BBR
BRAZILIAN BUSINESS REVIEW
Vol. 6, No.2
Vitória-ES, Mai – Ago 2009
p. 174-190 *ISSN 1807-734X* *DOI: http://dx.doi.org/10.15728/bbr.2009.6.2.4*

Organizações de Alta Confiabilidade e Administração de Risco Operacional

Janann Joslin Medeiros[†]
Universidade de Brasília

Wellington Pinto[Ω]
Faculdade do Meio-Ambiente e Tecnologia de Negócios – FAMATEC

RESUMO: Estudos da gestão do risco operacional em instituições financeiras utilizam abordagens predominantemente quantitativas e probabilísticas. Tais abordagens permitem estimar a probabilidade da ocorrência de falha operacional, mas não fornecem pistas sobre ações de gestão específicas a serem tomadas para evitar que a falha aconteça. Os resultados do presente estudo dos processos de uma grande instituição financeira brasileira sugerem que a teoria de Organizações de Alta Confiabilidade (OAC) pode contribuir à efetiva gestão do risco operacional. Compreensão dos mecanismos causais de falhas operacionais torna possível sua gestão e a redução da probabilidade de ocorrerem. Além de sugerir uma nova abordagem à gestão do risco operacional em instituições financeiras, o estudo testou a teoria de OAC em setor não previamente pesquisado. Os resultados demonstram claramente que os conceitos da teoria OAC têm relevância para instituições financeiras, ampliando o escopo dessa teoria.

Palavras-chave: organizações de alta confiabilidade; gestão de risco operacional; instituições financeiras.

Recebido em 23/12/2008; revisado em 28/06/2009; aceito em 29/08/2009.

Correspondência com autores*:

[†] *Professora da Universidade de Brasília*
Endereço: ICC Norte, Módulo 25 subsolo Veiga, Brasília- DF – Brasil - CEP: 70910-900, e-mail: janann@unb.br
Telefone: (61) 3307-2545

[Ω] *Coodenador na Faculdade do Meio-Ambiente e Tecnologia de Negócios*
Endereço: SQN 404, BLOCO N, Brasília – DF – Brasil - CEP: 70845-140, e-mail: wellington.pinto@caixa.gov.br
Telefone: (61)3222-7308

Nota do Editor: *Este artigo foi aceito por Antonio Lopo Martinez.*

1. INTRODUÇÃO

O Comitê de Basel de Supervisão Bancária foi criado com a missão de estabelecer padrões de operações para a minimização de riscos e a provisão de maior estabilidade para o sistema financeiro global. Em 1988 este Comitê publicou a Convergência Internacional de Medida de Capital e Padrões de Capital (BIS, 1988), contendo um jogo de diretrizes para minimizar os riscos de organizações financeiras e garantir que eles têm níveis mínimos de solvência e liquidez, enquanto estabelecendo limites seguros para operações e criando padrões uniformes. Após a publicação destes padrões e a adoção das medidas preventivas contida no documento, porém, casos que envolvem problemas de risco ocorreram em instituições financeiras, primeiramente entre eles sendo o caso do Barings Bank. Esta instituição financeira tradicionalmente inglesa falhou devido à perda de £869 milhão de operações realizadas por um empregado.

Este caso revelou que o Barings Bank teve deficiências em seus processos internos, falhas em seus controles internos e falta de mecanismos para proteger contra fraude interna, situações não contempladas no documento de 1988. Em conseqüência, o banco não pôde descobrir e corrigir estes problemas a tempo para prevenir conseqüências desastrosas para seu patrimônio (REASON, 1997). O caso de Barings, infelizmente, não era um caso isolado. O Marshall (2001) apresenta vários outros exemplos de amplas perdas financeiras vindas de resultados de fraudes e falhas de processos internos.

Ao analisar estes tipos de problemas, o Comitê de Basel percebeu que era necessário especificamente lidar com os fatores de risco que os geram: fracasso humano, fracassos de sistemas e fracassos de processo, fraudes e eventos externos. Estes fatores estavam definidos como risco operacional e em 2004, uma nova Convergência Internacional ou Basel II (BIS, 2004) foi adotado que contemplou, entre outras medidas, exigindo instituições financeiras administrar o risco operacional como uma forma de proteção contra perdas inesperadas em seus processos empresariais e a realização de maior efetividade em suas operações.

Instituições financeiras começaram, então, a adotar medidas para cumprir com futuras demandas. Estas medidas, até hoje, são limitadas a estudos da probabilidade de perdas operacionais realizadas por meio de técnicas quantitativas com o objetivo de determinar a quantidade de capital que deveria ser alocado para cobrir potencias perdas operacionais. Não houve nenhum uso de estudos ou técnicas para avaliar como a organização administra suas operações como um modo de identificar ações preventivas ou corretivas para potencias fraquezas operacionais.

Uma revisão da literatura em risco operacional não revela nenhuma discussão acadêmica ou reflexões científicas de natureza empírica. Ao contrário, a bibliografia no assunto consiste predominantemente de métodos prescritivos, técnicas e modelos para uso através de organizações. Porém, há um corpo de literatura no campo de estudos de organização que buscam a prevenção e correção oportuna de faltas operacionais de Organizações de alta confiabilidade (OAC).

Confiabilidade é geralmente entendida como um desempenho perfeito apesar da exposição para condições adversas. As OAC são organizações que apesar de ter características como processos complexos, forte interdependência com outras organizações ou entre unidades da mesma organização, uso de tecnologias sofisticadas, necessidade de agir constantemente sob pressão e em ambientes sujeito a alto risco de acidentes de dimensões catastróficas experimentam poucas ocorrências negativas e possui estratégias consistentes para mitigar fracassos operacionais se caso acontecer (REASON, 2000). Em outras palavras, embora eles

funcionem em ambientes de alto risco e realizam operações de grande complexidade, as OAC têm um desempenho operacional superior, com uma incidência de erro que se aproxima a zero.

Estudos em OAC começaram com a pesquisa em acidentes normais administrados por Perrow nos anos oitenta relacionados a processos complexos que envolvem tecnologias arriscadas (FORD et al., 2003). Perrow (1999) afirma que acidentes penetram organizações como resultado de junção apertada, falta de controle e complexidade operacional. Junção apertada é entendida como a impossibilidade de demorar ou adiar operações de processo, seqüência de processo invariável e caminhos únicos para alcançar objetivos, pouca flexibilidade em materiais, equipamento e pessoal e pouco tempo para corrigir tais fracassos que pode acontecer por acaso. A falta de controle está relacionada à ausência de planos de contingência se caso fracassos venham acontecer; enquanto operações complexas são caracterizadas por interconexões múltiplas entre partes de componente, unidades ou subsistema, rotinas de avaliação inexistente ou não-pensadas, uma variedade de parâmetros para controle de interações potenciais, fontes de informação indiretas ou deduzíveis e compreensão limitada de alguns processos (PERROW, 1999, p. 85-86).

Perrow (1999) observa que não há nenhuma tal coisa como um humano perfeito ou componente mecânico. Por isto, como pondera o REASON (1997), sistemas complexos têm necessidade de ter dispositivos de segurança como controles redundantes ou estendidos em camadas. Porém, processos complexo e firmemente acoplado têm seus mecanismos de segurança redundantes unidos um ao outro. Isto pode reduzir a confiança ao em vez de aumentar, principalmente fazendo estes mecanismos e seus inter-funcionamentos mais complexo (SAGAN, 2004). Além disso, a adoção de redundância em mecanismos de segurança freqüentemente leva os gerentes a colocar mais pressão até mesmo em processos de produção porque eles depositam confiança não comprovada na segurança oferecida e porque eles buscam aumento de resultados para compensar pelo investimento feito nestes mecanismos (SAGAN, 2004).

A pesquisa de Perrow estimulou a investigação de como algumas organizações conseguem manter padrões altos de segurança operacional apesar da complexidade e junção apertada de seus processos. Foi feita uma pesquisa inicial para identificar organizações que pertencem a este grupo e analisar como eles se estruturavam e administravam suas operações para atingir níveis de erro próximo ao zero esta pesquisa foi realizada com a Marinha Americana (ROBERTS; LIBUSER, 1993). Estes estudos sublinharam a importância de aprender sobre organizações que operam debaixo de condições adversas, mas têm um número de acidentes inferior ao nível esperado (FORD et al., 2003; ROBERTS; LIBUSER, 1993).

O estudo atual investiga a relação entre as características das Organizações de alta confiabilidade e as exigências para administração de risco operacional em instituições financeiras esboçadas pelo Comitê de Basel. Seu objetivo é identificar, desta perspectiva de estudo organizacional, o que poderia ser as causas prováveis de fracassos operacionais experimentadas por uma grande instituição financeira e avaliar se teorias sobre alta confiabilidade têm como contribuir à administração efetiva de risco operacional. Para estudar estas perguntas, dois processos nos quais fracasso operacional foi experimentado foram estudados em uma grande instituição financeira brasileira chamada, para propósitos deste estudo, o Banco Zeta.

Perrow (1999) observou que, apesar de que nenhum estudo ter sido realizado no setor, o sistema financeiro é um campo óbvio para realizar estudos sobre acidentes organizacionais, dado o volume alto, a complexidade e o acoplamento apertado das operações e de

instrumentos financeiros; e a literatura da OAC sugestiona a aplicabilidade de seus conceitos no setor bancário. (Veja, por exemplo, Roberts e Rousseau, 1989; Reason, 1998; e Vogus, 2003.) Porém, nenhum prévio estudo empírico especificamente investigou esta possível aplicabilidade.

Este estudo investiga a aplicabilidade dos conceitos de alta confiabilidade à administração de risco operacional através de instituições financeiras.

2. ALTO RISO E ALTA CONFIABILIDADE

De acordo com a literatura, as OAC exibem características que expõem suas operações a altos risco de fracassos, junto com características que promovem alta confiabilidade como uma forma de prevenir ou amolecer o impacto de ocorrências desastrosas.

O Roberts e Rousseau (1989) identificam as seguintes características de alto risco:

- hiper-complexidade: uma grande variedade de componentes, sistema e níveis.
- acoplamento apertado: interdependência entre unidades e níveis que não permitem esperas ou demoras entre uma atividade e outra ou variações na seqüência de procedimentos.
- intervalos curtos entre atividades**:** normalmente as atividades principais acontecem em intervalos medidos em segundos;
- ocorrência simultânea de operações críticas**:** ocorrência de várias operações complexas ao mesmo tempo, sem possibilidade de interromper qualquer deles (partidas e aterrissagens em aeroportos, por exemplo).

Bea e Moore (1993) indicam que a confiança organizacional freqüentemente é arruinada por metas ambiciosas de produção que fazem os operadores desconsiderar procedimentos de segurança. Confiabilidade, de acordo com estes autores, também chega a um acordo quando a administração de cúpula, quando está sob pressões de custo, não fornece recursos necessários para a promoção de segurança operacional. Como resultado, acidentes acontecem devido a uma combinação de falha humana (imprudência, falta de atenção), fracasso de sistema (falta de mecanismos preventivos ou mecanismos para alerta, descoberta e controle) e fracasso organizacional (supervisão inadequada, treinamento deficiente).

Embora eles exibam características de alto risco, as OAC têm outras características que reduzem a probabilidade da ocorrência de amplos fracassos, enquanto os diferenciando de outros tipos de organização. De acordo com Rochlin (1993), estas características são:

- a convicção que falhas podem ocorrer em qualquer lugar e que vigilância constante é o preço do sucesso;
- que os mecanismos monitorados são constantemente renovados e reanalizados, dado o fato que as fontes de erro são dinâmicas;
- a convicção que o ambiente operacional é uma fonte constante de ameaça e requer vigilância permanente;
- manutenção de modos redundantes de resolver problemas ao nível operacional e resistência a pressões para agilizar processos;
- criação, manutenção e uso de soluções contingentes organizacionais;
- compromisso organizacional para o uso de medidas preventivas como também medidas reativas para confrontar problemas reais e potenciais;
- treinando e provendo unidades organizacionais envolvidas no processo com autonomia para procurar e preparar para problemas reais como também

procurar pontos fracos ocultos em processos organizacionais que, em interação com certos tipos de condições, pode causar perdas organizacionais;
- relutância para testar os limites de confiabilidade;
- obediência para regras formais e códigos de conduta.

Os gerentes superiores das OAC consideram a segurança tão importante quanto à produtividade e concentram parte de seus esforços na redução de riscos potenciais (GRABOWSKI; ROBERTS, 1997; LALLY, 2002; ROBERTS; LIBUSER, 1993). A característica mais importante de um OAC é a preocupação coletiva com a possibilidade de erro. A administração superior acredita que enganos sempre acontecerão e treinarão sua mão-de-obra para reconhecê-los e estar preparado para eles. (REASON, 2000)

Weick e Sutcliffe (2001) caracterizam as OAC como estando em um estado de alerta constante para eventos inesperados que podem causar impactos negativos em suas rotinas. Este estado é alcançado por:

- preocupação constante para erro, análise constante de qualquer e todos os tipos de erros e tratamento de qualquer descuido como um sintoma que algo não vai dar certo;
- relutância para simplificar rotinas, visto na tentativa de entender cada fase das atividades complexas e manter as fases separa para permitir administração imediata se problemas acontecerem;
- sensibilidade para procedimentos operacionais, planejado para constantemente avaliar processos operacionais para identificar fatores com o potencial de causar erro;
- compromisso para com o funcionamento operacional, pelo estabelecimento de planos de contingência para manutenção de operações e baseado na premissa que não há nenhum sistema ou procedimento que sempre trabalham perfeitamente;
- respeito e consideração para profissionais altamente qualificados**,** comprovado pelo encorajamento da tomada de decisões para solução de problema por especialistas no assunto, independentemente de seu nível na hierarquia.

Para Weick e Sutcliffe (2001), os primeiros três destas características criam um estado de agilidade e preocupação pelo inesperado enquanto os últimos dois promovem condições para conter tais eventos quando acontecerem. Em resumo, eles atribuem o sucesso das OAC aos constantes esforços pelos sócios em agir efetivamente em face de eventos inesperados. Eles acreditam que as OAC são organizadas de tal modo que os operadores podem reconhecer e avaliar tais eventos, enquanto freando sua evolução ou restabelecendo o funcionando operacional, se necessário. A que diferencia as OAC de outras organizações não é a prevenção do inesperado, mas a habilidade para agir imediatamente, nas fases iniciais de uma ocorrência inesperada, quando há só uma sugestão que algo poderia estar errado.

A cultura organizacional pode ser definida como as convicções compartilhadas e valores que interagem com estruturas organizacionais e controlam sistemas para produzir normas de comportamento (REASON, 1997:192). Uma cultura organizacional orientada para alta confiabilidade contém certos elementos fundamentais (REASON, 1997; WEICK; SUTCLIFFE, 2001):

- comportamentos que buscam dirigir atividades para maximizar segurança, independente de pressões empresariais;
- a manutenção de altos e constantes níveis de preocupação com fraquezas

operacionais;

- apoio para a coleção e estudo de dados sobre acidentes e situações onde perdas quase aconteceram; até mesmo na ausência de fracassos amplos;
- manutenção, incentivo para e disseminação de mecanismos para comunicação de erros individuais;
- definição das medidas administrativas a serem adotadas no caso de acontecerem comportamentos não-aceitáveis. Estes são feito claro para todos os sócios da organização;
- procedimentos por adaptar-se a uma variedade de situações de crise, com flexibilidade de estrutura e do processo decisório;
- modos de trazer toda a informação para agüentar a chegada de conclusões sobre o melhor modo para programar segurança operacional.

Segundo as indicações da Tabela 1, uma revisão das literaturas respectivas sugere que muitas das condições identificadas na literatura da OAC como contribuindo a acidentes são semelhantes ou idênticos às causas de exposição aos riscos operacional identificado na literatura de risco operacional.

Tabela 1 - Comparação das Causas de Situações de Risco

Causas de risco operacional identificadas na literatura de risco operacional	Condições que contribuem para acidentes, identificadas na literatura da OAC.
Falha humana	Fator humano: falta de atenção, esquecimento, motivação pobre, descuido, falta de habilidade ou conhecimento, negligência (REASON, 1997).
O humano e a falha de sistema	Fator técnico: relação entre as pessoas e tecnologia (REASON, 1997).
Falha de processo	Fator de organização: processos inadequados ou orçamentos; conflitos de interesse; treinamento insuficiente ou inexistente (REASON, 1997).
Falha de sistema	Inovações tecnológicas (LALLY, 2002).

Uma diferença conceitual fundamental entre as duas literaturas é perceptível, porém, a literatura da OAC trata falha humana, falhas técnicas e organizacionais como *conseqüências* de "postura organizacional", de como a organização se trata dos vários fatores de risco. No caso da literatura de risco operacional, o humano e os erros técnicos são considerados as *causas* de risco deles mesmo. O foco está em projetar a probabilidade que eles poderem ocorrer ao invés de criar medidas para evitar sua ocorrência.

3. MÉTODOS

Baseado nos locais sobre confiabilidade organizacional oferecidos por Weick e Sutcliffe (2001) e Roberts e Libuser (1993), um modelo conceitual para análise foi desenvolvido consistindo em cinco variáveis ao longo de três dimensões: ambiente (clima organizacional e cultura e trabalhando condições); pessoas (atitudes e competência); e processos.

Dois processos organizacionais do Banco Zeta: administração do Sistema brasileiro de Pagamentos (SBP) e administração de Operações de Crédito foi estudada com uma visão para

identificar possíveis causas de exposição a risco operacional como definida por BIS (2004): falha humano, falha de processo, falha de sistema, fraude humana ou evento externo.

Estes processos específicos foram selecionados em base do volume de recursos envolvido e o número de transações diárias realizadas, como também a disponibilidade de dados e a possibilidade de manter confidência com respeito à identidade da organização.

Avaliar a exposição ao risco oferecida pelo variável "clima organizacional e cultura", o indicador usado foi "existência de recompensa ou castigo relacionada a erro." Além disso, foram buscadas indicações de evidência da presença de características de uma cultura de alta confiabilidade. Para investigar a variável "condições de funcionamento", dois indicadores foram utilizados: existência de pressões e suficiência de recursos. Para avaliar "atitudes", quatro indicadores foram utilizados: percepção, responsabilidade, proatividade e reatividade. Os indicadores utilizados para avaliar os riscos posados por "competência" foram aprendizados, treinamentos e conhecimentos. Baseado no Roberts e Rousseau (1989), Rochlin (1993) e Bea e Moore (1993), como discutido na seção anterior, foram utilizados seis indicadores para avaliar a exposição ao risco oferecido através de processos: acoplamento apertado, complexidade, constante ação humana, habilidade para voltar a normal funcionar, ocorrência de eventos inesperados e supressão de rotinas de segurança.

A pesquisa foi realizada por meio da aplicação de um questionário, observação não-participante e pesquisa documentária. Foram utilizados esboços de tópico, desenvolvidos dos conceitos utilizados no modelo analítico, para guiar a observação não-participante e a pesquisa documentária. A pesquisa documentária foi utilizada para colecionar dados com respeito a perdas e falhas operacionais e traçar os processos sendo analisados. Os documentos revisados eram documentos internos de Banco Zeta que se tratava de processos de banco nos quais perdas operacionais tinham sido ocorridas. Os respondentes do questionário foram os empregados do Banco Zeta envolvidos com os dois processos escolhidos para um estudo mais íntimo: sete que trabalham com administração do SBP e doze envolvido com administração de operações de crédito. A observação de não-participante foi realizada em cima do curso do projeto de pesquisa para fornecer um meio de verificar informação sobre processos contido nos documentos revisados e percepções de operadores obtidas por meio de questionário. Além disso, devido a certos pontos de vista expressos em respostas ao questionário, uma entrevista foi administrada com o gerente da Unidade de Tecnologia para entender como estes assuntos se apareceram em sua perspectiva.

Para análise dos dados, foram desenvolvidos fluxogramas dos processos estudados. Além disso, a técnica de combinar padrões foi utilizada analisando os dados nos quais comparações foram feitas entre os padrões das variáveis observados empiricamente e os padrões esperados em base a estrutura teórica utilizada (YIN, 2001).

4. RESULTADOS

Nesta seção, apresentamos os resultados nos processos selecionados para análise no Banco Zeta - administração do SBP e administração de Operações de Crédito.

Administração do sistema brasileiro de processo de pagamentos (SBP). A implantação de um novo Sistema de Pagamento brasileiro (SBP) aconteceu em abril de 2002. O objetivo principal do novo sistema era fazer a transferência de recursos entre os clientes e usuários de diferentes bancos mais ágil e seguro. A mudança mais notável provocada pelo SBP foi a introdução de um instrumento chamado Transferência Eletrônica Disponível (TED,

de suas rubricas em português), utilizada para efetuar transferência on-line de recursos entre bancos. O sistema funciona assim como se o cliente fizesse um deposito em dinheiro diretamente na conta de outro cliente que assim tem o dinheiro imediatamente disponível.

O novo sistema diminuiu o tempo durante o qual o dinheiro envolvido nas transações foi bloqueado e diminuiu os riscos de crédito assumidos por empresas empresariais, dado o fato que, diferente dos cheques que podem ser segurados ou ser devolvidos por falta de fundos, os TED são irreversíveis.

O objetivo do SBP era como um todo a melhoria da segurança do sistema financeiro. No sistema anterior, contas bancárias só eram atualizadas a cada 24 horas e, no caso de falha de alguma instituição financeira, era impossível desfazer todas as operações que já tinham sido realizadas sem prejudicar a solvência de outras instituições financeiras. O Banco Central brasileiro, ou os contribuintes brasileiros, tinham que absorver as despesas de tais falhas bancárias.

Debaixo do novo sistema, pagamentos são feitos individualmente, e somente se o banco no qual a transferência foi retirada tem fundos suficientes para cobrir a quantia. Deste modo, se um banco não tiver recursos disponíveis para honrar seus compromissos, deverá de deixar de operar naquele exato momento e assim não gerará riscos adicionais para outros bancos, para o Banco Central, para investidores ou para a sociedade.

Riscos operacionais. Nas primeiras semanas de funcionamento do SBP, um cliente transferiu R$11.071.333.34 do Banco Zeta para outro banco, mas a ligação de comunicação com o sistema do Banco Central estava abaixo. Isto criou uma reserva de mensagens a serem enviadas por meio do sistema de apoio perto da hora do fechamento estabelecida pela agência reguladora, gerando pressões para cumprir o prazo final estatutário. O procedimento contingente requer que um empregado do banco que usa um sistema manualmente entre na quantia da transferência e um empregado que utiliza um sistema diferente libere esta quantia.

Na liberação da quantia a ser transferida, o primeiro sistema forneceu toda a informação com respeito à operação, inclusive a quantia. Porém, este sistema não registra o período que separa centavos de *reais* (a moeda atual brasileira). O segundo sistema difere do primeiro no que requer que um período seja colocado antes dos centavos. Se isto não for feito, o sistema interpreta todos os dígitos como *reais*.

O primeiro empregado digitou a quantia correta, mas conforme o requerimento de sistema, não digitou um período antes dos centavos. No momento da confirmação deste valor, dado a proximidade do prazo final e a importância da quantia e do cliente, o segundo empregado inspecionou a quantia na tela de seu computador e telefonou a unidade que tinha solicitado a transferência antes de confirmar a operação. Confirmando que a quantia digitada (R$ 110713334) correspondia à quantia de R$ 1107133,34 solicitada, o segundo empregado apertou o *entra* na qual o sistema somou 00 automaticamente à quantia digitada, enquanto transformando R$ 11,071,333.34 em R$ 1,107,133,334.00. Isto criou um equilíbrio negativo na conta bancária do Banco Central de R$ 364,573,906.78 (trezentos e sessenta e quatro milhões, quinhentos e setenta e três mil, novecentos e seis *reais* e setenta e oito centavos).

A equipe que monitora o saldo da conta com o Banco Central descobriu o engano, mas o sistema do Banco Central já tinha fechado. A única alternativa era pedir que o banco receptor devolvesse a transferência no próximo dia. Isto aconteceu depois que fosse autorizado pelo o partido que recebeu a transferência, mas gerou o pagamento de custos para o Banco Central para o "empréstimo", na quantia de R $ 427.078,86 (quatrocentos e vinte e sete mil e setenta e oito *reais* e oitenta e seis centavos).

Podem ser observados vários fatores identificados na literatura da OAC como potenciais promotores de acidentes organizacionais neste caso: novos sistemas novos; pressão para cumprir prazos finais; interação de sistema-humano; treinamento inadequado; acoplamento apertado; falha de sistema; falha de procedimentos defensivos.

Ambiente. O prazo final estabelecido pelo Banco Central para concluir as operações de dias é o elemento negativo principal informado para este processo por respondentes do questionário. Porém, esta pressão de prazo final só fica inquieta quando houver um problema com o funcionamento dos sistemas para enviar e receber mensagens ou quando confirmação de mensagens está pendente devido a problemas de inscrição dentro do banco.

Dado o fato que o processo é predominantemente automatizado, não pode ser deduzido que o ambiente, como regra geral, posa alto risco para a organização com respeito a este processo. Porém, a situação muda quando a falha de sistema causa utilização de procedimentos contingentes e estes procedimentos contingentes envolvam manipulações manuais – uma situação de risco mostrada por Bea e Moore (1993), Perrow (1999), Razão (1997) e Weick e Sutcliffe (2001).

Com respeito ao clima organizacional e cultura, foi informado que nenhuma recompensa ou nenhum castigo aconteceu com respeito aos erros operacionais nos processos do SBP e que procedimentos são para lidar com erros e falhas que permitem livre expressão de opiniões. No entanto, exemplos citados tratavam exclusivamente de informar o incidente à unidade responsável ou para um superior hierárquico. A observação não-participante revelou que enquanto empregados que falam abertamente sobre erros operacionais causados por ou acontecidos em outras unidades da organização, são extremamente relutantes em comentar sobre os que aconteceram em suas próprias unidades. Isto indica um clima organizacional pouco propício para lidar abertamente com perguntas de segurança operacional. Características de uma cultura de alta confiabilidade postuladas por Reason (1997)--como um modo sistemático de localizar e disseminar falhas ativas ou fraquezas ocultas ou a existência de medidas administrativas claras a serem adotadas no caso de — comportamento não-aceitável não foi observado. Os dados colecionados e analisados não oferecem nenhuma evidência que os tipos de comportamentos, convicções ou valores estão presentes que formaria uma cultura organizacional de alta confiabilidade nas condições de Grabowski & Roberts (1997) e Reason (1997), ou que comportamentos existem para dirigir atividades para um máximo de segurança, independente de pressões empresariais.

Pessoas. Este fator foi investigado em termos de nível de consciência do potencial para ameaças para segurança operacional, sentimentos de responsabilidade para a segurança de operações, pro atividade com respeito a fraquezas operacionais e reatividade (habilidade para reagir adequadamente a ameaças quando identificada).

As OAC podem ser caracterizadas, entre outras coisas, por obediência para regras formais e códigos de conduta e pela convicção que o ambiente de funcionamento é uma fonte constante de ameaça (ROCHLIN, 1993). Os participantes no processo demonstram *consciência* do fato que a organização é assunto a eventos inesperados que têm o potencial de causar perdas operacionais, mas eles não evidenciam a convicção que as pessoas seguem normas estabelecidas e rotinas sempre corretamente.

Embora o processo de SBP seja visto como suscetível para eventos inesperados, os empregados não percebem sua unidade organizacional específica ou eles mesmos como tendo responsabilidade por segurança operacional, invariavelmente transferindo esta

responsabilidade a outras unidades da organização, especificamente para a Unidade de Tecnologia. Isto denota uma falta de compromisso pessoal à segurança operacional. Tal compromisso e a suposição de responsabilidade pessoal existem em OAC (WEICK; STUCLIFFE, 2001; ROCHLIN, 1993).

Com respeito à responsabilidade da Unidade de Tecnologia para falhas no processo, alegado por esses envolvidos no processo de SBP, o gerente responsável pela Unidade de Tecnologia declarou que há quase 500 sistemas que funcionam no Banco Zeta. Alguns são bastante velhos e lentos, mas seu uso é exigido pelas unidades empresariais do banco. Entre as responsabilidades administrativas das unidades empresariais é orçar para melhoria em rotinas de banco. Quando os gerentes são solicitados a colaborar com medidas direcionadas a melhora do desempenho de sistema, racionalização de bancos de dados, re-design de processos em outras palavras, atividades que não são relacionadas diretamente à missão de suas das próprias unidades--eles resistem e dão preferência às necessidades de seus próprios negócios. Então, da perspectiva deste gerente, a Unidade de Tecnologia não tem nenhum recurso além de buscar a correção de falhas de um modo não planejado depois que elas aconteceram. O problema não está com a Unidade de Tecnologia, mas com as unidades empresariais. Ele, como os operadores do processo SBP, não assumem nenhuma responsabilidade pela situação. Então, pode ser deduzido que, além da ausência de um elemento importante de cultura de alta confiabilidade – a suposição de responsabilidade pessoal para segurança operacional--há um fragmento e modo reativo de lidar como um todo com fraquezas operacionais dentro de Banco Zeta.

Atitudes preventivas com respeito à segurança operacional envolvem procura para erros primários e ocultos, vigilância constante do ambiente de trabalho (ROCHLIN, 1993); treinamento e simulações relacionadas a possíveis acidentes (ROBERTS, 1990); e avaliação constante de processos operacionais para identificar fontes potenciais de problemas operacionais (WEICK; SUTCLIFFE, 2001). Nenhuma tal atitude preventiva foi identificada com respeito à segurança operacional do processo de SBP. Aqui novamente nenhuma presença de uma cultura de alta confiabilidade organizacional foi detectada: nenhuma manutenção de altos e constantes níveis de preocupação com fragilidades operacionais até mesmo na ausência de falhas amplas, ou de atividades para coletar e estudar informação sobre incidentes, acidentes individuais e situações onde a perda *quase* ocorreu, como postulada por Reason (1997).

O único comportamento de "alta confiabilidade" informado pelos empregados é a da reatividade. Problemas operacionais, quando identificados, são negociados imediatamente e transformados em melhorias em rotinas operacionais. De acordo com Reason (1997), um mecanismo de defesa organizacional é a criação de entender e se interessar por onde o risco acontece. Ele sugere que o melhor modo para aumentar a segurança operacional é administrar e melhorar processos organizacionais em vez de somente exercitar controle direto.

Dois aspectos das variáveis "atitudes" são aparentes: o seu forte caráter reativo e a natureza preventiva fraca. A ausência de pro atividade, como indica Rochlin (1993), pode resultar em perdas futuras, determinado o fato que as fontes de erro são dinâmicas. Protegendo contra a última falha não protege contra a próxima.

A evidência sugere que no processo de SBP haja um alto grau de aprendizagem instalada, conhecimento e habilidade entre operadores; mas características importantes da cultura organizacional de alta confiabilidade descritas através de Reason (1997) estão faltando: conhecimento sobre problemas potenciais e atitude de responsabilidade para segurança operacional.

Processos. Considerando os aspectos principais de alto risco mencionados por Perrow (1999) - complexidade, acoplamento apertado e controles inadequado - e as condições de alto risco mostradas por Rochlin (1993), Weick;Sutcliffe (2001) e Roberts; Rousseau (1989), o processo de SBP não pode ser caracterizado como apresentando condições de alto risco. O processo requer pouca ação humana. Apresentam uma baixa freqüência de eventos inesperados, decisões tomadas em ambiente operacional, ou operações realizadas por especialistas. Uma forma alternativa existe para realizar atividades no caso de haver problemas o com sistema funcional, como fazem os mecanismos de controle defensivos. Porém, ambas as pesquisas de documentário e observação de não-participante forneceram evidências de pressões relacionadas a cumprir prazos finais e interação de sistema-humano.

Até mesmo na ausência de condições de alto risco inerente no processo, falha humana, falha de sistema e fracasso de organização juntos conduziram aos amplos resultados negativos informados neste caso, confirmando as predições sobre tais situações por Bea e Moore (1993) e Reason (1997).

Administração do processo de operações de crédito

Em geral, uma operação de crédito consiste em liberar os ’recursos financeiros bancário” para um prestatário em base de normas específicas e procedimentos para cada tipo de produto. Para que a transação seja realizada, certos passos têm que ocorrer para garantir conformidade a padrões, inclusive controle e outros procedimentos de administração. As fases principais do processo são: análise de cliente, concessão, manutenção e recuperação de crédito. Na fase de análise de cliente, há inscrição de informação de cliente e avaliação de risco de cliente que utiliza métodos prescritos. Na fase de concessão, é formalizado o contrato de empréstimo e os recursos são liberados. Durante a fase de manutenção, controles existem para receber as quantias devidas, inclusive custos devido a pagamento em atraso, e para finalizar a operação. Na fase de recuperação, são adotados procedimentos administrativos ou judiciais para recuperar quantias vencidas.

No Banco Zeta, operações de crédito envolvem várias unidades organizacionais que são responsáveis por fases específicas do processo e têm objetivos diferentes, como descritas abaixo.

- Administração de crédito - desenvolvimento, implementação e padronização de produtos de crédito. Objetivo: proporcionar a instituição com produtos de crédito destinados para o mercado.
- Administração de filial - atendimento ao consumido e formalização da operação de crédito. Objetivo: vender produtos e cumprir metas de vendas
- Risco de crédito – avaliação do risco apresentado por prestatários. Objetivo: administrar e operacionalizar políticas de risco de crédito.
- Recuperação de crédito-ações administrativas para recuperar quantias vencidas. Objetivo: administrar e recuperar quantias devidas.
- Legal - ação legal com respeito a quantias não recuperadas por meios administrativos. Objetivo: apoio empresarial.

Perdas operacionais. A recuperação de crédito vencido depende da existência de registros precisos de informações de cliente, nome, endereço e telefone, por exemplo – para que contatos de iniciação de negociação de dívida possam ser feito. Além disso, formalização correta do contrato é essencial (o próprio contrato, assinatura, nota promissória) para fornecer

uma base para entrar com uma ação legal para recuperar o que foi emprestado ou, quando aplicáveis, garantias contratuais.

Banco Zeta abriu 400 mil ações para recuperação de contas vencidas, somando quase 500 milhões de *reais*, até mesmo quando ajustes para os valores atuais de empréstimos passados não são feito. Estes são contratos de empréstimo que foram concedidos pelo menos dois anos atrás e para qual nenhum reembolso foi recebido por mais de 360 dias. O banco de dados de informação de cliente que contém informação registrada no momento que o contrato foi assinado (nome, endereço, telefones e e-mail), permitia a recuperação de informação com respeito a só 100 mil destes contratos. Mesmo assim, em só 25,000 arquivos (6.25% de contas vencidas) era esta informação corrija e atualizada, permitindo contato com o devedor. Foram achadas inexatidões na informação de cliente de aproximadamente 70% de contas passadas devidas durante 35 dias ou menos, prometendo problemas futuros de natureza semelhante.

Este processo, como um todo, expõe a instituição a eventos inesperados que causam perdas financeiras e para qual é difícil de entrar com ação medicinal. Isto é pelo menos devido em parte ao fato que não houve nenhuma determinação por parte da administração superior que tais ocorrências fossem eliminadas, contribuindo à ausência de uma cultura organizacional de alta confiabilidade.

As perdas descritas podem ser vistas para ser o resultado de fraquezas discutidas na literatura da OAC: ausência de defesas; descumprimento com padrões operacionais e rotinas; interação de sistema-humano; pressões; acoplamento apertado das fases do processo; incompatibilidades entre os objetivos das unidades envolvidas; condição de risco oculta; e ausência de uma cultura organizacional de alta confiabilidade.

Ambiente, pessoas e processos. As condições de funcionamento para o processo de Operações de Crédito levantam fontes potenciais de alto risco dadas às pressões para cumprir objetivos e prazos de vendas e os objetivos contraditórios das várias unidades envolvidas no processo, uma das preocupações de Weick e Sutcliffe (2001) e a falta de orientação para observar um máximo de segurança, independente de pressões empresariais (REASON, 1997).

Havia poucos consensos nas respostas recebidas com respeito à liberdade para falar sobre fracassos operacionais. Porém, observação de não-participante comprovou que o tópico não é tratado abertamente pelos empregados, como também foi observado com o processo de SBP. Ao mesmo tempo, o humano, recursos financeiros e tecnológicos disponível ao processo foram observados como sendo adequado.

Enquanto os empregados percebem exatamente a suscetibilidade do processo a eventos inesperados, foi observado que eles nem sempre agem do modo mais seguro. Como também foi o caso no processo de SBP, os empregados não se sentem pessoalmente responsáveis pela segurança de operações, jogando a culpa em outro lugar pelos fracassos que acontecem. Uma fuga favorita, mais uma vez, é a Unidade de Tecnologia. O gerente daquela unidade informou que há 32 sistemas relacionados ao processo de crédito, cada um respondendo às necessidades de um gerente específico, com seus próprios bancos de dados que não permitem uma visão integrada do processo inteiro.

Não havia nenhuma evidência de comportamentos preventivos com respeito a fraquezas organizacionais e falhas. Por tanto, não havia nenhuma evidência que a aprendizagem acontece no processo de Operações de Crédito. Falhas operacionais não são usadas como um modo de melhorar a segurança de rotinas, recomendado por Weick e Sutcliffe (2001) como um meio de construir alta confiabilidade. Além disso, o elemento de

reatividade está ausente neste processo, comprovado pelo fato que embora fossem identificadas fraquezas de desempenho, nenhum passo foi dado para corrigir estas fraquezas. Respondentes informam conflito entre unidades organizacionais como a causa de algumas demoras em decisões administrativas e na atualização de rotinas e produtos, como também lentidão no processo de administração, especialmente em termos de informação.

Enquanto o treinamento e conhecimento sobre o funcionamento operacional existem, ainda há pouco conhecimento instalado sobre nossa preocupação por fatores que poderiam causar problemas com segurança operacional. Isto é consistente com a ausência previamente informada de pro atividade por parte dos operadores deste processo e também com ausência das características de uma cultura de alta confiabilidade.

Condições de alto risco como esboçado por Perrow (1999) está presente nos processos de Operações de Crédito na forma de acoplamento apertado, grande complexidade (um número grande de interfaces entre unidades organizacionais e sistemas) e constantes interações sistema-humano.

Análise do fluxograma de operações desenvolvida de dados colecionados para o estudo permite a caracterização dos processos de operações de crédito como um de hiper-complexidade, nas condições de Roberts e Rousseau (1989): envolve uma grande variedade de componentes, sistemas e níveis e cada unidade operacional tem seus próprios objetivos, procedimentos, padrões, rotinas, treinamento e hierarquia de comando.

Do fluxograma, é também aparente que não há nenhuma camada de defesa e que decisões são altamente centralizadas. Além disso, pesquisa documentária revelou um número grande de erros humanos e que não há nenhuma única unidade ou pessoa como um todo com supervisão direta sob o processo. Além disso, o descumprimento com padrões e rotinas evidencia a falta de obediência para regras formais e códigos de conduta, contrastando negativamente com as características de alta confiabilidade sugerida por Rochlin (1993).

A evidência sugere que a administração do processo de Operações de Crédito apresenta características de alto risco discutidas na literatura da OAC e que estas são causas prováveis das amplas perdas operacionais identificadas.

5. DISCUSSÃO

Neste estudo nós investigamos da perspectiva de estudos em Organizações de Alta Confiabilidade o que poderia ser as causas de fracassos operacionais experimentadas por uma grande instituição financeira e se a literatura da OAC poderia oferecer possíveis soluções para qualquer fraqueza operacional identificada.

Os resultados mostram que os dois processos investigados diferem em aspectos fundamentais. Por exemplo, o processo de SBP não está caracterizado através de condições de alto risco. No entanto, a evidência demonstra claramente que a confiabilidade neste processo foi comprometida por uma combinação de erro humano (falta de atenção, falta de conhecimento), fracasso de sistema (ausência de mecanismos preventivos para descoberta, alerta e controle) e falha organizacional (supervisão inadequada, treinamento deficiente), resultando em uma ampla perda operacional. Nenhuma cultura de alta confiabilidade está criada que possa servir como a base para prevenir problemas futuros ou mitigar se ocorrerem. No caso do processo de Operações de Crédito, condições de alto risco estão presentes, em termos de hiper-complexidade, constante interação de sistema-humano, acoplamento apertado entre fases do processo e controle inadequado das atividades realizadas. A confiabilidade também fica comprometida por descumprimento com padrões operacionais e rotinas. Embora

fraquezas operacionais fossem identificadas, nenhuma ação foi tomada para contrariá-los. Tomar tais ações é difícil na ausência de uma cultura de alta confiabilidade e na presença de interesses divergentes e paroquiais.

Nenhum dos resultados do estudo é discrepante com os resultados dos últimos estudos de OAC. Pelo contrário, os resultados estão conforme os resultados anteriores e fornece evidência de um tipo de organização — anteriormente não estudada empiricamente-uma instituição financeira com respeito ao seguinte:

- pressões relacionadas à conformidade de tarefas podem conduzir à supressão de procedimentos de segurança na ausência de uma cultural organizacional de alta confiabilidade; e.
- acoplamento apertado entre fases do processo ou unidades pode começar uma reação de cadeia de erros ao longo do processo inteiro.

Os resultados do estudo estão conforme resultados anteriores de acidente normal e de pesquisas da OAC, e também, sugerem que fracassos operacionais são o resultado de uma variedade de combinações diferentes ou configurações de fatores ao invés de uma única causa (REASON, 1997; PERROW, 1999).

A comparação dos fracassos operacionais estudada no Banco Zeta, sugere uma possível afiação de foco com respeito a observações de estudos anteriores, no sentido que está evidente no fracasso de SBP que a ausência de condições de altos riscos não faz, por si só, garantir que o fracasso operacional não ocorrerá. Em outras palavras, fracasso operacional pode acontecer até mesmo debaixo de condições que são relativamente de baixo risco, dependendo da inter-relação entre os fatores presentes em uma determinada situação em um determinado período de tempo e a ausência de defesas adequadas. Estudos adicionais que especificamente focam em fracassos operacionais debaixo de condições de baixo risco parecem pertinentes.

6. CONCLUSÕES

A evidência do estudo claramente demonstra a relação das perdas operacionais experimentada pelo Banco Zeta em seu Sistema brasileiro de Pagamento (SBP) e processos de Operações de Crédito para causas de fracasso operacional preditas na literatura da OAC, permitindo uma resposta afirmativa para a primeira das perguntas direcionada da pesquisa.

A resposta para a segunda pergunta também é afirmativa. A teoria da OAC oferece soluções para administração dos fatores que, da perspectiva de administração de risco operacional, causa perda:

- lidar com erro humano: um alto grau de responsabilidade de operador: processo decisório rápido (ROBERTS; ROUSSEAU, 1989) vigilância constante, obediência para regras formais e códigos de conduta (ROCHLIN, 1993); estabelecimento de uma cultura organizacional de alta confiabilidade (GRABOWSKI; ROBERTS, 1997); recompensas e incentivos para melhorar a segurança (ROBERTS et al., 2001).
- lidar com erro de sistema: constante monitorando, solução contingente, pro - atividade e reação (ROCHLIN, 1993); administração de tecnologia em tempo real (ROBERTS; LIBUSER, 1993); planos de contingência (WEICK; SUTCLIFFE, 2001); especificações apropriadas, procedimentos empresariais apropriados e processos, capacidade operacional e tendência

organizacional para inovação (LALLY, 2002).

- lidar com erros de processo: redundância em controles e em sistemas de informação; processo decisório rápido (ROBERTS; ROUSSEAU, 1989); prever e reação (ROCHLIN, 1993); não-simplificação de rotinas, sensibilidade para procedimentos operacionais (WEICK; SUTCLIFFE, 2001);

- lidar com fraudes: nível alto de confiança operacional e segurança (La Porte e Consolini citaram em ROCHLIN, 1993); ordenação de segurança (GRABOWSKI; ROBERTS, 1997);
- lidar com eventos externos: vigilância constante do ambiente operacional (ROCHLIN, 1993).

Langley (1999) argumenta que desenhar pesquisa de processo que seletivamente aplica conceitos de tradições teóricas diferentes para processar os dados pode enriquecer a teoria. Isto é o que nós tentamos fazer neste estudo, trazendo conceitos da tradição da OAC para suportar problemas da tradição de administração de risco operacional. Nossos resultados não somente sugerem fortemente a teoria da OAC pode ser ampliada para incluir instituições financeiras, mas que o estudo e prática de administração de risco operacional poderiam beneficiar da incorporação de conceitos e soluções de teoria da OAC, oferecendo uma contribuição potencial tanto à literatura de OAC e para as literaturas de administração de risco operacionais.

7. LIMITAÇÕES AO MÉTODO

Dados de pesquisa documentária com respeito à inscrição de fracassos operacionais e fragilidades que existem em segurança operacional podem não estar completamente seguras. Alguns dos materiais consultados podem ser parciais, distorcidos ou incompletos. Os questionários confiaram em percepções de respondentes, também notoriamente parcial. Então, foram feitas tentativas para contrabalançar estas limitações por uso de fontes múltiplas de evidência e triangulação de dados. Revisão de documentos com respeito aos processos estudados e as perdas operacionais experimentadas foram completadas por revisão de contabilidade e relatórios de auditoria internos. Foram usadas observação de não-participante e uma entrevista com o gerente da Unidade de Tecnologia para completar as percepções dos operadores dos processos estudados.

Certas limitações são inerentes à estratégia de estudo de caso utilizada, chefe entre eles a pergunta de generalização dos resultados. Enquanto a estratégia de estudo de caso tiver suas limitações, também tem forças que podem exceder em valor as desvantagens, dependendo do propósito da pesquisa. A estratégia de estudo de caso é fiel à riqueza, dinamismo e complexidade de dados de processo e habilita um entendendo mais profundo de fenômenos organizacionais. Até mesmo em casos que utilizam dados de processo, um ou alguns casos oferecem a forte possibilidade de identificar os fundamentais motivadores de processo, freqüentemente sendo o suficiente para produzir perspicácias úteis (LANGLEY, 1999). Na investigação informada aqui, baseada em dados de processo detalhados, achamos evidência que os processos conduzindo os fracassos operacionais estudados eram iguais aos observados na literatura de OAC, permitindo a conclusão que princípios de OAC poderiam ter uma contribuição para fazer à administração de risco operacional em instituições financeiras. Obviamente, outros estudos com resultados semelhantes fortaleceriam este achado.

8. CONSIDERAÇÕES FINAIS

Nosso estudo direciona as OAC e o risco operacional como fenômenos de nível-firme. Enquanto todas as empresas em um determinado setor podem ser expostas a risco operacional, está claro através de OAC que empresas individuais dentro de um setor podem administrar seus riscos operacionais de tal modo que reduza a probabilidade de fracassos operacionais.

Os resultados de nosso estudo fortemente sugerem que a teoria de OAC, realmente, tem o potencial para enriquecer compreensão de e discussões sobre o risco operacional em instituições financeiras e contribuir à administração efetiva de tal risco. Entendendo os mecanismos causais subjacentes que contribuem a fracassos operacionais torna possível dar passos positivos para administrá-los ao invés de somente calcular a probabilidade que tais fracassos possam ocorrer.

Puschaver e Eccles (1997) sugerem que a administração de risco no sentido completo envolva administração de oportunidade, de perigo, e de incerteza. A administração de oportunidade (administração de risco da parte superior) envolve as ações realizadas pela a administração para alcançar ganhos positivos. A administração de perigo (administração de risco do lado inferior) envolve prevenção ou mitigações de ações, situações ou eventos que podem gerar perdas. Em nosso papel nós focalizamos exclusivamente nos aspectos de lado ruim de administração de risco operacional. Porém, há um possível aspecto de lado superior ao uso de técnicas de alta confiabilidade em administrar o risco operacional. Na realidade, a alta confiabilidade pode oferecer oportunidades estratégicas como uma possível competência principal que pode ser desenvolvida e então alavancadas para lucros mais altos. Esta possibilidade merece investigação adicional.

REFERÊNCIAS

BEA, R.G.; MOORE, W.H. Operational reliability and marine systems. In: ROBERTS, K.H. (Org.). **New challenges to understanding organizations**. New York: McMillan, 1993.

BIS – Bank of International Settlements. International convergence of capital measurement and capital standards. Basel: BIS, 1988.

_____. International convergence of capital measurement and capital standards. Basel: BIS, 2004.

FORD, E.W.; DUNCAN, W.J.; BEDEIAN, A.G.; GINTER, P.M.; ROUSCULP, M.D.; ADAMS, A.M. Mitigating risks, visible hands, inevitable disasters, and soft variables: management research that matters to managers. **The Academy of Management Executive,** v.17, n. 1, p. 46-60, 2003.

GRABOWSKI, M.; ROBERTS, K.H. Risk mitigation in large-scale systems: Lessons from high reliability organizations. **California Management Review,** v. 39, n. 4, p. 152-162, 1997.

LALLY, L. Complexity, coupling, control and change: An IT based extension to normal accident theory. **Decision Sciences Institute 2002 Annual Meeting Proceedings.** New York: Decision Sciences Institute, 2002**.** Available at: <http://proquest.umi.com/pqdweb>. Accessed June 6, 2004.

LANGLEY, A. Strategies for theorizing from process data. **Academy of Management Review**, v. 24, n. 4, p. 691-710, 1999.

MARSHALL, C.L. Measuring and managing operational risks in financial institutions: Tools, techniques, and other resources. Singapore: John Wiley and Sons, 2001.

PERROW, C. **Normal accidents: Living with high-risk technologies**. New Jersey: Princeton University Press, 1999.

PUSCHAVER, L.; ECCLES, R. **Managing Upside Risk.** DerivativesStrategy.com, Nov 1997. Available at: <http://www.derivativesstrategy.com/magazine/archive/1997/1197col1.asp> . Acessed January 28, 2009.

REASON, J. Managing the risks of organizational accidents. Aldershot: Ashgate, 1997.

_____. Human error: Models and management. **Western Journal of Medicine,** v. 172, n. 6, p.393-395, 2000.

ROBERTS, K.H.; ROUSSEAU, D.M. Research in nearly failure-free, high reliability organizations: Having the bubble. **IEEE Transactions on Engineering Management,** v. 36, n. 2, p. 132-139, 1989.

ROBERTS, K.H. Managing high reliability organizations. **California Management Review, v.** 32, n. 4, p. 101-113, 1990.

ROBERTS, K.H. Some Characteristics of one Type of High Reliability Organizations. **Organization Science.** California, v. 1, n. 2, p. 160-176, 2001.

_____; LIBUSER, C. From Bhopal to banking: Organizational design can mitigate risk. **Organizational Dynamics,** v. 21, n. 4, p. 15-28, 1993.

ROCHLIN, G.I. Defining high reliability organizations. In: K.H. Roberts (Org.). **New challenges to understanding organizations.** New York: McMillan, 1993.

SAGAN, S.D. Learning from normal accidents. **Organizations & Environment**, v. 17, n. 1, p. 15-19, 2004.

VOGUS, T.J. Mapping the territory: Positive organizing as collective mindfulness, resilience, and sensemaking. **Positive organizational scholarship**. University of Michigan Business School, 2003. Available at: <http://www.bus.umich.edu/positive/contributors/timothyvogus>. Accessed October, 2003.

WEICK, K.E.; SUTCLIFFE, K.M. Managing the unexpected: Assuring high performance in an age of complexity. San Francisco: Jossey-Bass, 2001.

YIN, R.K. **Estudo de caso.** 2. ed. Porto Alegre: Bookman, 2001.