	*Fr*	$\frac{Fr_{sup}}{máx(Fr_{sup})}$	$\sum \frac{Fr}{máx(Fr)}$
Segurança do operador na execução das manobras	2,71	1			4,29	0,50	4,09	1	**2,50**
Acesso aos equipamentos de manobra próximos ao sinistrado	1,39	0,51			8,63	1	1,03	0,25	**1,77**
Integridade física dos sistemas de combate e instalações adjacentes ao sinistro	2,54	0,94			2,40	0,28	0,83	0,20	**1,42**
Indicador de monitoramento de risco operacional			1,75	1,00					**1,00**
Participação da operação no simulado de incêndio	1,19	0,44	0,33	0,19	2,57	0,30			**0,92**
Dispersão da fumaça nas instalações	1,95	0,72			1,26	0,15			**0,87**
Periodicidade e ações de melhoria das reuniões do PAE			1,46	0,83					**0,83**
Influência do fator humano					0,89	0,10	2,76	0,67	**0,78**
Conhecimento dos procedimentos operacionais	1,46	0,54	0,25	0,14	0,73	0,08			**0,77**
Preparação física do operador	1,50	0,55			1,18	0,14			**0,69**
Cobertura da comunicação via Telefonia Móvel Restrita					2,95	0,34	1,23	0,30	**0,64**
Disponibilidade de recursos humanos da operação							2,17	0,53	**0,53**
Renovação do pessoal de execução	1,25	0,46							**0,46**
Comunicação entre bombeiros/operação/brigada	0,82	0,30			1,00	0,12			**0,42**
Adequação dos procedimentos operacionais do PAE							0,50	0,12	**0,12**

Na sequência, ainda seria necessário relacionar os fatores de resiliência (cuja Tabela 5 apontou quais seriam as maiores preocupações do ponto de vista operacional) com indicadores e/ou planos de ação vinculados a eles. A Tabela 6 traz as propostas para a formação destes indicadores/planos de ação.

Tabela 6 Ações e indicadores de resiliência propostos

Rn	*FATOR DE RESILIÊNCIA*	*PESO (p_n)*	*AÇÃO PROPOSTA*	*Id*	*AÇÃO/ INDICADOR*
1	Segurança do operador na execução das manobras	2,50	Solicitar laudo técnico à engenharia para resposta a pontos de preocupação de segurança	*Ir1*	Ação
2	Acesso aos equipamentos de manobra próximos ao sinistrado	1,77	Levantar pontos necessários para execução remota de manobras, e monitorar o percentual de disponibilidade destes	*Ir2*	Indicador/Ação
3	Integridade física dos sistemas de combate e instalações adjacentes ao sinistro	1,42	Divulgação do laudo técnico de consequências de *blast* e fogo	*Ir3*	Ação
4	Indicador de monitoramento de risco operacional	1,00	Indicador de capacidade de monitoramento da sala de controle central a riscos que podem eventualmente causar a explosão do transformador	*Ir4*	Indicador
5	Participação da operação no simulado de incêndio	0,92	Índice e frequência de participação dos operadores em simulados, participação nas reuniões de *feedback* do PAE	*Ir5*	Indicador/Ação
6	Dispersão da fumaça nas instalações	0,87	Solicitar estudo de dispersão de fumaça e fogo à engenharia	*Ir6*	Ação
7	Periodicidade e ações de melhoria das reuniões do PAE	0,83	Percentual de oportunidades de melhoria discutidas/resolvidas e monitoramento das propostas pela operação	*Ir7*	Indicador/Ação
8	Influência do fator humano	0,78	Solicitar ao gerenciamento do PAE incluir situações imprevistas nos treinamentos e simulações	*Ir8*	Ação
9	Conhecimento dos procedimentos operacionais	0,77	Índice de conhecimento operacional dos procedimentos do PAE	*Ir9*	Indicador
10	Preparação física do operador	0,69	Índice de capacidade física da operação; participação no plano de capacitação física	*Ir10*	Indicador/Ação
11	Cobertura da comunicação via Telefonia Móvel Restrita	0,64	Índice de cobertura do sinal de telefonia móvel restrita na Casa de Força	*Ir11*	Indicador
12	Disponibilidade de recursos humanos da operação	0,53	Reunião entre PAE e operação para verificar possibilidade de otimizar recursos da operação	*Ir12*	Ação
13	Renovação do pessoal de execução	0,46	Índice de treinamento dos operadores novos em simulados	*Ir13*	Indicador
14	Comunicação entre bombeiros/operação/brigada	0,42	Índice de treinamento dos bombeiros em assuntos de operação; realização do curso de operação a bombeiros	*Ir14*	Indicador/Ação
15	Adequação dos procedimentos operacionais do PAE	0,12	Solicitar ao PAE maior participação da operação nas reuniões de feedback dos simulados	*Ir15*	Ação

A formação dos pesos, portanto, possui a finalidade de:

c) Caso sejam propostas ações, ranqueá-las de acordo com a prioridade;

d) Caso seja proposto um indicador Ir_n, servir como um fator amplificador, de forma a quanto maior o peso p_n do item de resiliência, maior o impacto no indicador, segundo a fórmula

$$R_n = Ir_n^{\,p_n} \quad (4)$$

Onde R_n é o indicador de resiliência relativo ao índice Ir_n elevado ao peso p_n da Tabela 6. Como o indicador Ir_n é sempre menor do que 1 (pois índice medido em valor percentual), um peso maior do fator de resiliência, que representa uma maior preocupação dos profissionais, desfavorece o indicador. A formação dos índices Ir_n não faz parte do escopo deste trabalho; um exemplo seria um indicador Ir_5 - *Participação da operação no simulado de incêndio*, que indica o número de operadores que efetivamente participou do simulado e a

frequência de participação. Um indicador hipotético de 90% diria que a cada 10 operadores, 1 ainda não participou de nenhum simulado ou há muito tempo (a ser estipulado) não participa.

2.4.5 Aplicações dos fatores de resiliência às árvores de falhas e de eventos

Reiterando que o foco deste trabalho não é mostrar as probabilidades de falha/sucesso tampouco os cálculos detalhados das árvores de falhas e eventos vinculadas à "gravata borboleta", pois interessa menos no momento a abordagem completa da análise de risco do que a apresentação um método para a inserção dos princípios de ER em uma análise de risco, um exemplo de aplicação pode ser verificado na árvore de falhas simplificada da explosão do transformador, vista na Figura 2.

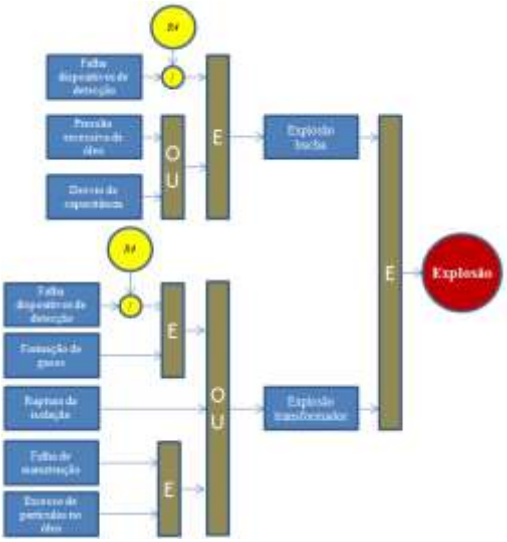

Figura 2 Árvore de falhas simplificada para explosão de transformador

A probabilidade do evento de falha "Falha dispositivos de detecção", comumente utilizado em árvores de falha convencionais, é dividido pelo indicador de resiliência R_4, que representa a capacidade da sala de controle em detectar variações que podem em curto prazo levar à explosão do transformador. Hipoteticamente, caso o indicador da capacidade de monitoramento da sala de controle Ir_4 fosse igual a 90%, o valor de R_4 também seria 90% pois em $R_n = {Ir_n}^{p_n}$ (2) o peso p_4 é igual a 1. A probabilidade de falha na detecção, portanto, seria agravada na proporção de 0,9, já que o resultado da divisão $\frac{P_{falha}}{R_4}$ é maior do que P_{falha}. Assumindo, por exemplo, que a probabilidade de falha seja de **5%**, o indicador "agravado" seria de 5/0,9 = **5,6%**. Extrapolando para outros casos, quanto maior o peso p_n maior é o impacto negativo no indicador R_n e, portanto, quanto menor este fator, maior é o impacto na probabilidade de falha do evento em que ele estiver "conjugado". E quanto mais se aproxima

de zero o peso p_n, menor sua influência em Ir_n pois o valor de R_n se aproxima de 1 e a probabilidade de falha não é alterada pelo indicador de resiliência. O que indica que, quanto menor o peso p_n (significando que o fator importa menos para a organização), menos importa o indicador de resiliência para a probabilidade de falha.

Da análise, a árvore de falhas apresentaria somente este indicador R_4 de resiliência; uma vez que os entrevistados neste trabalho foram os profissionais da operação, e que a operação se vê no momento significativamente mais ligada a ações de mitigação do que de prevenção, a maior parte dos indicadores de resiliência é ligada à árvore de eventos da "gravata borboleta", o que aponta a oportunidade de melhoria para o desenvolvimento de indicadores proativos para a análise de risco.

A árvore de eventos apresentada na Figura 3 tem a intenção de demonstrar a aplicação do método. O pouco detalhamento em ramos da árvore faz com que haja mais de um fator de resiliência para cada ação operacional. Na análise de risco completa, devem ser detalhados todos os ramos e calculadas as probabilidades, fazendo com que seja mínima a conjugação de mais um indicador de resiliência R_n para cada ramo da árvore de eventos.

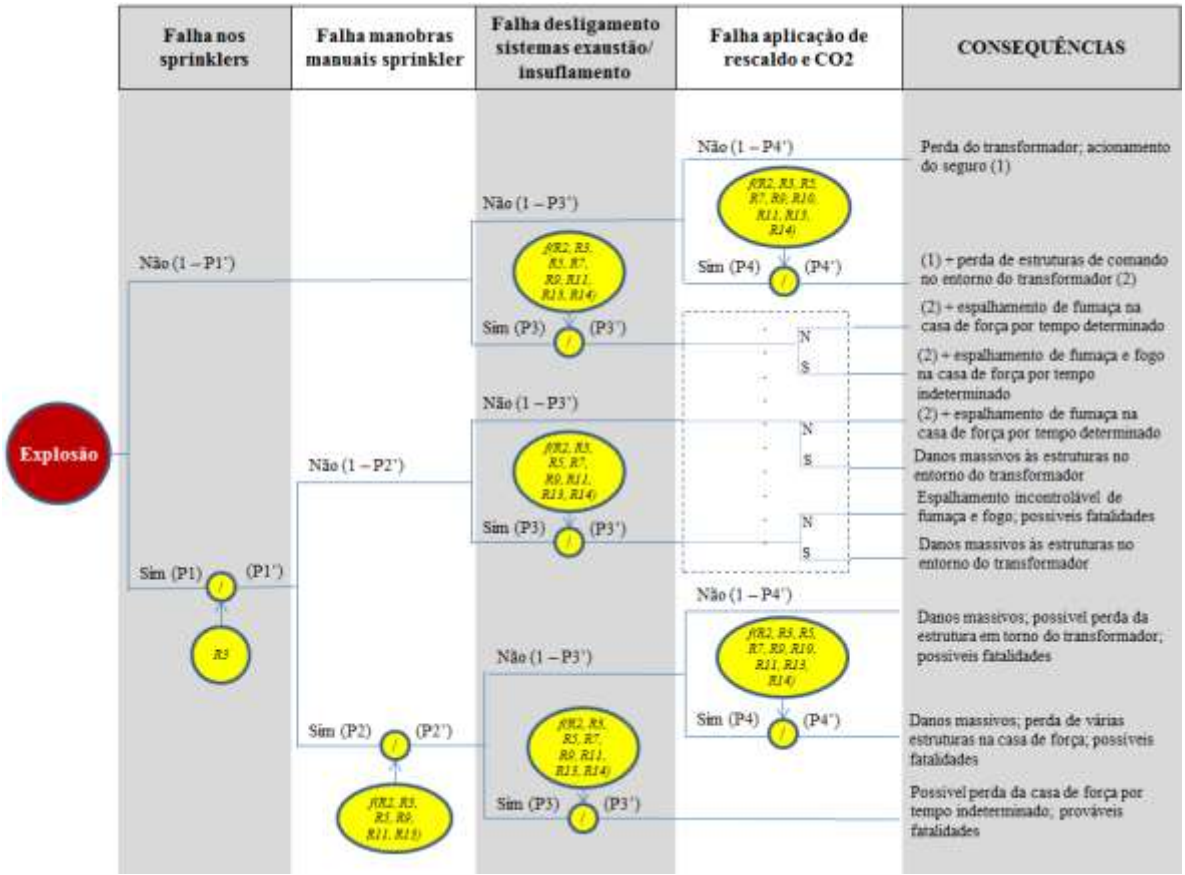

Figura 3 Árvore de eventos simplificada para explosão do transformador

Entretanto, de fato pode ocorrer que em uma simples ação do operador esteja envolvido mais de um indicador de resiliência R_n. Nas manobras manuais do sistema *sprinkler*, por exemplo, estão envolvidos pelo menos seis indicadores: R_2, R_3, R_5, R_9, R_{12} *e* R_{13}. A forma de se trabalhar matematicamente com tais indicadores para torná-los um único que represente o grupo de indicadores Ir_n e os pesos p_n está disposta na equação

$$R_t = \frac{\sum {Ir_n}^{p_n}}{\sum p_n} \quad (3)$$

Esta fórmula garante que ao maior peso p_n será conferido o maior impacto no indicador R_t. Como forma de demonstrar tal solução, utilizaram-se como exemplo um hipotético ramo da árvore de eventos que conjugaria os fatores R_1, R_{11} e R_{15} da Figura 3.

$$R_t = \frac{{Ir_1}^{2,5} + {Ir_{11}}^{0,64} + {Ir_{15}}^{0,12}}{2,5 + 0,64 + 0,12}$$

Para cada uma das três foram obtidos os valores de R_t mantendo-se constante dois dos indicadores Ir_n e variando um deles. A Figura 4 mostra que que, quanto maior o peso do indicador que varia, mais ampla é a resposta do indicador total R_t. Ou seja, o valor de R_t "responde" com uma amplitude maior quando varia o indicador Ir_n de maior peso. O que é desejado, tendo em vista que o valor de Ir_n reflete as preocupações do *staff* operacional aderentes a habilidades resilientes da organização, conforme já abordado.

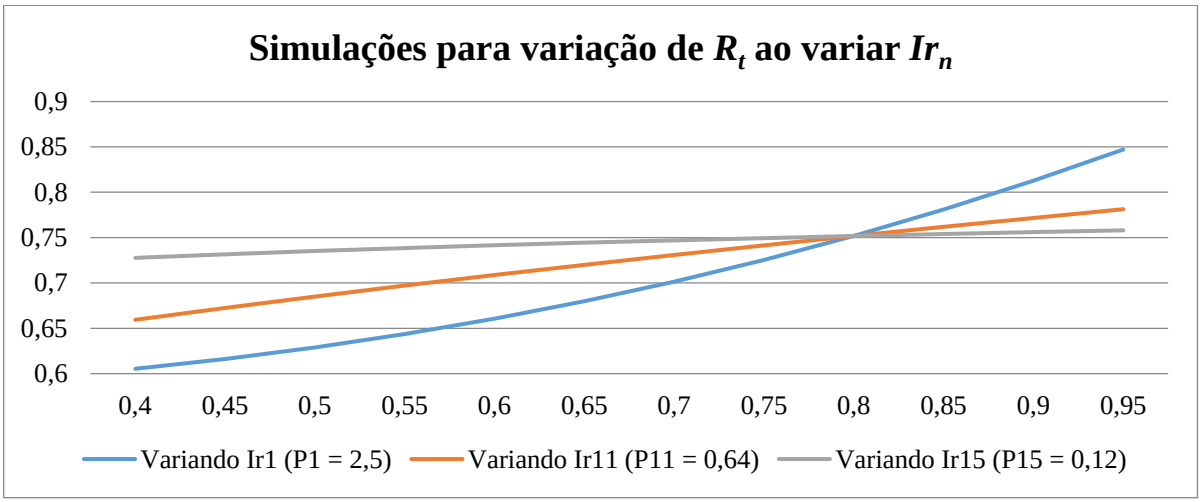

Figura 4 Variação de valores de R_t para diferentes Ir_n e p_n

Com relação aos fatores de resiliência cuja ação proposta não é um indicador e, portanto, não figuram nas árvores de falhas ou eventos, foram propostos planos de ação individualizados e os pesos divulgados internamente para que sejam conhecidas as principais preocupações da operação.

2.5 CONCLUSÃO

Este estudo propôs analisar uma abordagem de risco tradicional de incêndio em um dos transformadores da Itaipu Binacional e nela inseriu elementos que se provaram, durante seu desenvolvimento, aderentes à Engenharia de Resiliência (ER). As abordagens tradicionais de risco, como a montagem de árvores de falhas e eventos, permitem que, por meio de probabilidades de falha de componentes ou sistemas, determine-se um nível de risco de instalações, mas, no entanto, os mecanismos de causa e efeito não revelam como os eventos podem se desenvolver na realidade, conforme buscado na abordagem sistêmica de segurança preconizada pela ER.

Primeiramente, foram estudados artigos de alguns dos principais autores envolvidos na abordagem de ER, de onde extraíram-se os princípios da resiliência. Na sequência, foram realizadas entrevistas com profissionais responsáveis pelas ações de supervisão, controle e mitigação de danos causados por uma eventual explosão em um transformador para que provessem suas percepções e/ou preocupações referentes ao processo. Tais preocupações foram estruturadas e posteriormente verificada sua aderência aos princípios de resiliência. Aos "fatores de resiliência" criados e categorizados com base nas citações, levando em consideração o número de repetições e a ordem destas, foram calculados pesos que levaram em consideração a categoria do profissional que as expressaram para avaliar sua importância e capacidade de impactar um indicador de resiliência a ser definido. Cada fator gerou um indicador que seria vinculado à análise de risco ou à necessidade de um plano de ações para mitigação. Por fim, foi apresentada uma abordagem simplificada da análise de risco da explosão de um transformador por meio de árvore de falhas e de eventos (método "gravata borboleta") com uma sugestão de como seria feita a inserção matemática dos indicadores de resiliência desenvolvidos – sozinhos ou em conjunto com outros – às tradicionais probabilidades de falha.

Apesar da crescente preocupação em promover uma nova abordagem de gestão de segurança de ativos que deixa de focar as falhas para focar os sucessos sob as mais diversas circunstâncias, de forma a assegurar o funcionamento do sistema sociotécnico e tornar a gestão de segurança mais proativa do que reativa, reconhece-se que o assunto ainda é incipiente. Poucas investigações empíricas estão devidamente consolidadas e muito do que se produziu até o momento está no campo teórico. Medir-se quantitativamente a capacidade de uma organização de antecipar, monitorar, prever, resistir e responder a uma disrupção é um

campo que ainda carece de desenvolvimento. Portanto, as principais contribuições deste trabalho para o desenvolvimento da disciplina de ER são:

a) a proposta de inserção quantitativa de princípios e indicadores da ER a uma análise de risco tradicional, estendendo-a;

b) a base teórica para a formação de um indicador de risco operacional de incêndio em transformador de unidade geradora da Itaipu Binacional;

c) a ênfase na participação e na opinião dos profissionais que efetivamente são os responsáveis por executá-la na organização como norteadora da formação de indicadores e planos de ação aderentes aos princípios da ER.

2.6 REFERÊNCIAS

[1] J. Hassan and F. Khan, "Risk-based asset integrity indicators," *J. Loss Prev. Process Ind.*, vol. 25, no. 3, pp. 544–554, 2012.

[2] E. Hollnagel, "Resilience - the Challenge of the Unstable," in *Resilience Engineering: Concepts and Precepts*, 1st ed., E. Hollnagel, N. G. Leveson, and D. D. Woods, Eds. Hampshire: Ashgate, 2006, p. 397.

[3] IAEA, "IAEA Report INSAG-7 Chernobyl Accident: Updating of INSAG-1," Vienna, 1992.

[4] J. Kemeny *et al.*, "Report of the President's Commission on the accident at Three Mile Island: The need for change," Washington, DC, 1979.

[5] IAEA, "Iaea International Fact Finding Expert Mission of the Nuclear Accident Following the Great East Japan Earthquake and Iaea Expert Mission To Japan," Vienna, 2011.

[6] P. V. R. De Carvalho, T. H. Benchekroun, and J. O. Gomes, "Analysis of information exchange activities to actualize and validate situation awareness during shift changeovers in nuclear power plants," *Hum. Factors Ergon. Manuf.*, vol. 22, no. 2, pp. 130–144, 2012.

[7] E. Hollnagel, *Safety-I and Safety-II The Past and Future of Safety Management*, 1st ed. Farnham: Ashgate, 2014.

[8] N. N. Taleb, *The Black Swan: The Impact of the Highly Improbable.*, 1st ed. New York: Random House, 2007.

[9] A. M. Madni and S. Jackson, "Towards a conceptual framework for resilience engineering," *IEEE Syst. J.*, vol. 3, no. 2, pp. 181–191, 2009.

[10] D. D. Woods, *Essential Characteristics of Resilience*, 1st ed. Hampshire: Ashgate, 2006.

[11] Itaipu Binacional, "Perfil Institucional | Visão," 2016. [Online]. Available: https://www.itaipu.gov.br/institucional/visao. [Accessed: 26-Nov-2014].

[12] N. Leveson, "A systems approach to risk management through leading safety indicators," *Reliab. Eng. Syst. Saf.*, vol. 136, pp. 17–34, 2015.

[13] EPRI, “Final report on Leading Indicators of Human Performance,” Palo Alto, CA, 2001.

[14] L. Adolph, B. Lafrenz, and B. Grauel, “Safety Management Systems , Safety Culture and Resilience engineering : Comparison of Concepts,” in *Proceedings of HFES*, 2012, no. 2008.

[15] M. F. Costella, T. A. Saurin, and L. B. de Macedo Guimarães, “A method for assessing health and safety management systems from the resilience engineering perspective,” *Saf. Sci.*, vol. 47, no. 8, pp. 1056–1067, Oct. 2009.

[16] G. H. A. Shirali, M. Motamedzade, I. Mohammadfam, V. Ebrahimipour, and A. Moghimbeigi, “Challenges in building resilience engineering (RE) and adaptive capacity: A field study in a chemical plant,” *Process Saf. Environ. Prot.*, vol. 90, no. 2, pp. 83–90, Mar. 2012.

[17] R. Francis and B. Bekera, “A metric and frameworks for resilience analysis of engineered and infrastructure systems,” *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 90–103, 2014.

[18] A. Hale and T. Heijer, “Defining Resilience,” in *Resilience Engineering: Concepts and Precepts*, 1st ed., E. Hollnagel, D. D. Woods, and N. G. Leveson, Eds. Burlington: Ashgate, 2006, pp. 35–40.

[19] R. Steen and T. Aven, “A risk perspective suitable for resilience engineering,” *Saf. Sci.*, vol. 49, no. 2, pp. 292–297, Feb. 2011.

[20] T. A. Saurin, P. Wachs, A. W. Righi, and É. Henriqson, “The design of scenario-based training from the resilience engineering perspective: A study with grid electricians,” *Accid. Anal. Prev.*, no. 68, pp. 30–41, 2013.

[21] A. Azadeh, V. Salehi, M. Arvan, and M. Dolatkhah, “Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant,” *Saf. Sci.*, vol. 68, pp. 99–107, Oct. 2014.

[22] V. De Dianous and C. Fiévez, “ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance,” *J. Hazard. Mater.*, vol. 130, pp. 220–233, 2006.

[23] N. Khakzad, F. Khan, and P. Amyotte, “Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 8, pp. 925–932, 2011.

[24] N. Khakzad, F. I. Khan, and P. Amyotte, “Quantitative risk analysis of offshore drilling operations: A Bayesian approach,” *Saf. Sci.*, vol. 57, pp. 108–117, 2013.

[25] N. Khakzad, F. Khan, and P. Amyotte, “Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network,” *Process Saf. Environ. Prot.*, vol. 91, no. 1–2, pp. 46–53, 2013.

[26] N. Khakzad, F. Khan, and P. Amyotte, “Dynamic risk analysis using bow-tie approach,” *Reliab. Eng. Syst. Saf.*, vol. 104, pp. 36–44, 2012.

[27] B. Knegtering and H. Pasman, “The safety barometer. How safe is my plant today? Is instantaneously measuring safety level utopia or realizable?,” *J. Loss Prev. Process Ind.*, vol. 26, no. 4, pp. 821–829, 2013.

[28] L. T. T. Dinh, H. Pasman, X. Gao, and M. S. Mannan, “Resilience engineering of industrial processes: Principles and contributing factors,” *J. Loss Prev. Process Ind.*, vol. 25, no. 2, pp. 233–241, Mar. 2012.

[29] P. T. W. Hudson, “Process indicators: Managing safety by the numbers,” *Saf. Sci.*, vol. 47, pp. 483–485, 2009.

[30] P. Wachs and T. A. Saurin, “Proposta de um programa de capacitação com enfoque em habilidades não técnicas: Um estudo de caso no setor elétrico,” in *31 ENEGEP, Belo Horizonte, MG, Brasil, 04 a 07 de outubro de 2011*, 2011, no. 0, pp. 1–13.

[31] F. S. Fogliatto and L. B. de Macedo Guimarães, “Design Macroergonômico: uma proposta metodológica para projeto de produto,” *Produto & Produção*, Porto Alegre, pp. 1–15, Oct-1999.

[32] P. Gustavsson, “Resilience and Procedure Use in the Training of Nuclear Power Plant Operating Crews,” Linköping University, 2011.

[33] G. A. Shirali, I. Mohammadfam, and V. Ebrahimipour, “A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry,” *Reliab. Eng. Syst. Saf.*, vol. 119, pp. 88–94, Nov. 2013.

3 FOCO NO SUCESSO: ABORDAGEM DE SEGURANÇA-II PARA MANOBRAS OPERACIONAIS DA USINA HIDRELÉTRICA ITAIPU BINACIONAL

3.1 INTRODUÇÃO

Acidentes de grandes proporções que ocorram em uma organização de alta complexidade sociotécnica causam, não raro, grande impacto social e econômico. Chernobyl, (1986), Three Mile Island (1979), Sayano-Shushenskaya (2009), Fukushima (2011) e Deepwater Horizon (2010) são exemplos. Em todos, as variabilidades que atuam no processo operacional, mesmo durante a operação normal, tornaram-se fora de controle, impactando funções vitais do processo operacional, por fim levando às falhas. Em situações de acidentes de menores proporções, como no caso da indústria ou do serviço de saúde, entre outros, também tenta-se entender o porquê de um acidente ou falha, utilizando técnicas como RCA [1] por exemplo, que buscam os fatores que contribuíram para o dano, "focando no que dá errado" em uma abordagem conhecida como "Segurança-I" [1]. É uma abordagem tradicional, baseada na suposição de que há certo grau de previsibilidade em todas as operações e que todas as atividades podem ser decompostas, no que repousa sua principal desvantagem [2]. Na falta de todas as informações sobre os acidentes, o método tradicional direciona a investigação. Assim, na abordagem tradicional a causa ou causas são construídas e os relatórios pouco revelam sobre a real situação do sistema sociotécnico.

Mesmo que as análises posteriores tenham sido bem-sucedidas em apontar as causas-raiz destes acidentes e, no que foi possível, estabelecer novos padrões de segurança, evitando ao máximo sua recorrência, não se pode negar que se as condições nas quais os acidentes aconteceram tivessem sido previstas e corrigidas a tempo, provavelmente eles seriam evitados. Para isso, seria necessária uma abordagem diferente da operação normal, e mesmo uma maneira diferente de se pensar a segurança. Ao invés de reativa, deveria ser proativa: perceber os "perigos" do processo antes que saíssem do controle. Esta nova abordagem, denominada "Segurança II", considera importante concentrar na capacidade de adaptação para manter o controle frente a perturbações ou acontecimentos imprevistos [2]. Além disso, a segurança não deve focar nos raros casos de falhas, porque eles não explicam o porquê de o

desempenho quase sempre ser satisfatório e como ele ajuda a cumprir as metas organizacionais. Focar na falta de segurança, ou seja, na falha, não mostra adequadamente a direção a tomar para melhorar a segurança. No entanto, o "foco no sucesso" preconizado pela abordagem de Segurança-II e baseada nos princípios da Engenharia de Resiliência como abordagem válida de gestão de segurança de ativos ainda possui espaço para desenvolvimento teórico e prático [3]. Mesmo os métodos que de alguma forma podem ser aproveitados para levantar "o que dá certo" precisam de alguma adaptação à realidade estudada [4] para que, enfim, logrem algum êxito.

Este artigo objetiva contribuir para a literatura apresentando um estudo de caso da aplicação de princípios e conceitos de Segurança-II à operação da Usina Hidrelétrica Itaipu Binacional considerando quatro manobras típicas, classificadas por periodicidade e complexidade.

A Itaipu Binacional possui dois setores onde sua energia é gerada: 50 e 60Hz, cada um com dez unidades geradoras de 700MW, totalizando 14.000MW de potência instalada na usina. É a maior geradora de energia do mundo, já tendo produzido mais de 2,4 bilhões de MWh em seus 32 anos de operação. Itaipu 50Hz conecta-se ao Sistema Interligado Nacional Brasileiro (SIN-BR) por meio do Elo de Corrente Contínua 600kV e ao Sistema Interligado Nacional Paraguaio (SIN-PY) por meio de uma linha 500kV e quatro linhas 220kV. Itaipu 60Hz conecta-se ao SIN-BR pelo sistema de transmissão 765kV entre Foz do Iguaçu e São Paulo, com derivação para o sul na subestação Ivaiporã, e pela linha de 525kV entre Foz do Iguaçu e Cascavel.

Desligamentos intempestivos de unidades geradoras da Itaipu Binacional têm potencial de causar perda de produção e estabilidade dos sistemas nela interconectados: no caso do SIN-BR, perturbações de grande porte podem iniciar eventos em cascata e levá-lo a condições críticas. Diminuir os riscos e as consequências destas perturbações é das principais preocupações das autoridades do setor elétrico nacional. Porém, quanto mais baixa a probabilidade de ocorrência de determinado evento, mais complexa é a implantação de sistemas de proteção específicos [5]. No caso do SIN-PY, sua dependência da Itaipu Binacional ainda é mais significativa, uma vez esta ser a responsável por pelo menos 75% do fornecimento de energia daquele país, de maneira que perturbações na usina são quase certamente percebidas por meio de cortes de energia.

Neste contexto, interessa às sociedades brasileira e paraguaia que a organização assuma a postura proativa preconizada pelas diretrizes de Segurança-II. Ao basear-se no princípio de equivalência entre "sucessos" e "falhas", assume que tanto operações normais

quanto eventuais acidentes emergem da mesma origem. Segundo este enfoque, segurança é uma consequência da maneira como o sistema complexo se comporta, não uma propriedade estática [6]. Alinhado ao entendimento de que a Itaipu Binacional é reconhecida como líder de produção de energia e sustentabilidade, adotar práticas de Segurança-II vai ao encontro da visão de produção sustentável e alto desempenho operativo.

A segunda seção deste artigo apresenta o referencial teórico dos dois enfoques de segurança, o enfoque reativo de Segurança-I e o enfoque proativo de Segurança-II. A terceira seção apresenta o método utilizado para abordar com "foco no sucesso", a operação da Usina Hidrelétrica Itaipu Binacional, especificamente para quatro manobras representativas dos quadrantes periodicidade-complexidade. A quarta seção apresenta os resultados da análise das manobras em estudo, traça os passos da operação normal de tais manobras, determina as variabilidades que influenciam cada um dos passos das manobras escolhidas, avalia o impacto de cada passo da manobra no resultado global (sucesso ou erro), e por fim analisa as falhas já ocorridas para verificar a aderência do estudo a situações já vivenciadas. A última seção apresenta reflexões dos resultados e considerações para estudos futuros.

3.2 REFERENCIAL TEÓRICO

Estudiosos dedicam esforço significativo no sentido de definir termos chave de gestão de riscos operacionais. O trabalho destes profissionais tem se baseado na assunção de que um campo científico ou disciplina baseia-se em termos bem definidos e universalmente aceitos. No entanto, a realidade aponta que as iniciativas organizacionais não têm sido bem-sucedidas em trazer clareza a este campo. Em vez disso, mais problemas e confusão têm emergido do discurso [3].

Uma linha de pesquisa, denominada engenharia de resiliência, tem se destacado ao propor uma diferenciação entre abordagens de segurança. Segundo esta, há fundamentalmente duas maneiras (não exclusivas mas complementares) de se tratar segurança, uma reativa – "Segurança-I" e outra proativa – "Segurança-II" [7].

3.2.1 Abordagem reativa da Segurança-I

Tradicionalmente, segurança é a ausência de resultados indesejados na operação normal, tais como incidentes ou acidentes. Portanto, o objetivo do gerenciamento

"tradicional" da segurança, denominado Segurança-I, é manter a condição segura, na qual o número de resultados indesejados é o menor possível: as metas são definidas em termos da redução de resultados indesejados medidos em um período de tempo [4].

Sob esta perspectiva, o ponto de partida para discussões acerca de segurança tem sido a ocorrência de acidentes (resultados adversos) ou riscos reconhecidos (potenciais resultados adversos). Novos tipos de acidentes acontecem simplesmente porque sua causa origem não foi eliminada por ser até então desconhecida. Mudanças de tecnologia, fatores humanos ou organizacionais são mudanças que podem levar ao aparecimento de novas causas. As causas e os fatores que contribuem para um evento não desejado são vistos como perigos para o sistema [1].

A Segurança-I promove assim uma maneira bimodal de enxergar trabalho e atividades: quando as coisas dão certo, é porque o sistema funciona como deve e porque as pessoas trabalham da maneira prescrita, como se imagina (*Work-As-Imagined*); quando dão errado, é porque alguma coisa deixou de funcionar ou falhou. A segurança é a qualidade do sistema necessária e suficiente para assegurar que o número de eventos potencialmente prejudiciais aos trabalhadores, público ou meio ambiente seja aceitavelmente baixo [4].

Hollnagel [8] explica que há uma distinção entre o trabalho efetivamente realizado, o trabalho como é feito (*Work-As-Done*) ou trabalho real, e o trabalho prescrito ou o trabalho previsto para ser realizado (*Work-As-Imagined*). Este último é o geralmente considerado na Segurança-I, que explica a falha, ou a falta de segurança, como um desvio do trabalho previsto, não aceitando que o trabalho, no dia a dia, não é feito como imaginado no projeto [8]. É um erro considerar seres humanos como máquinas capazes de apresentar um número finito de comportamentos e responder de finitas maneiras a infinitas possibilidades. A assunção seria verdadeira somente se todos os componentes da "máquina humana" funcionassem exatamente da maneira pela qual foram projetados e não houvesse conflitos entre critérios de segurança e produtividade. Qualquer problema teria uma causa raiz e poderia ser explicada logicamente [8].

Em suma, na abordagem de Segurança-I, segurança, por definição, diz respeito principalmente à avaliação de erros e acidentes, ou seja, à falta de segurança, ao invés da presença de segurança. Ora, quando o sistema funciona satisfatoriamente, é normal que não se preste muita atenção a este sucesso. No entanto, o número de falhas e acidentes é geralmente bem menor do que de acertos e sucessos. Estudos [4] mostram que a probabilidade de uma falha é de 1 em 10.000 ou seja, a chance de acertos é de 9.999 em 10.000 (Figura 5). Portanto, este modelo de segurança acaba empregando tempo e dinheiro para analisar ocorrências raras

ao invés de analisar o comportamento do sistema na maior parte do tempo de operação. Além disso, não se pode ter certeza que as coisas estão dando certo apenas prevenindo-as de dar errado. Aprende-se muito mais ao se entender como o sistema funciona na maior parte do tempo (*Work as Done*) e como e por que ele está dando certo.

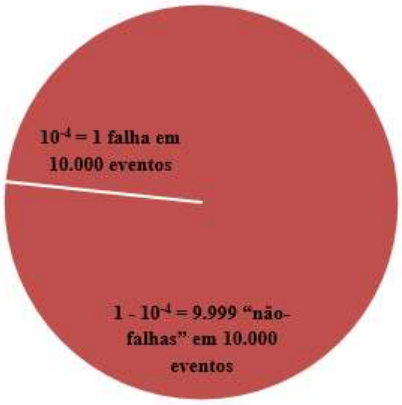

Figura 5 Probabilidade de as coisas darem certo (acertos) e de darem errado (erros/falhas)
FONTE: Adaptado de [4]

Apesar de a abordagem da Segurança-I focar na "falta de segurança", basear-se na análise retroativa do erro, e portanto ter caráter reativo, ela é muito difundida por ser efetiva em prover soluções de curto prazo, nas quais a autoridade responsável pela organização é instada a fornecer respostas rápidas à sociedade para que o acidente não ocorra novamente [4]. A situação é diferente para os eventos bem-sucedidos. Autoridades reguladoras não produzem regulamentos para analisar o que funciona bem, de acordo com as especificações (à exceção de agências de pesquisa ou auditorias); dados são escassos, há pouca literatura sobre modelos e métodos de análise de situações bem sucedidas e mesmo o vocabulário específico ainda está em desenvolvimento [4]. O pouco que se tem sobre segurança daquilo que dá certo, que caracteriza a segurança proativa ou Segurança-II, deriva da Engenharia de Resiliência e é abordada a seguir.

3.2.2 Abordagem proativa da Segurança-II

Segurança-I é baseada em uma visão de segurança desenvolvida entre 1965 e 1985. As demandas e condições de trabalho são muito diferentes agora comparados a esse período. Os sistemas industriais, para começar, eram analógicos, exigiam menor capacidade de interpretação do que os digitais de hoje [9]. Da mesma forma, a dependência da tecnologia da

informação era limitada – funções de suporte eram poucas e relativamente simples, independentes umas das outras – e havia pouca interdependência entre estes sistemas. O nível de integração era baixo, os sistemas de monitoramento e diagnóstico praticamente inexistentes.

Atualmente, a segurança não pode se basear em premissas de que os procedimentos são abrangentes, completos e corretos, os sistemas são bem projetados, os operadores se comportam da maneira esperada (*Work as Imagined*), e todas as contingências estão mapeadas. Há algum tempo não é mais verdadeira a assunção de que seres humanos, sem qualquer auxílio, estavam aptos a controlar os processos. Acidentes em organizações de alto desempenho operacional, com graves consequências socioeconômicas são raros, principalmente devido a que suas instalações são projetadas para garantir um nível de segurança superior e, via de regra, seu *staff* operacional receber capacitação contínua. No entanto, à medida que a tecnologia avança e novas variabilidades são inseridas no processo, aumenta o desafio em se manter uma operação segura e confiável.

A abordagem contemporânea de segurança, denominada Segurança-II, é baseada no princípio de equivalência entre "sucessos" e "falhas", bem como nos "ajustes finos" de desempenho, que fazem com que o desempenho sempre seja variável. Mesmo em uma operação normal, uma determinada variabilidade pode propagar-se de função em função, levando enfim a um resultado não esperado, ou efeitos não-lineares [9]. Portanto, tanto operações normais quanto eventuais acidentes emergem de funções cujos resultados são influenciados por variabilidades presentes em qualquer operação, normal ou falha. A amplitude de tais variabilidades (e o seu monitoramento) é que vai definir o resultado da operação. Segurança é, portanto, uma propriedade emergente que envolve a operação de um sistema complexo sendo uma consequência da maneira como o sistema se comporta, não uma propriedade estática deste. Esta visão requer o entendimento de que, para evitar um acidente, um sistema deve garantir, de maneira proativa, que todos os seus atributos estão sob controle [6] sendo imprescindível que uma empresa tenha a habilidade de ajustar seu desempenho, já que a capacidade de adaptação, ou resiliência, é um caminho para responder, de forma adequada a ameaças previstas e imprevistas [1].

Ameaças ao sistema podem ser classificadas como regulares, irregulares e inéditas, como internas e externas. Antecipar, responder e adaptar-se a estas ameaças de forma adequada é uma característica fundamental de sistemas resilientes [1].

Uma ameaça regular é a que ocorre com frequência suficiente a ponto de a organização ou sistema ser capaz de desenvolver uma resposta padrão (uma instrução

normativa, um plano de treinamento). As ameaças irregulares são de "baixa probabilidade", mas potencialmente catastróficas. Sua extemporaneidade torna muito complicado, ou inviável, que se desenvolva um processo padrão para contê-la. Um exemplo de acidente causado por este tipo de ameaça é o do voo JJ3054 em 2007, no qual fatores de baixa probabilidade (um deles, o reversor do motor 2 desativado durante procedimento de pouso) contribuíram para que ocorresse [10].

Ameaças inéditas são aquelas inesperadas a ponto de serem consideradas inimagináveis; exigem mais do que capacidade de adaptação e improvisação, exigem uma mudança essencial na maneira de pensar. Os ataques de 11/set são exemplos de ameaças inéditas [1]. Outro é o da usina hidrelétrica Sayano-Shushenskaya, no qual houve rompimento dos parafusos que sustentavam a tampa da turbina da unidade geradora 2, situação até então inédita em usinas hidrelétricas de grande porte [11].

Em suma, a perspectiva de “Segurança-II” é baseada em um princípio simples e instigante: de que se deve entender e apoiar o muito que dá certo [1] em vez de investir praticamente todos os esforços e recursos no pouco que dá errado. Focar o sucesso em vez de focar o fracasso implica em entender que as ações humanas são executadas sobre situações reais, sujeitas a alta variabilidade, e não a situações previamente imaginadas e projetadas, mas irreais. Segundo esta visão, deve-se evitar tratar falhas como eventos únicos, mas vê-las como a expressão da variabilidade de desempenho na rotina diária. É uma boa aposta dizer que as coisas que dão errado já deram certo muitas vezes antes, e darão certo muitas outras vezes no futuro. Em outras palavras, quando acontece o erro, deve-se começar entendendo o porquê da ação normalmente ser correta, em vez de procurar causas específicas que explicam somente a falha [9]. Sendo assim, focar o trabalho real (*Work as Done*) e a variabilidade de desempenho inerente à função, sendo o objetivo mapear e monitorar as variabilidades durante a operação normal, a que ocorre com maior frequência. É interessante notar que a variabilidade, um dos maiores obstáculos para obtenção da qualidade, sob o enfoque da disciplina “Qualidade”, é um fator chave, considerado normal, na Segurança-II.

3.3 MÉTODO

Na prática, ainda é incipiente o tratamento de segurança segundo os preceitos de Segurança-II. Há muitos métodos que podem apresentar uma abordagem para encontrar o

“foco no sucesso”. Nenhum dos métodos, no entanto, é específico de Segurança-II. São abordagens que podem ser adaptadas para atingir este intuito em pelo menos um critério [4].

Para este estudo, foram verificados os métodos disponíveis na literatura de engenharia de resiliência, citados em [4]. Nenhum deles mostrou-se integralmente aplicável à prática deste estudo: os métodos *Day-to-day safety survey* (D2D) e *Normal Operations Safety Survey* (NOSS) são abordagens voltadas a entender a variabilidade de desempenho e ajustes na operação *Work-As-Done*; requerem a coleta de dados de segurança durante a operação cotidiana, requerendo a observação diária do trabalho. Enquanto NOSS é baseado no gerenciamento de ameaças e erros, D2D é baseado no uso de técnicas consideradas “boas práticas” de operação e analisa o ambiente livre de ameaças [12].

O principal método a servir de inspiração para o estudo do ponto de vista conceitual foi o *Functional Resonance Analysis Method* (FRAM), por refletir o pensamento de Segurança-II e de Engenharia de Resiliência [13]. De acordo com [14], pode ser utilizado tanto para avaliação de risco quanto para análise de acidentes, apesar do seu uso completo requerer um alto nível de entendimento da teoria que lhe dá suporte além de não ser simples a obtenção de resultados práticos [14] .

FRAM pretende o entendimento de sistemas sociotécnicos de alta complexidade a partir de cinco passos principais [15]:

- Fornecer subsídio para verificar se a análise do sistema é retrospectiva ou prospectiva;
- Identificar as funções do trabalho cotidiano que tornam o sistema bem-sucedido;
- Descrever a variabilidade de tais funções;
- Entender como essas variabilidades conectam-se entre si;
- Propor maneiras de gerenciar as possíveis ocorrências de desempenho fora de controle.

Os procedimentos, detalhados em [13], mostram que o método se preocupa com as funções de um sistema ao invés de seus componentes – como ocorre em uma abordagem tradicional de risco – questionando “o que dá certo” para que o sistema atinja seus objetivos.

Com inspiração no método FRAM, foram mapeadas as funções das manobras típicas de operação normal (*Work as Done)* da usina Itaipu Binacional, suas variabilidades, e as condições (ruídos) interferentes. Devido a haver número significativo (qualitativa e quantitativamente) de manobras executadas para operação da usina Itaipu Binacional, cada uma com vários passos, comandos e supervisões, com níveis de complexidade/atenção diferentes, foi criada uma matriz de quatro quadrantes com categorias “complexidade” e

“periodicidade” de forma que quatro manobras representariam o universo para fins deste estudo. A *periodicidade*, ou *frequência*, da manobra diz respeito à quantidade de vezes nas quais ela foi executada no período em questão. A *complexidade* da manobra diz respeito à quantidade de passos a serem executados e, durante estes passos, à quantidade de fatores (vulnerabilidade/ruídos) que podem influenciar em seu sucesso.

O primeiro passo para definir a operação normal e as variabilidades foi escolher manobras executadas no período entre 2006 e 2015, dentre as mais de quinhentas executadas pela operação da usina Itaipu Binacional, que representem o universo de manobras. O banco de dados do relatório diário da operação foi a base para estratificação destas por “periodicidade”. Um dos critérios para a escolha da manobra foi que ela deve causar, em caso de falha no processo operacional, impacto na produção ou na segurança das pessoas, das instalações ou do meio ambiente no entorno da usina.

O Departamento de Operação da Usina e Subestações da Itaipu Binacional conta no total com 19 (dezenove) engenheiros, 97 (noventa e sete) técnicos de operação e 6 (seis) assistentes técnicos e administrativos. A operação em tempo real da usina trabalha em regime de turnos de revezamento de 6 (seis) horas, ininterruptos, do qual fazem parte 11 (onze) técnicos de operação por turno, responsáveis por supervisionar e controlar a usina enquanto em operação. Inspecionam os equipamentos em funcionamento, realizam manobras, analisam e monitoram os mais de 20.000 (vinte mil) estados digitais e analógicos que apontam a situação das instalações, equipamentos e sistemas da usina. Enquanto os técnicos efetivamente executam as manobras, os engenheiros fornecem subsídios técnicos e de gestão ao trabalho de tempo real, nas fases de pré e pós-operação.

Para: a) escolher as manobras que representariam um dos quatro quadrantes da matriz periodicidade-complexidade; b) determinar as variabilidades que influenciam cada um dos passos das manobras escolhidas; c) avaliar o impacto de cada passo da manobra no resultado global (sucesso ou erro) foram conduzidas entrevistas com 31 técnicos de operação e incluídas as opiniões de 8 engenheiros de operação, quanto a itens não identificados pelos primeiros. O perfil de experiência e idade dos voluntários envolvidos no estudo está disposto na Tabela 7.

Tabela 7 Perfil dos profissionais envolvidos no estudo

Cargo	***Quantidade***	***Experiência na empresa (média)***	***Idade (média)***
Engenheiros de Operação	8	7,1	35,9
Técnicos de Operação	31	21,8	44,7

Entrevistas *in loco* também foram conduzidas, com o pesquisador, engenheiro de operação, acompanhando as manobras de rotina. O envolvimento do pesquisador com o tema e com as pessoas investigadas caracteriza uma pesquisa participante, aplicada e exploratória.

3.4 RESULTADOS E DISCUSSÃO

A Figura 6 mostra a quantidade de manobras operacionais na usina Itaipu Binacional das quatro manobras típicas selecionadas para o estudo nos últimos dez anos e a quantidade de falhas de manobra que redundaram em perda de produção de energia, confiabilidade ou em danos em equipamentos. Nota-se que, no período de 2006 a 2015, as falhas representam 0,025% enquanto as manobras bem-sucedidas somam 99,975% do total, resultado aderente à Figura 5.

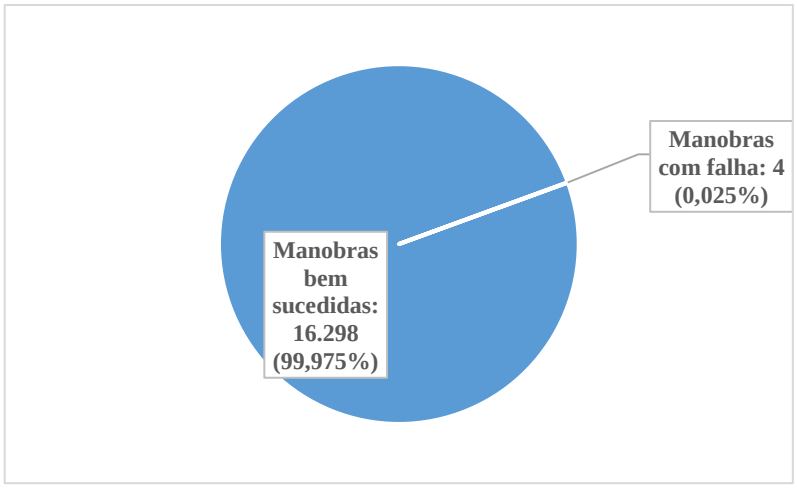

Figura 6 Manobras bem-sucedidas x falhas na Itaipu Binacional, período 2006 a 2015

No período de 2006 a 2015, houve apenas 4 (quatro) falhas de processo operacional entre as 16302 manobras executadas, categorizadas por periodicidade e complexidade conforme a Tabela 8. Para cada um destes eventos de falha, foram produzidos relatórios, estudos de causa-efeito, gestão de providências, para evitar sua recorrência. Os detalhes de cada falha estão descritos mais adiante.

Pouco, ou nada, se produziu a respeito da fatia que representa 99,975% do gráfico, ou seja, pouco se produziu no sentido de responder à pergunta “o que estamos fazendo certo?”, justificando a importância deste estudo sob o enfoque da Segurança-II. A relação entre os 0,025% de manobras com falhas que impactaram na produção ou na segurança de equipamentos e as 99,975% de manobras executadas com sucesso dá suporte a um dos princípios fundamentais de Segurança-II: que se deve estudar o trabalho que dá certo, e que

tem a maior incidência, em vez de concentrar todos os esforços em eventuais falhas que, de tão raras, jamais se repetem nas mesmas condições físicas, técnicas e ambientais [1].

Tabela 8 Manobras contempladas no estudo no período de 2006 a 2015

Manobra	Periodicidade	Complexidade	Total manobras executadas
Selecionar unidades geradoras para controle convencional	BAIXA	BAIXA	**553**
Separação de unidades geradoras para a ANDE	BAIXA	ALTA	**27**
Reversão de bombas do regulador de velocidade	ALTA	BAIXA	**10400**
Partida e parada de unidade geradora	ALTA	ALTA	**5322**
TOTAL			**16302**

As manobras, conforme a Tabela 8, podem ser assim sucintamente descritas:

Selecionar unidades geradoras para controle convencional: em caso de falha ou manutenção no sistema digital de controle e supervisão da Sala de Controle Central, é necessário cumprir etapas até as unidades geradoras operarem em modo convencional (analógico); é uma manobra de baixa complexidade, no entanto, se não devidamente executados com atenção, podem acarretar a redução da produção de energia de todo um setor da usina (50 ou 60Hz).

Separação de unidades geradoras para a ANDE: necessidades dos sistemas elétricos brasileiro ou paraguaio podem levar à Itaipu Binacional executar manobras em seu setor de geração de 50Hz que separe o sistema brasileiro do paraguaio sem que haja qualquer perda de intercâmbio com nenhum país. É uma manobra de alta complexidade tendo em vista os muitos passos envolvidos e o impacto que um eventual erro poderia causar (desligar totalmente o sistema paraguaio).

Reversão de bombas do regulador de velocidade: a reversão é toda manobra que objetive estabelecer um rodízio entre equipamentos duplos ou triplos, com vistas a otimizar a vida útil dos equipamentos, evitando que a concentração de trabalho em determinado componente acarrete em desgastes excessivos. É uma manobra de baixa complexidade, porém um erro pode causar a parada intempestiva de uma unidade geradora.

Partida e parada de unidade geradora: é a manobra completa de, estando a unidade geradora parada, parti-la até a sincronização ao sistema, e pará-la de maneira normal (sem atuação de proteção). É de alta complexidade tendo em vista as várias etapas de diferentes fontes e sujeitas a diferentes variabilidades.

Pelas entrevistas com os oito engenheiros e trinta e um técnicos de operação, foram levantadas as variabilidades que influenciam estes quatro tipos de manobras operacionais.

Verificou-se que, não importando a complexidade e periodicidade da manobra, 16 (dezesseis) variabilidades, agrupadas em 6 categorias, pelo pesquisador, são comuns aos quatro tipos de manobras, conforme disposto na Tabela 9.

Tabela 9 Variabilidades que influenciam a operação

Categoria	***Variabilidade***
Operador	Conhecimento
	Capacidade de adaptação a situações inesperadas
	Necessidade de confirmar o passo
Comunicação	Disponibilidade de equipamento
	Operador/supervisor comunica os passos
	Qualidade da comunicação operativa
Recursos Humanos	Disponibilidade de recursos humanos
	Coordenação/hierarquia na execução do passo
Instrução	Qualidade da instrução
	Restrições operativas em vigência
Ambiente de manobra	Situações que tiram a atenção do operador (telefone/alarme)
	Situações de urgência/emergência/trabalhos concomitantes
	Similaridade com outro ambiente de manobra
Equipamento de manobra	Funcionamento
	Disponibilidade de sistemas informatizados
	Peculiaridades do equipamento (não estão descritas em nenhum lugar)

Durante o fluxo da manobra, desde seu início até sua conclusão, vários passos são executados. Para efeito do estudo, existem três tipos de passos:

1) Passos-chave: funções centrais através das quais o objetivo da manobra é alcançado. Exemplos: fechamento do disjuntor, sincronização da unidade;
2) Passo relevante: apesar de não serem centrais, contribuem com o fluxo normal da manobra de maneira decisiva; uma falha nestes pode influenciar o passo-chave, e, portanto, causar erro na manobra. Exemplos: acionar preparação de partida, confirmar barramento sem tensão;

A Tabela 10 mostra os passos de uma das manobras (Selecionar unidades geradoras para controle convencional) com algumas das variabilidades (especificamente, a que envolve operadores) para ilustrar como foi a montagem da tabela geral. Considerou-se que é menos importante entender o significado de cada passo do que entender como cada variabilidade influencia o passo-chave da manobra, também destacado na tabela.

A informação de que o passo é do tipo “passo relevante” também está na Tabela 10.

Tabela 10 Exemplo de manobra e variabilidades

	Passo	***Passo relevante para eventual erro (ressonância funcional)?***	***Operador - Conhecimento***	***Operador - Capacidade de adaptação a situações inesperadas***	***Operador - Necessidade de confirmar o passo***
1	*Solicitar ao despacho que desligue CAG/CAT*	N			
2	*Ajustar potência de referência no JCC*	S	X	X	X
3	*Confirmar no JTC o voltímetro de zero central em zero*	S			
4	*Ajustar tensão de referência no painel JCC*	S	X	X	
5	*Selecionar unidades, linhas, barras, vão do TA de Scada 1 para convencional*	S	X	X	X
6	*Confirmar no JCC a chave 43JCS na posição convencional*	N			
7	*Compatibilizar a seleção das unidades no painel CD (analógico)*	N	X	X	

Para exemplificar, considerou-se que a variabilidade "Conhecimento do operador" não influencia no passo "Solicitar ao despacho que desligue CAG/CAT", uma vez que se trata somente de uma comunicação com outro agente. O conhecimento do operador não é relevante para o resultado deste passo. Por outro lado, considerou-se que a "Capacidade de adaptação a situações inesperadas" influencia no passo "Ajustar tensão de referência no painel JCC" porque, havendo uma situação inesperada na hora desta manobra – por exemplo, perturbação no sistema elétrico –, o operador deve ter capacidade de adaptar a manobra a esta situação (inclusive abortar sua realização, se for o caso).

Cada uma das quatro manobras objetos do estudo possuem um número específico de passos-chave, passo relevante e periféricos. A quantidade de passos de cada manobra e a quantidade de passos do tipo "passo relevante", as que importam para este estudo por influenciarem no resultado da manobra, são mostrados na Tabela 11.

Tabela 11 Número de passos das manobras estudadas: total e "caminho crítico"

Manobra	**Número de passos da manobra**	**Número de passos "Caminho Crítico"**
Selecionar unidades geradoras para controle convencional	7	5
Separação de unidades geradoras para a ANDE	20	18
Reversão de bombas do regulador de velocidade	6	4
Partida e sincronização de unidade geradora	22	14
TOTAL	**55**	**41**

Com base na avaliação dos integrantes da operação e observação do pesquisador – que acompanhou as manobras –, para cada um dos 41 (quarenta e um) passos do tipo "passo relevante" fez-se a pergunta "quais as variabilidades da Tabela 9 influenciam este passo?". O

resultado geral, com as frequências de cada variabilidade, está na Tabela 12, que fornece uma visão geral das quatro manobras, sem separá-las por complexidade e periodicidade.

Tabela 12 Frequência das variabilidades nos passos “caminho crítico”, cômputo geral

Variabilidade	Frequência
Ambiente de manobra – Situações que tiram a atenção do operador (telefone/alarme)	83%
Ambiente de manobra – Similaridade com outro ambiente de manobra	80%
Equipamento de manobra – Funcionamento	83%
Instrução – Restrições operativas em vigência	75%
Ambiente de manobra – Situações de urgência/emergência/trabalhos concomitantes	73%
RH – Disponibilidade de recursos humanos	73%
Operador – Conhecimento	68%
Operador – Necessidade de confirmação do passo	63%
Instrução – Qualidade	65%
Comunicação – Operador/supervisor comunica os passos	58%
RH – Coordenação/hierarquia na execução do passo	25%
Operador – Capacidade de adaptação a situações inesperadas	30%
Comunicação – Qualidade da comunicação operativa	25%
Comunicação – Disponibilidade de equipamento	25%
Equipamento de manobra – "Macetes", "dicas" que não estão descritos em nenhum lugar	23%
Equipamento de manobra – Disponibilidade de sistemas informatizados	0%

Pela Tabela 12, 83% dos passos executados nos quatro tipos de manobras deste estudo são influenciadas pela variabilidade “Situações que tiram a atenção do operador (telefone/alarme)”.

A partir deste ponto, partiu-se para a formação da matriz complexidade x periodicidade, conforme Tabela 13, que mostra a frequência de variabilidades específica para cada um dos quatro quadrantes da matriz.

Tabela 13 Frequência das variabilidades nos passos “caminho crítico”, estratificado

BAIXA COMPLEXIDADE			**ALTA COMPLEXIDADE**	
Ambiente de manobra - Similaridade com outro ambiente de manobra	85%		Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	76%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	62%		Equipamento de manobra - Funcionamento	74%
Instrução - Restrições operativas em vigência	62%		Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	74%
Instrução - Qualidade da instrução	54%		RH - Disponibilidade de recursos humanos	67%
Operador - Conhecimento	46%		Operador - Necessidade de confirmar o passo	64%
Operador - Capacidade de adaptação a situações inesperadas	46%		Instrução - Restrições operativas em vigência	64%
BAIXA PERIODICIDADE			**ALTA PERIODICIDADE**	
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	93%		Equipamento de manobra - Funcionamento	61%
RH - Disponibilidade de recursos humanos	85%		Operador - Conhecimento	57%
Instrução - Qualidade da instrução	85%		Ambiente de manobra - Similaridade com outro ambiente de manobra	57%
Operador - Necessidade de confirmar o passo	81%		Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	50%
Instrução - Restrições operativas em vigência	78%		Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	50%
Ambiente de manobra - Similaridade com outro ambiente de manobra	74%		Instrução - Restrições operativas em vigência	50%

Da Tabela 13, pode-se tecer algumas conclusões:

a) O “ambiente de manobra” é uma categoria de significativa importância em todas as situações de complexidade e periodicidade.
b) O “conhecimento do operador”, apesar de ser uma variabilidade significativa e de fundamental importância, não aparece como principais variabilidades nas manobras de alta complexidade e de baixa periodicidade.
c) À maior parte dos passos incide a variabilidade “Similaridade com outro ambiente de manobra”; deve-se a um fato comum em usinas com várias unidades geradoras: a tendência é que cada ambiente onde o operador execute a manobra seja exatamente igual ao de todas as outras unidades, à exceção das identificações operativas.
d) A categoria “instrução” afeta de maneira mais significativa as manobras de baixa complexidade ou de baixa periodicidade
e) Em manobras *cuja periodicidade é baixa*, muitas das variabilidades afetam praticamente todos os passos. A principal variabilidade a afetar a operação normal advém de situações

que tiram a atenção do operador. Tal afirmação não é estranha pois à medida que a manobra deixa de ser executada, o operador tende a voltar sua atenção para ela, e as condições ambientais que lhe tiram essa atenção influenciam a operação normal. Não menos importante é notar que outra variabilidade muito afetada é a disponibilidade de recursos humanos. Contar com alguém para auxiliar a manobra é condição essencial para o sucesso.

f) Em manobras de *alta complexidade*, as duas variabilidades que mais afetam as funções ("Ambiente de manobra – Situações de urgência/emergência/trabalhos concomitantes" e "Equipamento de manobra – Funcionamento") são externas à operação, de forma que há pouco a propor como ação concreta da operação para diminuir suas influências na operação normal. Aqui se faz mister ressaltar a importância da experiência da equipe de operação bem como a gestão do conhecimento na operação como forma de aumentar sua capacidade de adaptação e resposta a eventual disrupção, um dos preceitos fundamentais da engenharia de resiliência [16].

Como resultado, algumas ações foram propostas para diminuir a influência da variabilidade no resultado global da manobra. Somente foram propostas ações para as variabilidades que aparecem em mais de 50% dos passos das manobras do estudo.

Tabela 14 Ações propostas

BAIXA COMPLEXIDADE		AÇÃO PROPOSTA	Id_ação
Ambiente de manobra - Similaridade com outro ambiente de manobra	85%	Investir em identificações operativas visíveis, de qualidade e com manutenções periódicas. No caso de sistemas digitais, incluir regras de operação que avisem o operador caso uma manobra em curso esteja violando instruções.	1
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	62%	Solicitar que outro operador acompanhe a manobra; para manobras executadas na Sala de Controle Central, criar sinalização visual "em manobra" para que outros profissionais saibam que há manobra em andamento.	2
Instrução - Restrições operativas em vigência	62%	Utilizar ferramenta tecnológica para montar um mapa de restrições operativas, disponível em todos os equipamentos portáteis usados pelos operadores.	3
Instrução - Qualidade da instrução	54%	A operação da usina é cliente; deve estabelecer canal de proposições de melhoria contínua com a área responsável pelas instruções.	4
BAIXA PERIODICIDADE		**AÇÃO PROPOSTA**	**Id_ação**
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	93%	Ver Id_ação 2.	2
RH - Disponibilidade de recursos humanos	85%	Afixar sinalização visual lembrando que toda manobra deve ser executada por pelo menos dois profissionais. Caso não haja disponibilidade, a manobra não deve ser executada.	5
Instrução - Qualidade da instrução	85%	Ver Id_ação 4.	4
Operador - Necessidade de confirmar o passo	81%	Fazer instrução específica de comunicação operacional.	6
Instrução - Restrições operativas em vigência	78%	Ver Id_ação 3.	3
Ambiente de manobra - Similaridade com outro ambiente de manobra	74%	Ver Id_ação 1.	1
ALTA COMPLEXIDADE		**AÇÃO PROPOSTA**	**Id_ação**
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	76%	Variabilidade externa. Investir na gestão do conhecimento e na experiência da equipe (sempre ter pelo menos um operador muito experiente no turno de operação).	7
Equipamento de manobra - Funcionamento	74%	Variabilidade externa muito influenciada pela experiência da equipe e sua capacidade de adaptação ao executar a manobra (o que fazer caso um equipamento falhe). Investir em gestão do conhecimento e experiência da equipe é fundamental.	8
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	74%	Ver Id_ação 2.	2
RH - Disponibilidade de recursos humanos	67%	Ver Id_ação 5.	5
Operador - Necessidade de confirmar o passo	64%	Ver Id_ação 6.	6
Instrução - Restrições operativas em vigência	64%	Ver Id_ação 3.	3
ALTA PERIODICIDADE		**AÇÃO PROPOSTA**	**Id_ação**
Equipamento de manobra - Funcionamento	61%	Ver Id_ação 8.	8
Operador - Conhecimento	57%	Capacitação, treinamento e gestão do conhecimento na operação.	9
Ambiente de manobra - Similaridade com outro ambiente de manobra	57%	Ver Id_ação 1.	1

Ao tratar separadamente a complexidade e a periodicidade das manobras, foi mais fácil identificar ações de melhoria pois é menos complicado tratar estes parâmetros separadamente do que entrevistar o *staff* toda vez que for feita a classificação por periodicidade e complexidade juntos. Assim, considerou-se que um passo adiante neste estudo seria estudar um número maior de manobras.

Apesar da Segurança-II enfatizar a análise do sucesso ao invés das falhas, entendeu-se que seria importante confrontar os resultados obtidos com as quatro falhas ocorridas entre 2006 e 2015.

Primeira falha de processo operacional: ocorrida em 2010. Manobra de baixa complexidade e alta periodicidade. A análise operacional da falha apontou que em 5 (cinco) dos 6 (seis) passos houve falha de processo. Iniciou-se com o primeiro passo caminho crítico e se propagou por todo o caminho até o passo-chave.

Na ocasião, um alarme relativo à condição de pressão do sistema de regulação de velocidade estava acionado; havia outros trabalhos em execução no equipamento, que na realidade não tinham relação com esse alarme; porém, por conta dessa intervenção, o operador que foi fazer a inspeção de rotina no equipamento foi equivocadamente orientado a ignorá-lo. Havia, portanto, um defeito real no equipamento (eram necessárias três bombas de pressurização do sistema de regulação de velocidade para que a pressão se mantivesse estável; em situação normal, uma bomba é suficiente). Ao executar a manobra prevista na inspeção (transferir a bomba), não houve análise adequada da situação operacional do sistema, fazendo com que a pressão caísse abruptamente e a unidade geradora desligasse automaticamente por atuação de sua proteção.

O relatório concluiu que:

a) houve coincidência entre acionamento do alarme e execução de trabalho no equipamento, sem vinculação entre os mesmos, o que exigiria atenção especial das equipes de tempo real. *Variabilidades: Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)* e *Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes*.

b) ao chegar na frente do equipamento e realizar sua inspeção, houve falha na análise da situação operacional momentânea, causando a execução de manobras indesejadas de transferência de bombas. *Variabilidades: Operador - Conhecimento* e *Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes*.

c) havia defeito no sistema de controle hidráulico da pressão de óleo do regulador de velocidade, que causou a entrada em operação das três bombas. *Variabilidade: Equipamento de manobra - Funcionamento*.

As variabilidades na Tabela 15 são as mesmas da Tabela 13; as realçadas estavam presentes na ocasião e foram determinantes para o resultado indesejado. Solicitar a outro operador para acompanhar a manobra tendo em vista a situação incomum, ação proposta na Tabela 14 como resposta à variabilidade "Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)", diminuiria muito a probabilidade de esta falha ter ocorrido.

Tabela 15 Variabilidades na falha operacional de 2010

BAIXA COMPLEXIDADE	
Ambiente de manobra - Similaridade com outro ambiente de manobra	85%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	62%
Instrução - Restrições operativas em vigência	62%
Instrução - Qualidade da instrução	54%
Operador – Conhecimento	46%
Operador - Capacidade de adaptação a situações inesperadas	46%
ALTA PERIODICIDADE	
Equipamento de manobra – Funcionamento	61%
Operador – Conhecimento	57%
Ambiente de manobra - Similaridade com outro ambiente de manobra	57%
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	50%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	50%
Instrução - Restrições operativas em vigência	50%

Segunda falha de processo operacional: ocorrida em 2008. Manobra de alta complexidade e baixa periodicidade. Nesta, em 2 (dois) dos 17 (dezessete) passos houve falha de processo.

Na ocasião, a unidade geradora U9A deveria ser retirada do sistema (desligada) para ensaios de manutenção. A potência da unidade foi reduzida de maneira controlada para que, na sequência, fossem abertos os seus disjuntores, efetivamente desligando-a. Todos os passos até então transcorreram sem anormalidades. No entanto, havia, no mesmo momento, solicitação do sistema elétrico para que mais tarde fosse desligada a unidade U03.

Ao entrar na tela do sistema digital para abrir os disjuntores da U9A, o operador coordenador da manobra estava induzido por informações de que posteriormente deveria ser parada a U03, e que os disjuntores desta unidade, por defeito em seu sistema de comando, deveriam ser abertos manualmente antes de ser acionada parada, então solicitou equivocadamente ao executante da manobra que acessasse a tela de comando do sistema digital associada à U03, quando deveria ter solicitado que fosse aberta a tela associada ao vão

da U9A. Foram assim abertos os disjuntores referentes à U03, quando deveriam ter sido abertos os disjuntores referentes à U9A, provocando rejeição de carga na U03.

O relatório concluiu que:

a) o defeito no sistema de comando dos disjuntores da U03 contribuiu para a falha pois, em seu processo de parada, eles teriam de ser abertos antes de ser efetuado comando de parada da unidade. Assim, como a U9A já estava parada, bastou o comando nos disjuntores da U03 para que a falha se consumasse. *Variabilidade: Equipamento de manobra - Funcionamento*.

b) ambos os envolvidos na manobra a executaram sem que estivessem claros o objetivo e as implicações envolvidas. *Variabilidade: Operador - Necessidade de confirmar o passo*.

c) as telas de manobra de todas as unidades geradoras são praticamente iguais, à exceção da identificação da unidade geradora. *Variabilidades: Operador - Necessidade de confirmar o passo* e *Ambiente de manobra - Similaridade com outro ambiente de manobra*.

As variabilidades na Tabela 16 são as da Tabela 13; as realçadas estavam presentes na ocasião e foram determinantes para o resultado indesejado. Uma regra no sistema digital que fizesse aparecer uma janela de alerta quando o operador executasse o comando de abrir os disjuntores relativos à U03 estando essa em operação normal, ação proposta na Tabela 14 como resposta à variabilidade "Ambiente de manobra – Similaridade com outro ambiente de manobra" diminuiria consideravelmente a probabilidade de esta falha ter ocorrido.

Tabela 16 Variabilidades na falha operacional de 2008

ALTA COMPLEXIDADE	
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	76%
Equipamento de manobra – Funcionamento	74%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	74%
RH - Disponibilidade de recursos humanos	67%
Operador - Necessidade de confirmar o passo	64%
Instrução - Restrições operativas em vigência	64%
BAIXA PERIODICIDADE	
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	93%
RH - Disponibilidade de recursos humanos	85%
Instrução - Qualidade da instrução	85%
Operador - Necessidade de confirmar o passo	81%
Instrução - Restrições operativas em vigência	78%
Ambiente de manobra - Similaridade com outro ambiente de manobra	74%

Terceira falha de processo operacional: ocorrida em 2014. Manobra de alta complexidade e alta periodicidade. Nesta, em 3 (três) dos 22 (vinte e dois) passos houve falha de processo.

Na ocasião, a unidade U09 deveria partir e sincronizar ao sistema elétrico. Para executar a sequência de partida de forma automática, seria necessário um operador comparecer ao painel local da unidade para comutar o modo de comando da unidade para automático. Com a dificuldade de localizar o operador, resolveu-se executar a manobra manualmente. Com outros trabalhos em andamento na sala de controle, a manobra foi realizada por um só operador. Neste processo, houve o fechamento do disjuntor da U09 fora das condições ideais de sincronismo, resultando em esforços elétricos e mecânicos danosos à unidade; ademais, o efetivo fechamento deveria ter sido impedido pelo painel de sincronismo, no entanto um defeito interno ao painel permitia o fechamento do disjuntor com qualquer defasagem angular.

O relatório concluiu que:

a) o defeito no painel de sincronismo contribuiu para a falha pois permitiu o fechamento do disjuntor da unidade em qualquer condição de defasagem angular. *Variabilidade: Equipamento de manobra - Funcionamento*.

b) o operador executou a manobra sozinho por haver outros trabalhos e situações urgentes no momento da manobra dentro da sala de controle, portanto não confirmou os passos da manobra com nenhum outro operador. *Variabilidades: RH - Disponibilidade de recursos humanos, Operador - Necessidade de confirmar o passo* e *Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes*.

As variabilidades na Tabela 17 são as da Tabela 13; as realçadas estavam presentes na ocasião e foram determinantes para o resultado indesejado. A execução da manobra por dois operadores, ação proposta na Tabela 14 como resposta à variabilidade "RH – Disponibilidade de Recursos Humanos" diminuiria consideravelmente a probabilidade de esta falha ter ocorrido.

Tabela 17 Variabilidades na primeira falha operacional de 2014

ALTA COMPLEXIDADE	
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	76%
Equipamento de manobra - Funcionamento	74%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	74%
RH - Disponibilidade de recursos humanos	67%
Operador - Necessidade de confirmar o passo	64%
Instrução - Restrições operativas em vigência	64%
ALTA PERIODICIDADE	
Equipamento de manobra - Funcionamento	61%
Operador - Conhecimento	57%
Ambiente de manobra - Similaridade com outro ambiente de manobra	57%
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	50%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	50%
Instrução - Restrições operativas em vigência	50%

Quarta falha de processo operacional: ocorrida em 2014. Manobra de alta complexidade e alta periodicidade. Nesta, em 3 (três) dos 22 (vinte e dois) passos houve falha de processo.

Na ocasião, durante o processo de parada da unidade U05 para atender condições do sistema elétrico, efetuou-se manobra de compatibilização do estado de seleção de fonte da unidade geradora na U04. Foi necessário parar a U04, que operava normalmente no sistema.

O relatório concluiu que:

a) as telas de supervisão de ambas as unidades são praticamente iguais, à exceção da identificação da unidade geradora. *Variabilidades: Ambiente de manobra - Similaridade com outro ambiente de manobra*.

b) o operador executou a manobra sozinho, portanto não confirmou os passos da manobra com nenhum outro operador. *Variabilidades: RH - Disponibilidade de recursos humanos e Operador - Necessidade de confirmar o passo.*

As variabilidades na Tabela 18 são as da Tabela 13; as realçadas estavam presentes na ocasião e foram determinantes para o resultado indesejado. Instrução específica que incentive e controle a confirmação dos passos da manobra, ação proposta na Tabela 14 como resposta à variabilidade "Operador – Necessidade de confirmar o passo", diminuiria consideravelmente a probabilidade de esta falha ter ocorrido.

Tabela 18 Variabilidades na segunda falha operacional de 2014

ALTA COMPLEXIDADE	
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	76%
Equipamento de manobra - Funcionamento	74%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	74%
RH - Disponibilidade de recursos humanos	67%
Operador - Necessidade de confirmar o passo	64%
Instrução - Restrições operativas em vigência	64%
ALTA PERIODICIDADE	
Equipamento de manobra - Funcionamento	61%
Operador – Conhecimento	57%
Ambiente de manobra - Similaridade com outro ambiente de manobra	57%
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	50%
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)	50%
Instrução - Restrições operativas em vigência	50%

Sem levar os percentuais em consideração, a Tabela 19 mostra as variabilidades que atuaram nas quatro falhas de processo entre 2006 e 2015.

Tabela 19 Resumo das variabilidades nas quatro falhas

Falha 1: ***Ocorrência de 2010***	***Falha 2:*** ***Ocorrência de 2008***	***Falha 3:*** ***1a.ocorrência de 2014***	***Falha 4:*** ***2a.ocorrência de 2014***
Baixa complex / alta periodic	**Alta complex / baixa periodic**	**Alta complex / alta periodic**	**Alta complex / alta periodic**
Ambiente de manobra - Situações que tiram a atenção do operador (telefone/alarme)			
Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes		Ambiente de manobra - Situações de urgência/emergência/trabalhos concomitantes	
	Ambiente de manobra - Similaridade com outro ambiente de manobra		Ambiente de manobra - Similaridade com outro ambiente de manobra
	Operador - Necessidade de confirmar o passo	Operador - Necessidade de confirmar o passo	Operador - Necessidade de confirmar o passo
Operador - Conhecimento			
Equipamento de manobra - Funcionamento	Equipamento de manobra - Funcionamento	Equipamento de manobra - Funcionamento	
		RH - Disponibilidade de recursos humanos	

Apesar de terem sido falhas totalmente diferentes em termos circunstanciais, notam-se algumas similaridades que corroboram algumas das conclusões tomadas a partir da Tabela 13, repetidas aqui com os resumos das conclusões dos relatórios de falhas:

a) *O "ambiente de manobra" é uma categoria de significativa importância em todas as situações de complexidade e periodicidade*. Os relatórios apontaram que em todas as falhas houve influência fundamental do ambiente de manobra, corroborando essa conclusão;

b) *O "conhecimento do operador" não aparece como uma das principais variabilidades a afetar as manobras de alta complexidade e de baixa periodicidade*. De fato, os relatórios apontaram que nos casos das falhas 2, 3 e 4 todos os envolvidos tinham pleno conhecimento do procedimento operacional, somente afetou a falha da manobra de alta periodicidade;

c) *À maior parte dos passos incide a variabilidade "Similaridade com outro ambiente de manobra"*. No caso em questão, em duas das quatro falhas ela se fez presente;

d) *A categoria "instrução" afeta de maneira mais significativa as manobras de baixa complexidade ou de baixa periodicidade*. Nestes casos, não se fez presente.

e) *Em manobras cuja periodicidade é baixa, muitas das variabilidades afetam praticamente todos os passos*. *A principal variabilidade a afetar a operação normal advém de situações que tiram a atenção do operador*. Nos casos em questão, as situações de emergência e a necessidade de confirmar os passos foram condições fundamentais para as falhas.

f) *Em manobras de alta complexidade, as duas variabilidades que mais afetam as funções ("Ambiente de manobra – Situações de urgência/emergência/trabalhos concomitantes" e "Equipamento de manobra – Funcionamento") são externas à operação, de forma que há pouco a propor como ação concreta da operação para diminuir suas influências na operação normal.* De qualquer forma, a análise dos relatórios provou que o mau funcionamento dos equipamentos de manobra e as situações de emergência/trabalhos concomitantes são condições básicas de falha. A operação deve manter a prioridade de seus sistemas de gestão do conhecimento e treinamentos para diminuir a influência destes nos resultados das manobras.

3.5 CONCLUSÃO

Este estudo procurou aplicar conceitos de Segurança-II a um conjunto de quatro manobras representativas de complexidade e periodicidade altas e baixas executadas pela operação da usina Itaipu Binacional. Para tal, foram estudados artigos relativos à abordagem de Segurança-II e aos métodos de aplicação de alguns dos princípios relacionados, para os quais o método FRAM, que se preocupa com as funções do sistema (aqui "passos" das manobras) e suas variabilidades, serviu de inspiração. Entrevistas com técnicos e engenheiros de operação da Itaipu Binacional determinaram a operação normal e as variabilidades que atuam nos passos destas manobras típicas. Verificou-se, com base neste levantamento, que as variabilidades que influenciam a operação são comuns aos tipos de manobra estudados.

A partir deste ponto, para cada passo de cada manobra foram marcadas as variabilidades que neles atuam e, uma vez tabulados os resultados, concluiu-se quais delas mais influenciam positiva ou negativamente a operação normal, de forma geral (para todas as manobras) e específica (para cada manobra representada no diagrama periodicidade/complexidade). Em seguida, foram propostas ações para diminuir a influência das principais variabilidades no resultado global da manobra. Complementando a abordagem, um comparativo entre a análise das variabilidades em situação normal com os relatórios de quatro falhas ocorridas entre 2006 e 2015 apontou que estes não necessariamente contribuem

para entender as variabilidades, uma vez que analisaram somente quatro das mais de dez mil manobras efetuadas no período. Mesmo assim, por terem tratado de casos reais de falha, fornecem subsídios ao estudo e à comparação dos resultados do estudo com as situações vivenciadas a fim de verificar aderência à realidade.

Concluiu-se, corroborando o estudo retrospectivo das quatro falhas supracitadas, que algumas variabilidades atuam de forma decisiva em praticamente todas as manobras. Dentre elas, as da categoria "ambiente de manobra", e a "necessidade de confirmar os passos das manobras". Ainda, concluiu-se que situações que tiram a atenção do operador ("telefone/alarme", "similaridade com outro ambiente de manobra", "situações de urgência/emergência/trabalhos concomitantes") atuaram nas falhas e também foram muito citadas na avaliação das manobras típicas tanto pelos técnicos quanto pelos engenheiros de operação. Por outro lado, o "conhecimento do operador" não foi mapeado como uma variabilidade fundamental presente nas falhas, o que o senso comum poderia indicar o contrário.

As comparações entre a operação normal e os casos de falha provou que o sucesso e a falha advêm da mesma fonte, princípio basilar do método, e aderente aos princípios de Engenharia de Resiliência. Identificadas as funções das manobras do estudo, foi possível mapear as variabilidades mais importantes a atuar sobre a operação normal, fornecendo subsídios à organização para a tomada de decisão antes de um evento de falha.

Tem-se como principais contribuições deste trabalho ao desenvolvimento da disciplina de segurança de ativos:

1) A constatação de que, para essa amostragem de manobras, as mesmas variabilidades influenciam nos passos operacionais, não importando a complexidade tampouco a periodicidade da manobra. O que muda é a presença ou não de tal variabilidade e o grau em que ela afeta a operação;
2) O registro histórico de dados de falha corroborou aspectos fundamentais do estudo;
3) A proposição de ações concretas a partir do levantamento das variabilidades, com o fim de dirimi-las. Estas ações são válidas em qualquer ambiente tecnológico, independem das mudanças tecnológicas.

3.6 REFERÊNCIAS

[1] M. Patterson and E. S. Deutsch, “Safety-I, Safety-II and Resilience Engineering,” *Curr. Probl. Pediatr. Adolesc. Health Care*, vol. 45, no. 12, pp. 382–389, 2015.

[2] J. Lundberg and B. J. E. Johansson, “Systemic resilience model,” *Reliab. Eng. Syst. Saf.*, vol. 141, pp. 22–32, 2015.

[3] T. Aven, “Foundational Issues in Risk Assessment and Risk Management,” *Risk Anal.*, vol. 32, no. 10, pp. 1647–1656, 2012.

[4] EUROCONTROL, “From Safety-I to Safety-II: A White Paper,” *Netw. Manag.*, pp. 1–32, 2013.

[5] A. P. Tochetto, R. J. G. C. da Silva, and J. B. Mota Jr., “O impacto no SIN-BR do desligamento de unidades geradoras na UHE-ITAIPU 60Hz e 50Hz,” in *XXII SNPTEE*, 2013.

[6] A. M. Madni and S. Jackson, “Towards a conceptual framework for resilience engineering,” *IEEE Syst. J.*, vol. 3, no. 2, pp. 181–191, 2009.

[7] E. Hollnagel, *Safety-I and Safety-II The Past and Future of Safety Management*, 1st ed. Farnham: Ashgate, 2014.

[8] F. Vanderhaegen, “Erik Hollnagel: Safety-I and Safety-II, the past and future of safety management,” *Cogn. Technol. Work*, vol. 17, no. 3, pp. 461–464, 2015.

[9] E. Hollnagel, R. L. Wears, and J. Braithwaite, “From Safety-I to Safety-II: A White Paper,” *Netw. Manag.*, p. 43, 2015.

[10] CENIPA, “Relatório Final A–067/CENIPA/2009,” 2009.

[11] I. G. Belash, “Hydrotechnical construction: Causes of the failure of the no. 2 hydraulic generating set at the Sayano-Shushenskaya HPP: Criticality of reliability enhancement for water-power equipment,” *Power Technol. Eng.*, vol. 44, no. 3, pp. 165–170, 2010.

[12] EUROCONTROL, “Ensuring Safe Performance in ATC Operations: Observational Safety Survey Approaches - A White Paper,” 2011. [Online]. Available: https://www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-white-paper-20111.pdf. [Accessed: 11-Feb-2016].

[13] E. Hollnagel, J. Hounsgaard, and L. Colligan, *FRAM – the Functional Resonance Analysis Method - A handbook for the practical use of the method*, 1st ed., no. june. Middelfart, Denmark, 2014.

[14] A. W. Righi, T. A. Saurin, and P. Wachs, “A systematic literature review of resilience engineering: Research areas and a research agenda proposal,” *Reliab. Eng. Syst. Saf.*, vol. 141, pp. 142–152, 2015.

[15] C. Nemeth, “Erik Hollnagel: FRAM: The functional resonance analysis method, modeling complex socio-technical systems,” *Cogn. Technol. Work*, pp. 117–118, 2012.

[16] D. D. Woods, *Essential Characteristics of Resilience*, 1st ed. Hampshire: Ashgate, 2006.

4 COMENTÁRIOS FINAIS

Este capítulo apresenta as conclusões do trabalho e sugere algumas abordagens sobre o tema para trabalhos futuros.

4.1 CONCLUSÃO

Esta dissertação teve como tema a Engenharia de Resiliência (ER), uma nova visão de segurança, proativa, ou Segurança-II, suplementar à gestão de segurança tradicional, ou Segurança-I, baseada em análises retrospectivas de falha e no estado estático de componentes e sistemas. Para tal, duas foram as abordagens, distintas, porém sob os mesmos princípios: a aplicação de conceitos e heurísticas de ER para complementar uma análise de risco tradicional de incêndio em um transformador da usina hidrelétrica Itaipu Binacional, e a aplicação de conceitos de Segurança-II, umbilicalmente ligada à Engenharia de Resiliência, a quatro manobras típicas executadas pelos operadores da usina. Em ambos os casos, a experiência e o conhecimento do *staff* operacional foram a base sobre a qual foi a estrutura da pesquisa foi montada.

Retomando os objetivos do trabalho, propôs-se, no primeiro artigo, um método para quantificar a resiliência da organização para o caso específico da explosão de um dos transformadores principais da usina, método que pode ser aplicado em outras contingências críticas. Considerando que é difícil para uma empresa migrar diretamente da Segurança-I para a Segurança-II, foi proposta a suplementação da análise de risco tradicional com elementos de ER, aderentes às habilidades que uma organização que se pretenda resiliente deve apresentar: Monitorar, Aprender, Responder e Antecipar. Apesar das abordagens da ER serem de cunho preferencialmente qualitativo, concluiu-se ser possível desenvolver métodos para quantificação das habilidades de resiliência de uma organização.

No segundo artigo, procurou-se avaliar, com base em resultados históricos, as relações entre sucessos e falhas operacionais e a aderência da teoria de Segurança-II às falhas operacionais havidas nos últimos dez anos na Itaipu Binacional. Para isso, foram apresentados conceitos e técnicas da visão de Segurança-II, uma abordagem que foca o estudo da segurança no “que dá certo”, na operação normal, estudados e aplicados a quatro manobras executadas pela operação da Itaipu Binacional, categorizadas por periodicidade e complexidade. Foram

levantadas a operação normal de tais manobras e as variabilidades que incidem nos passos executados pelos operadores. Para cada passo de cada manobra foram marcadas as variabilidades que neles atuam e, uma vez tabulados os resultados, analisado quais delas mais influenciam a operação normal. Concluiu-se que há variabilidades que atuam de forma decisiva em praticamente todas as manobras. A análise histórica das quatro falhas ocorridas no período de 2006 a 2015 apontou que o sucesso e a falha advêm da mesma fonte, e que algumas variabilidades como "ambiente de manobra", a "necessidade de confirmar os passos das manobras" e situações que tiram a atenção do operador atuam de forma decisiva em praticamente todas as manobras. Por fim, foram propostas ações para diminuir a influência das variabilidades no resultado global da manobra, destacando que os relatórios de falhas não necessariamente contribuem para entender as variabilidades, uma vez que analisaram somente quatro das mais de dez mil manobras efetuadas no período

4.2 SUGESTÕES PARA TRABALHOS FUTUROS

O tema Engenharia de Resiliência é ainda incipiente e mesmo as definições a respeito ainda carecem de solidez. No campo teórico, autores como Eric Hollnagel, David Woods, Nancy Leveson e outros desbravam o caminho e tentam estabelecer as bases teóricas do que se entende como uma nova visão de segurança proativa. No entanto, a prática de uso é o que vai consolidar ou não a teoria. Desta forma, aplicações como a deste estudo não são pontos finais, mas apenas pontos de partida para que, em um futuro, uma efetiva gestão de segurança operacional e de ativos seja baseada em abordagens proativas, suplementares à gestão tradicional.

De maneira específica, pode-se citar algumas sugestões para trabalhos que sigam esta mesma linha de estudo:

1) Ampliar o leque de manobras estudadas sob o ponto de vista de Segurança-II, partindo das variabilidades definidas neste estudo, a fim de corroborar os resultados quanto as variabilidades para mais manobras, ajustando-as caso necessário;
2) Utilizar métodos de estabelecimento de pesos para as citações das variabilidades, para aprimorar seu ranqueamento, priorizando as ações de combate às variabilidades que mais afetam a operação;
3) Com vistas à atualização tecnológica das instalações, imaginar, com o auxílio de operadores diretos e indiretos, o que seria a "operação normal" neste novo contexto de

operação e delinear as variabilidades antecipadamente, no que for possível, bem como propor ações para dirimi-las antes mesmo de os novos sistemas entrarem em operação;

4) Desenvolver um painel de segurança operacional que monitore em tempo real as ameaças críticas ao sistema – instalações, pessoas, meio ambiente –, utilizando métodos de BI (*Business Intelligence*) para capturar os dados da planta e cujos indicadores sejam baseados nos princípios, conceitos e heurísticas de ER.

REFERÊNCIAS

AVEN, T. Foundational Issues in Risk Assessment and Risk Management. **Risk Analysis**, v. 32, n. 10, p. 1647–1656, 2012.

AZADEH, A. et al. Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. **Safety Science**, v. 68, p. 99–107, out. 2014.

FOGLIATTO, F. S.; GUIMARÃES, L. B. M. Design Macroergonômico: uma proposta metodológica para projeto de produto. **Produto & Produção**, p. 1–15, out. 1999.

HALE, A.; HEIJER, T. Defining Resilience. In: HOLLNAGEL, E.; WOODS, D. D.; LEVESON, N. G. (Eds.). . **Resilience Engineering: Concepts and Precepts**. 1. ed. Burlington: Ashgate, 2006. p. 35–40.

HASSAN, J.; KHAN, F. Risk-based asset integrity indicators. **Journal of Loss Prevention in the Process Industries**, v. 25, n. 3, p. 544–554, 2012.

HOLLING, C. S. Resilience and Stability of Ecological Systems. **Annual Review of Ecology and Systematics**, v. 4, n. 1, p. 1–23, 1973.

HOLLNAGEL, E. **Safety-I and Safety-II: The Past and Future of Safety Management**. Boca Raton, FL: CRC Press, 2014.

HOLLNAGEL, E.; WEARS, R. L.; BRAITHWAITE, J. From Safety-I to Safety-II: A White Paper. **Network Manager**, p. 43, 2015.

ITAIPU BINACIONAL. **Participação nos mercados**. Disponível em: <https://www.itaipu.gov.br/energia/participacao-nos-mercados>. Acesso em: 20 fev. 2016a.

ITAIPU BINACIONAL. **Perfil Institucional | Visão**. Disponível em: <https://www.itaipu.gov.br/institucional/visao>. Acesso em: 26 nov. 2014b.

KRÖGER, W. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. **Reliability Engineering and System Safety**, v. 93, p. 1781–1787, 2008.

LABAKA, L.; HERNANTES, J.; SARRIEGI, J. M. Resilience framework for critical infrastructures: An empirical study in a nuclear plant. **Reliability Engineering and System Safety**, v. 141, p. 92–105, 2015.

PORTELA, J. C. et al. **Itaipu Binacional and its relationship with major blackouts in Brazilian power system**. Hydrovision Russia. **Anais**...Moscow: 2011

SÆTREN, G. B.; LAUMANN, K. Effects of trust in high-risk organizations during technological changes. **Cognition, Technology and Work**, v. 17, n. 1, p. 131–144, 2014.