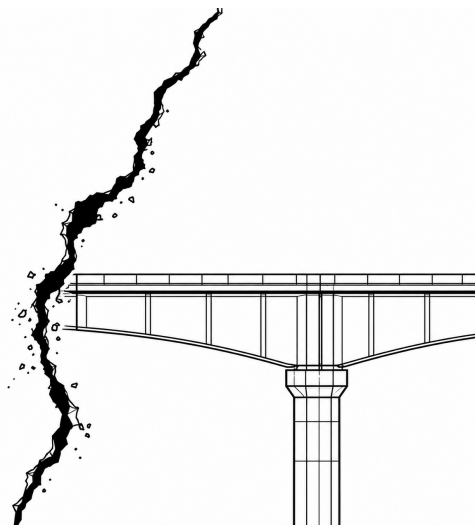


UMA INVESTIGAÇÃO SOBRE LIMITES,
DECISÕES E CONSEQUÊNCIAS

A QUEBRA

Como falhas nos protocolos transformam
pequenos desvios em grandes colapsos



“A quebra visível encerra a história. A quebra do protocolo é o momento em que ela realmente começa.”

**RICARDO XAVIER
DE OLIVEIRA**

EDIÇÃO EDITORIAL REVISADA

UMA INVESTIGAÇÃO SOBRE LIMITES,
DECISÕES E CONSEQUÊNCIAS

A Quebra

Como falhas nos protocolos transformam
pequenos desvios em grandes colapsos



RICARDO XAVIER DE OLIVEIRA

EDIÇÃO EDITORIAL REVISADA · 2026

A Quebra

Copyright © 2026 por Ricardo Xavier de Oliveira. Todos os direitos reservados.

Nenhuma parte desta obra poderá ser reproduzida, armazenada ou transmitida por qualquer meio, eletrônico ou mecânico, sem autorização expressa do autor e da editora, exceto em citações breves para fins de crítica, pesquisa ou resenha.

Título: A Quebra

Subtítulo: Como falhas nos protocolos transformam pequenos desvios em grandes colapsos

Autor: Ricardo Xavier de Oliveira

Edição: revisão documental e de navegação, 11 de outubro de 2026.

Ano: 2026. Formato: 15,24 × 22,86 cm.

ISBN, CIP, editora e créditos de produção: a definir.

Revisão jurídica para publicação: a definir.

Nota sobre os casos

Esta edição contém 32 casos: o relato pessoal anonimizado “A Farsa” e 31 casos públicos. O contraponto Qantas 32 completa a contagem. As notas documentais identificam as fontes, distinguem sua natureza e registram limites de verificação. As conclusões autorais sobre protocolos não substituem as conclusões dos documentos citados.

O relato pessoal não foi acompanhado de documentação pública para verificação independente.

Nos casos públicos, referências identificadas nesta revisão não são automaticamente atribuídas à pesquisa da redação original. O alcance da conferência é informado nas notas.

Paginação: 159 páginas no arquivo, contadas desde a capa. Folhas de abertura e folhas em branco podem omitir o número impresso. Sumário, índice, notas e glossário usam a mesma contagem.

Notas: p. 135. Glossário: p. 155.

*Aos que tiveram a coragem de parar
quando todos pediam para continuar.*

*E aos que pagaram o preço
porque ninguém interrompeu a sequência.*

***“Uma regra que pode ser suspensa
pela conveniência
não é um limite. É uma sugestão.”***

RXO

Sumário

Prólogo - A fábrica que fechou muito antes de fechar	9
Introdução - O que quebra primeiro?	12
PARTE I - ANTES DO COLAPSO	16
Capítulo 1 - O último elo à vista de todos	17
Capítulo 2 - O voo que começou a cair antes de decolar	21
Capítulo 3 - A exceção que funciona	25
Capítulo 4 - Setenta e três segundos	27
Capítulo 5 - O teste que não precisava terminar	31
PARTE II - BARREIRAS, MARGENS E SINAIS	35
Capítulo 6 - A cidade que dormia ao lado do perigo	37
Capítulo 7 - A máquina disse que estava tudo bem	41
Interlúdio - Quando uma pessoa vira a última barreira	44
Capítulo 8 - A barragem que já não podia confiar nos próprios sinais	47
Capítulo 9 - O avião que sabia mais que o piloto	51
Capítulo 10 - O alerta que perdeu autoridade	55
Interlúdio - Quando o desvio chega ao público	58

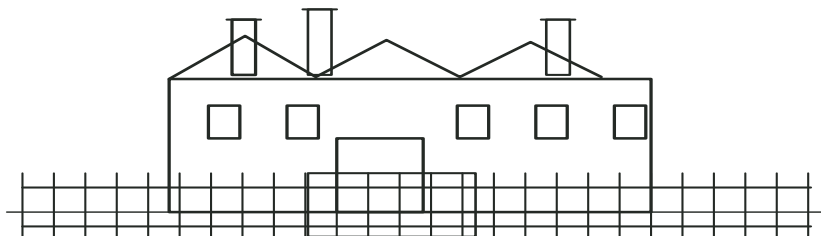
Sumário

PARTE III - QUANDO O SISTEMA APRENDE A PARECER CORRETO	61
Capítulo 11 - O carro que reconhecia o laboratório	63
Capítulo 12 - O teste aprovado pelo desejo de terminar	67
Interlúdio - Quando a aparência substitui o controle	70
Capítulo 13 - A torre que já havia sido avisada	73
Capítulo 14 - O resultado que não podia atrasar o lote	77
Caso AdeS - Os oitenta segundos que a fábrica não conteve	81
Capítulo 15 - A inovação que dispensou a prova	85
Capítulo 16 - O desvio que virou espetáculo	89
Capítulo 17 - O perigo embarcado como carga comum	93
Capítulo 18 - O defeito que viajou entre departamentos	97
Interlúdio - Três produtos, três verdades adiadas	101

Sumário

PARTE IV - ANATOMIA DA QUEBRA	104
Capítulo 19 - As nove formas de quebrar um protocolo	105
Capítulo 20 - Quando a meta derrota o limite	109
Capítulo 21 - Quem responde pelo sistema	111
PARTE V - ANTES QUE QUEBRE	113
Capítulo 22 - O protocolo que funciona	115
Capítulo 23 - O mensageiro não é o problema	117
Capítulo 24 - A decisão de parar	119
Capítulo 25 - Como verificar uma barreira	123
Interlúdio - QF32: quando uma falha não vira colapso	126
PARTE VI - O CAMINHO QUE AINDA EXISTE	128
Epílogo - A fábrica que ainda poderia ter sido salva	129
Conclusão - Antes da próxima quebra	132
Agradecimentos	134
Notas documentais e referências	135
Referências conceituais	152
Índice de casos	153
Glossário	155
Sobre o autor	158

A fábrica que fechou muito antes de fechar



Este livro não nasceu em Imola. Não nasceu no centro de controle de Chernobyl, na plataforma do Challenger ou na cabine do avião que levava a Chapecoense para Medellín. Nasceu numa fábrica que eu conhecia por dentro.

Em 30 de junho de 2026, o vigilante girou a chave pela última vez. Durante décadas, aquele portão havia recebido caminhões, operadores, fornecedores, clientes e projetos. Naquela tarde recebeu apenas o silêncio. As últimas pessoas saíram carregando caixas com fotografias, canecas, capacetes e pequenos objetos que pareciam insuficientes para representar uma vida inteira de trabalho.

Nos dias seguintes, surgiram explicações rápidas. A unidade perdera competitividade. Os custos haviam crescido. Um cliente estratégico fora perdido. O mercado já não perdoava ineficiências. Tudo isso era verdade. Nada disso, porém, respondia à pergunta que começou a me perseguir: quando aquela fábrica realmente começou a fechar?

A primeira coisa que desapareceu foi a verdade

A resposta não estava no balanço final. Estava em pequenas decisões que, isoladamente, pareciam administrar problemas. Uma reclamação de cliente deixou de ser registrada porque pioraria os indicadores. Um novo lote foi enviado, o desconforto imediato desapareceu e todos puderam tratar o assunto como resolvido.

A solução parecia eficiente. Na realidade, o sistema perdia memória. Sem registro não havia frequência. Sem frequência não havia recorrência. Sem recorrência não existia razão estatística para atacar a causa. O problema não fora eliminado. Apenas deixara de existir na versão oficial da operação.

A mesma lógica alcançou outras áreas. Acidentes demoravam a ser comunicados. Pesquisas internas eram conduzidas com o cuidado de não produzir respostas que pudessem reduzir investimentos. Inventários dependiam de estimativas pouco auditadas. Auditorias eram precedidas por uma preparação

quase teatral: documentos organizados, áreas escolhidas, respostas alinhadas. O papel descrevia uma operação. A rotina praticava outra.

Quem apresentava um problema parecia incapaz. Quem apresentava números verdes parecia competente. Quando a distorção começou a produzir bônus, prestígio e proteção, deixou de ser uma exceção e tornou-se um método de seleção. Pessoas que protegiam a narrativa prosperavam. Pessoas que confrontavam a realidade se tornavam inconvenientes.

O dia em que deveria ter parado

Em determinado período, a principal fonte de água da fábrica sofreu uma deterioração severa. A estação de tratamento não havia sido projetada para receber aquela condição. A decisão técnica era simples e desagradável: interromper a produção.

Parar exporia fragilidades. Havia um cliente estratégico a abastecer, metas a cumprir e uma cultura que tratava qualquer interrupção como derrota. A fábrica já não sabia admitir que não possuía condições para continuar. Então continuou.

O produto foi fabricado, embalado e enviado. O protocolo de parada, criado para impedir que uma condição inadequada alcançasse o produto, foi substituído pela prioridade de manter o volume. Nada aconteceu imediatamente. O material saiu, a operação prosseguiu e os resultados foram registrados. A ausência de uma consequência imediata repetiu a mensagem que a organização já conhecia: talvez o risco tivesse sido exagerado.

Meses depois, reclamações cresceram de maneira extraordinária. Consumidores descreviam odor e sabor incompatíveis. O cliente iniciou uma investigação e encontrou registros, históricos e amostras testemunhas que deveriam preservar a verdade daquele período.

As amostras não apresentavam a anomalia. Segundo o relato que fundamenta esta passagem, elas haviam sido substituídas. Não apresento essa afirmação como conclusão judicial. Apresento como parte da experiência que me levou a compreender um mecanismo: a primeira quebra expôs o produto; a quebra seguinte destruiu a capacidade de aprender com a primeira.

Por que passei a chamar essa história de A Farsa

Vieram novos documentos, novos treinamentos, novas assinaturas e ações marcadas como concluídas. A fábrica acrescentou papel a um sistema que já demonstrara capacidade de neutralizar o papel. O problema não era a falta de procedimentos. Era uma cultura em que o procedimento podia ser ignorado quando ameaçava o resultado e exibido depois como prova de conformidade.

Quando uma nova manifestação surgiu, a liderança da unidade foi substituída. O cliente, porém, já havia chegado à própria conclusão. Ele não precisava apenas de um produto dentro da especificação. Precisava acreditar que, diante de uma falha, receberia a verdade. A confiança terminou antes do contrato.

A perda de volume aumentou custos, reduziu competitividade e limitou investimentos. Gestores passaram a se suceder rapidamente. Cada nova liderança recebia uma operação mais frágil, menos confiável e mais dependente de uma versão conveniente de si mesma. Até que o portão foi fechado.

Passei a chamar essa história de A Farsa não por causa de uma única mentira, mas porque a aparência de controle havia ocupado o lugar do controle. A organização não quebrou apenas o protocolo de produção. Quebrou o registro, a preservação das evidências, a investigação, a reação, a aprendizagem e, por fim, o compromisso de dizer a verdade ao cliente.

Foi esse caso que me levou a procurar a mesma arquitetura em acontecimentos aparentemente distantes. Um carro de Fórmula 1, um ônibus espacial, uma aeronave sem combustível, uma usina nuclear, uma barragem, um alimento contaminado e um recall não possuem a mesma causa física. Mas todos obrigam a fazer a mesma pergunta: qual limite deveria ter interrompido a sequência e por que ele perdeu autoridade?

A condição da água criou um problema temporário. A quebra dos protocolos transformou esse problema em destino empresarial.

Nota documental: Relato pessoal anonimizado, sem documentação pública apresentada para verificação independente. Ver ND-01, p. 135.

O que quebra primeiro?

A última falha recebe o nome da tragédia. Este livro procura a anterior.

O mundo costuma nomear os grandes colapsos pela última coisa que falhou.

O avião caiu porque o combustível terminou. A barragem rompeu porque perdeu estabilidade. O produto foi recolhido porque uma peça apresentou defeito. O alimento foi contaminado porque um microrganismo atravessou o processo.

Essas explicações podem estar corretas e, ao mesmo tempo, chegar tarde demais. O combustível terminou no fim do voo, mas a reserva havia desaparecido no planejamento. A estrutura caiu em segundos, mas sinais anteriores não produziram interdição. A peça se rompeu no acidente, mas projeto, modificação ou validação já poderiam ter retirado a margem necessária.

A quebra visível recebe câmeras, manchetes e processos. A anterior quase nunca é fotografada. Pode acontecer numa reunião, num cálculo, numa mudança não avaliada, numa inspeção adiada, num lote liberado, num alarme relativizado ou na frase mais perigosa da vida operacional: apenas desta vez.

A quebra física encerra a história. A quebra do protocolo é o momento em que ela realmente começa.

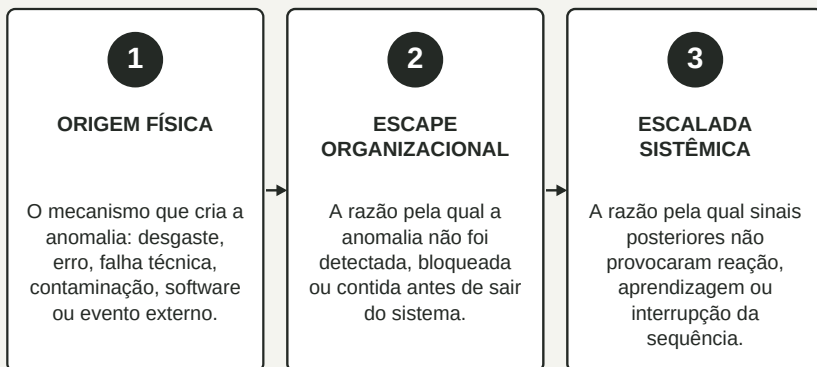
A tese, formulada com precisão

Este livro não sustenta que toda anomalia nasce de descumprimento. Equipamentos envelhecem, materiais variam, pessoas se enganam, fenômenos imprevistos surgem e tecnologias podem falhar de maneiras ainda desconhecidas.

A tese é mais específica e mais exigente: todo grande desvio organizacional evitável contém, em algum ponto de sua cadeia, uma quebra no sistema de protocolos que deveria reconhecer, conter, interromper ou aprender com o risco.

A falha técnica pode criar a anomalia. É a perda de autoridade das barreiras que permite que ela atravesse o sistema e se transforme em acidente, não conformidade, reclamação, recall, fraude, dano ambiental ou perda de confiança.

TRÊS CAMADAS DA INVESTIGAÇÃO



A tese do livro se concentra nas duas últimas camadas: o ponto em que a organização ainda podia intervir.

Protocolo não é apenas procedimento

Neste livro, protocolo não significa somente um documento escrito. Significa o sistema real criado para impedir que um risco avance. Pode ser uma regra, especificação, reserva, barreira física, teste, validação independente, bloqueio, permissão de trabalho, segregação, critério de parada ou obrigação de comunicar.

Um procedimento com código, revisão e assinaturas pode ser apenas uma descrição. Torna-se protocolo quando as pessoas o compreendem, possuem competência e recursos para executá-lo, encontram supervisão na prática e sabem que o desvio produzirá reação, mesmo quando cumprir a regra custa produção, prazo, dinheiro ou prestígio.

Em grandes organizações, a ausência do protocolo necessário não é um espaço neutro. Existem processos de gestão destinados a identificar perigos, avaliar riscos, controlar mudanças, validar projetos, aprender com incidentes e criar padrões. Se o controle específico não foi criado, é preciso perguntar qual processo superior deixou de cumprir essa função.

Não ter o protocolo necessário pode ser a forma mais profunda de quebrá-lo.

Quando a tese pode ser aplicada

A expressão quebra de protocolo não deve servir como explicação automática para qualquer resultado ruim. Para que o conceito tenha valor analítico, precisa aceitar limites e possibilidade de contestação.

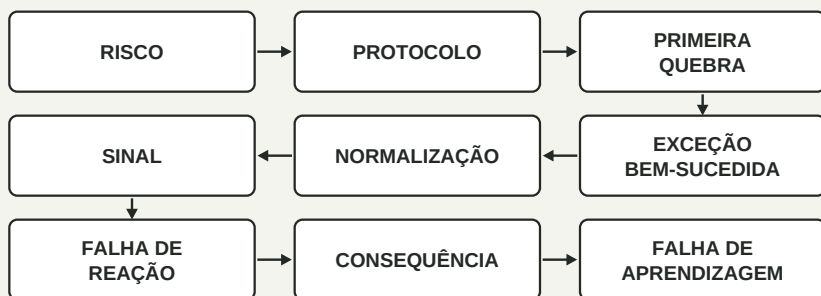
QUANDO É LEGÍTIMO FALAR EM QUEBRA DE PROTOCOLO?**O risco era conhecido ou razoavelmente identificável?****A organização possuía autoridade ou capacidade de intervir?****Havia, ou deveria haver, uma barreira proporcional ao risco?****A ausência, inadequação ou neutralização da barreira contribuiu para o resultado?****Sinais posteriores poderiam ter mudado a decisão ou limitado a consequência?**

Sem esses elementos, “quebra de protocolo” se tornaria apenas um rótulo impossível de contestar.

Uma causa comum não é uma causa única

Acidentes, contaminações, recalls, fraudes e colapsos não possuem uma única causa física. Sistemas complexos falham pela combinação de mecanismos diferentes. Uma explosão pode exigir vazamento, mistura inflamável e fonte de ignição. Uma contaminação pode depender de matéria-prima, temperatura, higienização e tempo. Um acidente aéreo pode reunir planejamento, comunicação, meteorologia, decisão e falha técnica.

A tese é sistêmica. Causas imediatas diferentes produzem consequências porque o sistema encarregado de controlá-las perdeu eficácia: o protocolo não existia, era inadequado, estava desatualizado, não podia ser executado, não foi treinado, não foi cumprido, não foi verificado, não gerou reação ou não incorporou o aprendizado.

MAPA-MESTRE DA QUEBRA

A consequência chama atenção. O método recua até o primeiro ponto em que um limite perdeu autoridade.

Responsabilidade sem simplificação

A execução direta pode pertencer ao operador. A garantia do sistema pertence à liderança. O operador responde por executar e relatar. O supervisor responde por treinar, observar, diagnosticar e reagir. O gerente responde por assegurar que o sistema exista, funcione, seja verificado e aperfeiçoado. A direção responde por prioridades, recursos, incentivos, governança e consequências coerentes.

Responsabilidade gerencial não significa culpa jurídica automática. Culpa penal, responsabilidade civil e sanções administrativas dependem de jurisdição, dever legal, conhecimento, nexos causal, capacidade de intervenção e provas. A análise organizacional responde a outra pergunta: quem tinha autoridade para impedir que o risco continuasse avançando?

Como ler as histórias

Cada capítulo começa pela ocorrência conhecida e depois recua. Qual risco existia? Qual limite deveria controlá-lo? O protocolo era adequado? Havia condições para cumpri-lo? Quando perdeu autoridade? Que sinais apareceram? Por que não provocaram interrupção? O que teria acontecido se a barreira funcionasse?

Os fatos serão separados das hipóteses. Controvérsias técnicas não serão escondidas. Relatórios oficiais terão prioridade. Quando a documentação não permitir conclusão segura, a dúvida será preservada. Nenhum caso deve ser forçado a confirmar a tese.

No fim das histórias centrais, o quadro O Ponto de Ruptura apresentará protocolo, primeira quebra, consequência, caminho alternativo e veredito. Não para reduzir acontecimentos complexos a uma frase, mas para localizar o momento em que ainda havia uma escolha capaz de mudar o desfecho.

A pergunta deste livro não é apenas “por que aconteceu?” É: “em que momento essa história ainda poderia ter terminado de outra forma?”

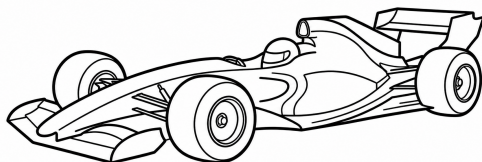
PARTE I

ANTES DO COLAPSO

A margem costuma desaparecer muito antes de a consequência aparecer.



O último elo à vista de todos



1º de maio de 1994. Ayrton Senna entrou no fim de semana de Imola pressionado por um carro difícil e por um início de temporada sem os resultados esperados.

Na sexta-feira, Rubens Barrichello sofreu um acidente grave e sobreviveu. No sábado, Roland Ratzenberger morreu durante a classificação. No domingo, a corrida começou sob a atmosfera de um esporte que já recebera dois avisos em menos de quarenta e oito horas.

Senna largou na pole position. Depois de uma interrupção inicial, a prova foi retomada. Na sétima volta, o Williams seguiu reto na Tamburello.

| A peça quebrada apareceu no fim. As perguntas começaram antes.

Um carro que exigia adaptação

O Williams FW16 nascera em uma temporada de mudanças técnicas. Recursos eletrônicos que ajudavam a estabilizar os carros haviam sido proibidos, e as equipes precisavam reaprender a transformar potência em controle.

Senna buscava uma posição de condução mais adequada. A coluna de direção foi modificada para ajustar a relação entre o piloto, o volante e o espaço do cockpit.

Modificar não é sinônimo de errar. A engenharia existe justamente para alterar sistemas. O problema começa quando um componente crítico é modificado sem que dimensionamento, fabricação, inspeção e validação produzam evidência proporcional ao risco.

A coluna não era um acabamento. Era o elo físico entre a decisão do piloto e a direção das rodas. Uma falha ali não deixaria tempo para compensação.

Quanto mais grave a consequência de uma falha, menos aceitável é depender de uma única suposição.

A explicação que parece completa

Murgia relata a conclusão judicial italiana: o acidente foi atribuído à falha da coluna modificada. A narrativa parecia simples: a peça se rompeu, o carro deixou de responder e o impacto veio depois.

Outros especialistas questionaram a ordem exata dos acontecimentos. A ruptura teria se iniciado antes da saída da pista ou ocorrido durante a sequência do impacto? A controvérsia não desapareceu, e um livro sério não deve fingir que ela desapareceu.

Mas a incerteza sobre o gatilho não impede outra investigação. Mesmo quando a microsequência permanece discutida, ainda é possível perguntar quais protocolos deveriam impedir que uma única falha produzisse uma consequência irreversível.

A engenharia não controla apenas a causa mais provável. Controla também a possibilidade de que algo improvável ocorra.

O fim de semana já havia falado

Imola não ofereceu um domingo isolado. O acidente de Barrichello e a morte de Ratzenberger haviam alterado o contexto. O risco, que normalmente permanece abstrato, estava diante das equipes, dos organizadores e dos pilotos.

Sinais não são protocolos. Eles não param uma operação por conta própria. Precisam encontrar critérios, autoridade e disposição para mudar a decisão.

Depois de um acontecimento grave, existem perguntas que não podem ser tratadas como burocracia: o sistema continua seguro? Alguma condição mudou? As barreiras disponíveis ainda são suficientes? O que precisa ser verificado antes de prosseguir?

A resposta pode ser continuar. Mas continuar precisa ser uma conclusão técnica, não a opção automática produzida pelo calendário.

O muro não foi a primeira barreira

A discussão sobre Senna costuma concentrar-se na coluna de direção e no impacto. O protocolo, porém, não termina na peça.

Antes dela, existiam o projeto, a especificação do material, a geometria da modificação, a qualidade da solda, os ensaios, a inspeção e a liberação. Depois dela, existiam a capacidade do carro de absorver energia, a distância até a barreira, a configuração da curva e as proteções destinadas a limitar uma saída de pista.

Cada camada possuía uma função diferente. Nenhuma precisava ser perfeita. Precisavam, juntas, impedir que uma falha isolada atravessasse todo o sistema.

Quando várias defesas dependem da mesma condição favorável, o sistema parece redundante no papel e permanece frágil na realidade.

O que quebrou primeiro?

Talvez a coluna tenha sido o gatilho físico. Talvez a ordem exata continue discutida. A tese deste livro não depende de transformar uma controvérsia técnica em certeza conveniente.

A pergunta útil é anterior: uma modificação em componente crítico foi submetida a uma cadeia de validação capaz de demonstrar sua segurança? Os sinais daquele fim de semana produziram uma reavaliação proporcional? As barreiras do carro e do circuito poderiam impedir que uma perda de controle se tornasse fatal?

A primeira quebra pode não estar em uma única sala, pessoa ou assinatura. Pode estar na soma de decisões que permitiu que o sistema chegasse à corrida com menos margem do que acreditava possuir.

Essa distinção não reescreve a história. Apenas muda o ponto em que começamos a investigá-la.

O PONTO DE RUPTURA

PROTOCOLO

Qualquer alteração em componente crítico de direção deve ser dimensionada, fabricada, ensaiada, inspecionada e liberada com evidência suficiente. O veículo e o circuito devem possuir camadas capazes de limitar a consequência de uma saída de pista.

PRIMEIRA QUEBRA

A coluna modificada chegou à corrida em condição considerada inadequada pela Justiça italiana, enquanto sinais e barreiras disponíveis não impediram que uma perda de controle se tornasse fatal.

CONSEQUÊNCIA

Uma falha ou perda de controle atravessou sucessivas camadas insuficientes e produziu um impacto sem recuperação.

SE FOSSE CUMPRIDO

Uma peça não validada não seria liberada. Mesmo que outra dinâmica provocasse a saída de pista, barreiras mais eficazes poderiam reduzir a consequência.

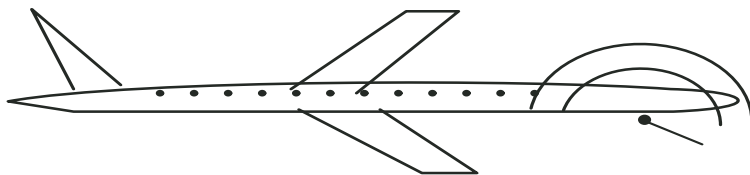
VEREDITO

O gatilho exato permanece discutido. O que não se discute é que uma cadeia de validação e proteção mais robusta abriria outro desfecho.

Nota documental: Reconstrução técnica de Murgia e histórico de segurança da FIA. A conclusão judicial é referida por intermédio do estudo; preserva-se a controvérsia técnica. Ver ND-02, p. 136.

O caso Senna não prova que toda quebra começa em uma peça. Prova que uma peça nunca deveria estar sozinha diante da consequência.

O voo que começou a cair antes de decolar



28 de novembro de 2016. A viagem levava uma equipe brasileira à partida mais importante de sua história.

O avião partiu da Bolívia para a Colômbia. Os motores funcionavam, a rota estava aberta e o destino parecia ao alcance. O problema, contudo, já estava presente antes da decolagem.

Estava nos números. O voo direto havia sido planejado praticamente com o combustível esperado para percorrer a rota, sem preservar de forma adequada as reservas necessárias para espera, desvio, aproximação adicional e pouso em aeroporto alternativo.

O plano transformava a normalidade absoluta em requisito de sobrevivência.

A reserva existe porque o plano falha

Nenhum voo pode depender de vento perfeito, rota livre, aproximação imediata e ausência de imprevistos. A reserva é o espaço entre aquilo que se espera e aquilo que o mundo real pode exigir.

Retirar essa margem não faz o risco desaparecer. Apenas transfere a responsabilidade para a esperança de que nada saia do previsto.

A primeira oportunidade de interromper a sequência surgiu antes da partida. O plano poderia ser recusado, a rota dividida ou uma escala de reabastecimento incluída. Nada disso exigia descobrir um perigo novo. Bastava cumprir uma regra conhecida.

A decisão segura teria um custo imediato: atraso, combustível, explicações. A decisão insegura preservava o cronograma e deixava o risco sem testemunhas.

As oportunidades de voltar

O avião decolou. Durante algum tempo, a decisão insegura produziu resultados. A rota avançava, o prazo era preservado e ninguém precisava explicar uma parada.

Durante o trajeto, outra oportunidade permaneceu disponível. A tripulação poderia pousar para abastecer. Isso custaria tempo e dinheiro, mas reconstruiria a margem retirada no planejamento.

Quando surgiu a advertência de baixo combustível, ainda era possível mudar o plano e comunicar claramente a condição crítica. Um alerta não existe para descrever o problema. Existe para obrigar a decisão a mudar.

Cada oportunidade ultrapassada tornou a seguinte mais cara e menos eficaz.

A espera não criou o problema

Na região do destino, outro avião precisava de prioridade. O controle organizou a sequência e determinou espera sem conhecer inicialmente toda a gravidade da situação.

A espera não criou a falta de combustível. Apenas revelou que a aeronave chegara sem capacidade de suportar um acontecimento comum da aviação.

A tripulação pediu prioridade, mas a declaração inequívoca de emergência veio quando a margem já estava quase esgotada. O sistema tentou abrir caminho. Prioridade, porém, não produz combustível. Apenas permite usar com preferência aquilo que ainda resta.

Os motores começaram a apagar. A aeronave não alcançou a pista.

O custo que parecia maior

Cada decisão segura possuía um preço visível. A escala custaria tempo e dinheiro. O desvio exporia o erro. A emergência produziria perguntas.

Continuar parecia proteger cronograma, reputação e conveniência. Quando a consequência chegou, descobriu-se que nenhum desses custos se aproximava do preço real.

Essa é uma característica recorrente das quebras de protocolo. O benefício aparece primeiro. A consequência fica distante, incerta e sem nome.

Se o protocolo fosse cumprido, a viagem poderia atrasar, mudar de rota ou terminar em outro aeroporto. O perigo da distância permaneceria. O esgotamento em voo, não.

O que quebrou primeiro?

A causa imediata foi o esgotamento de combustível. A cadeia anterior envolveu planejamento sem reservas adequadas, aceitação do plano, oportunidade de reabastecimento ultrapassada, reação insuficiente aos alertas e comunicação tardia da emergência.

Nenhum desses elos, isoladamente, explica toda a ocorrência. Juntos, mostram o sistema perdendo a capacidade de interromper uma decisão que se tornava progressivamente mais perigosa.

A primeira quebra não foi o apagamento dos motores. Foi aceitar uma operação na qual a chegada dependia de o mundo obedecer ao plano sem exigir margem.

A tragédia terminou perto de Medellín. O caminho para ela começou antes da decolagem.

O PONTO DE RUPTURA

PROTOCOLO

Planejar combustível com reservas regulamentares, alternativa viável, monitoramento contínuo e declaração imediata de emergência quando a margem deixasse de existir.

PRIMEIRA QUEBRA

O voo foi aceito sem reserva adequada, continuou sem reabastecimento e comunicou a condição extrema tarde demais.

CONSEQUÊNCIA

O combustível se esgotou antes do pouso, os motores pararam e a aeronave não alcançou a pista.

SE FOSSE CUMPRIDO

O voo não partiria naquele plano ou realizaria uma escala. Mesmo depois da decolagem, o desvio para reabastecimento ou a emergência antecipada interromperia a sequência.

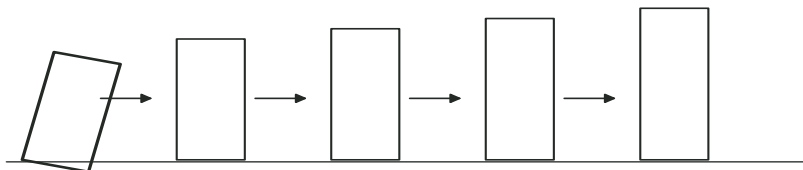
VEREDITO

A distância tornou o risco possível. A quebra dos protocolos de margem e reação tornou a queda real.

Nota documental: Aerocivil, relatório final COL-16-37-GIA. Voo LaMia 2933; CP2933 é a matrícula da aeronave. Ver ND-03, p. 136.

Senna mostrou a fragilidade de uma barreira crítica. A Chapecoense mostrou o desaparecimento progressivo da margem. Nos dois casos, a consequência apareceu depois que as oportunidades de interromper já haviam sido consumidas.

A exceção que funciona

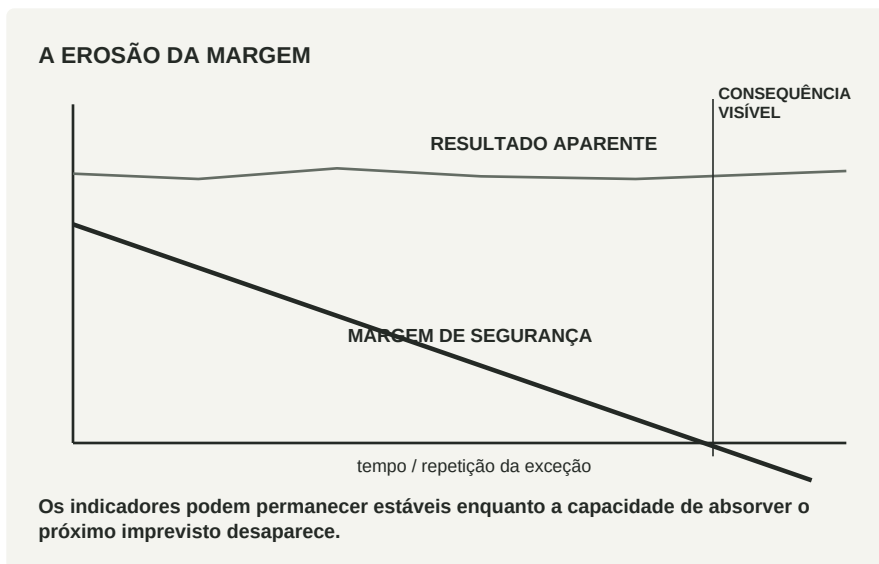


O equipamento precisava continuar. O turno estava atrasado, a parada exigiria explicações e nada indicava falha imediata. A decisão pareceu pequena: terminar agora e verificar depois.

O turno terminou. O equipamento não quebrou. O produto saiu. Nenhuma reclamação apareceu.

A exceção entregou resultado antes de cobrar o risco.

Foi exatamente aí que o problema começou.



O benefício aparece primeiro

Toda quebra de protocolo oferece alguma vantagem imediata. Evita uma parada, preserva o prazo, reduz o conflito ou mantém o indicador dentro da meta.

Cumprir o protocolo cobra um preço conhecido. Rompê-lo transfere a possível consequência para um futuro que talvez nunca chegue.

BENEFÍCIO	SILÊNCIO	PRECEDENTE
A decisão insegura entrega resultado agora.	A consequência não aparece imediatamente.	A exceção passa a parecer experiência.

Sobreviver a uma exposição não demonstra que ela era aceitável. Demonstra apenas que, naquela ocasião, as demais condições impediram o pior desfecho.

A sorte não se apresenta como sorte. Ela chega disfarçada de experiência.

Quanto mais vezes o desvio termina bem, mais difícil se torna defender o limite que continuou protegendo o sistema sem receber crédito.

Quando a exceção vira regra real

A primeira concessão provoca desconforto. A segunda encontra um precedente. A terceira já possui uma história capaz de justificá-la.

Ninguém precisa revogar formalmente o protocolo. Basta demonstrar que ele pode ser negociado. A regra continua no sistema, o treinamento continua na agenda e a auditoria continua procurando assinaturas.

O que muda é sua autoridade. Violação vira flexibilidade. Falta de controle vira contingência. Decisão sem evidência vira experiência operacional.

Foi assim que a margem desapareceu no voo. É assim que inspeções, validações, limites ambientais e critérios de liberação começam a perder força em organizações aparentemente normais.

A regra para ler este livro

Os próximos capítulos não começarão por definições. Começarão por pessoas, decisões, peças, dados, alarmes e momentos em que ainda existia outro caminho.

Depois de cada história, quatro perguntas organizarão a investigação:

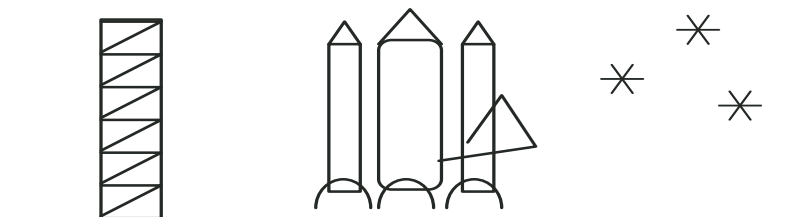
- 1 Qual risco estava presente?
- 2 Qual limite deveria contê-lo?
- 3 Quando esse limite perdeu autoridade?
- 4 O que mudaria se ele tivesse funcionado?

Nem toda ocorrência possui uma única causa física. Mas grandes desvios compartilham com frequência uma perda de controle: o sistema deixa de transformar risco em limite, limite em execução e anomalia em aprendizagem.

A partir daqui, cada história começará no fato conhecido e voltará até a primeira quebra.

Porque a consequência chama a atenção. Mas é o primeiro limite rompido que explica por que ela conseguiu chegar.

Setenta e três segundos



Havia gelo na estrutura. Os sete tripulantes estavam a bordo, entre eles a professora Christa McAuliffe, cuja presença transformara a missão em um acontecimento nacional.

O último elo foi visto por milhões. Os primeiros haviam se formado durante anos.

A peça que já havia avisado

Os foguetes auxiliares eram montados em grandes segmentos unidos por juntas. Dois anéis de borracha, os O-rings, deveriam impedir que gases extremamente quentes escapassem durante a queima.

Em temperaturas baixas, a borracha respondia mais lentamente. A junta podia se abrir antes que o anel ocupasse o espaço necessário. Isso não foi descoberto depois da tragédia. Missões anteriores já haviam revelado erosão, fuligem e passagem de gases.

Os anéis não tinham sido projetados para sofrer erosão. Mesmo assim, os voos voltaram em segurança. A anomalia deixou marcas, mas não produziu a pior consequência.

O desvio ganhou histórico. O histórico ganhou tolerância. A tolerância começou a se parecer com conhecimento.

A matemática da sorte

Quando um componente falha e a missão termina bem, a organização recebe duas mensagens. A primeira é técnica: existe uma anomalia. A segunda é emocional: sobrevivemos.

A mensagem emocional costuma chegar primeiro. Ela reduz o desconforto, protege o cronograma e permite que a correção seja adiada. Aos poucos, a sobrevivência deixa de ser tratada como sorte e passa a ser apresentada como prova de robustez.

O QUE OS DADOS DIZIAM	O QUE A ROTINA APRENDEU
Temperaturas menores estavam associadas a maior deterioração das juntas. Havia um problema conhecido e ainda não resolvido.	As missões anteriores voltaram. Portanto, a erosão parecia administrável e o lançamento podia continuar.

Uma força-tarefa estudava uma solução definitiva. Paradoxalmente, o documento que reconhecia o problema também ajudava a mantê-lo ativo: se alguém estava estudando, parecia haver controle.

Os dados existiam. A história contada por eles, não.

Depois do acidente, o histórico completo mostrou uma relação inquietante entre temperatura e deterioração dos O-rings. Antes do lançamento, porém, os números haviam sido organizados de modo que o padrão permanecia difícil de enxergar.

Dados não falam sozinhos. Dependem da pergunta, da comparação e da forma de apresentação. Uma tabela pode revelar que o risco aumenta no frio. Outra, construída com os mesmos voos, pode sugerir que não existe tendência conclusiva.

Essa diferença parece gráfica. Na realidade, é gerencial. Quem decide o que comparar também decide o que a liderança conseguirá perceber.

A primeira quebra nem sempre está no dado falso. Pode estar no dado verdadeiro apresentado de maneira incapaz de produzir decisão.

A noite anterior

Na teleconferência da noite anterior, engenheiros da empresa responsável pelos foguetes recomendaram não lançar abaixo da menor temperatura já experimentada com segurança. O lançamento anterior mais frio havia ocorrido perto de 12 graus Celsius. Para a manhã seguinte, a previsão estava próxima de zero.

A recomendação deveria ter encerrado a discussão. O componente era crítico, a consequência potencial era catastrófica e não existiam dados que demonstrassem funcionamento naquela condição.

A lógica, contudo, foi invertida. Em vez de a organização provar que o lançamento era seguro, os engenheiros foram pressionados a provar que o frio causaria a falha.

Depois de uma pausa interna, a recomendação foi revertida. A autorização apareceu. A dúvida permaneceu.

A aprovação que não resolveu nada

Houve reunião, dados, assinatura e decisão. A aparência era de governança. Todos os elementos formais estavam presentes.

Mas o objetivo de uma revisão de prontidão não é produzir autorização. É impedir que a operação prossiga enquanto uma dúvida crítica permanecer sem resposta.

Quando uma reunião começa a trabalhar para justificar a continuidade, ela deixa de funcionar como barreira. A ata poderá registrar consenso. O risco continuará exatamente onde estava.

APROVAÇÃO FORMAL	GARANTIA REAL
A decisão possui registro, responsáveis e uma conclusão compatível com o cronograma.	A incerteza foi eliminada ou controlada por evidências suficientes antes de expor pessoas ao risco.

Setenta e três segundos

No momento da ignição, os anéis endurecidos pelo frio não responderam com a velocidade necessária. Pequenos sinais de fumaça apareceram na região da junta.

Resíduos da combustão formaram uma vedação temporária. Por alguns segundos, uma barreira casual fez o trabalho que o projeto deveria garantir.

Quando essa vedação perdeu eficácia, uma chama escapou do foguete auxiliar e atingiu estruturas próximas. O veículo perdeu integridade aos setenta e três segundos.

O Challenger carregava no céu os sinais de missões passadas, uma correção adiada e uma autorização que não resolvera a dúvida técnica.

O frio não criou o risco

O frio tornou visível uma fragilidade que já existia. Em condições mais favoráveis, a borracha respondia melhor e o sistema encontrava margem para sobreviver. Naquela manhã, a margem desapareceu.

Isso explica por que desvios anteriores podem ser mais perigosos quando terminam bem. Eles não apenas deixam de produzir aprendizagem. Produzem confiança na capacidade de continuar.

A organização passa a acreditar que conhece o limite porque já chegou perto dele. Na verdade, conhece apenas as combinações em que teve sorte suficiente para voltar.

A normalização do desvio começa quando a ausência de desastre recebe mais credibilidade do que a presença repetida da anomalia.

Onde a história poderia ter terminado

O lançamento poderia ter sido bloqueado na primeira erosão sem causa eliminada. Poderia ter sido suspenso quando uma força-tarefa reconheceu a gravidade da junta. Poderia ter sido adiado na noite anterior, quando a temperatura prevista saiu da experiência conhecida.

Nenhuma dessas decisões exigia prever o segundo exato da falha. Exigia apenas respeitar uma regra simples: dúvida crítica sem resposta não autoriza exposição catastrófica.

O custo seria um atraso. A tripulação desembarcaria, os dados seriam reorganizados e a junta seria redesenhada. Depois do acidente, foi exatamente isso que ocorreu.

A primeira quebra não foi o O-ring. Foi a perda de autoridade da dúvida técnica.

O PONTO DE RUPTURA

PROTOCOLO

Não lançar diante de uma dúvida crítica não resolvida, especialmente fora da faixa conhecida e com recomendação técnica contrária.

PRIMEIRA QUEBRA

A recomendação de não lançamento foi revertida sem que a incerteza fosse eliminada. O desvio conhecido parecia tolerável porque missões anteriores haviam sobrevivido.

CONSEQUÊNCIA

O O-ring não vedou adequadamente no frio, gases escaparam e o veículo perdeu integridade setenta e três segundos após a decolagem.

SE FOSSE CUMPRIDO

A missão seria adiada. A tripulação desembarcaria, a relação entre temperatura e falha seria revista e a junta seria corrigida antes de outro lançamento.

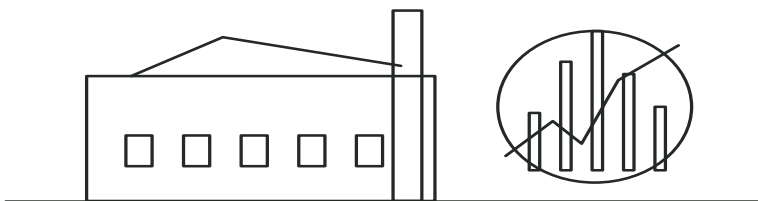
VEREDITO

Os voos anteriores não provaram que o desvio era seguro. Apenas ensinaram a organização a tolerá-lo.

Nota documental: Comissão Rogers, relatório de 1986, v. I. A interpretação sobre normalização do desvio é distinguida da conclusão técnica. Ver ND-04, p. 137.

Quando o processo de aprovação passa a servir à decisão já desejada, o protocolo continua existindo apenas como cenário.

O teste que não precisava terminar



26 de abril de 1986. Naquela madrugada, a unidade 4 de Chernobyl não estava produzindo apenas eletricidade. Estava tentando concluir um teste adiado.

A pergunta parecia legítima: por quanto tempo as turbinas ainda forneceriam energia após a perda da alimentação elétrica, antes que os geradores de emergência assumissem?

O ensaio seria realizado durante a parada programada do reator. O problema começou quando as condições necessárias deixaram de existir e a necessidade de terminar permaneceu.

O teste não precisava terminar naquela noite. O reator precisava voltar ao controle.

Um teste que esperou nove horas

A redução de potência começou durante o dia. A rede elétrica, porém, ainda precisava da geração da usina. O operador do sistema solicitou que o reator permanecesse produzindo por mais algumas horas.

A espera não provocou sozinha o acidente. Mas alterou o cenário. O teste atravessou mudanças de turno, chegou à madrugada e foi entregue a uma equipe que não o havia preparado desde o início.

Planos críticos dependem de condições. Quando o tempo muda, a equipe muda e a operação muda, a primeira obrigação é confirmar se o plano continua válido.

Em Chernobyl, o cronograma do teste continuou vivo mesmo depois que o contexto que o sustentava havia mudado.

Quando a potência despencou

Durante a redução, a potência caiu muito abaixo do previsto, chegando a apenas algumas dezenas de megawatts térmicos. O reator entrou numa condição difícil de controlar.

O combustível acumulava xenônio, um produto que absorvia nêutrons e dificultava a recuperação. Para elevar novamente a potência, muitas barras de controle foram retiradas.

Esse era o momento mais barato para encerrar a história. A condição planejada havia desaparecido. O teste deveria ser interrompido, o reator estabilizado ou desligado e o ensaio remarcado.

A operação, contudo, recuperou parcialmente a potência e prosseguiu.

Um reator fora da faixa

O RBMK possuía características que tornavam a operação em baixa potência especialmente delicada. À medida que a água virava vapor, a reação podia aumentar em vez de diminuir.

Esse comportamento, chamado coeficiente de vazio positivo, não era uma curiosidade acadêmica. Significava que, em determinadas condições, mais vapor poderia produzir mais potência, que produziria ainda mais vapor.

O reator estava com poucas barras efetivamente inseridas, baixa margem operacional e grande quantidade de energia potencial concentrada numa condição instável.

O problema não era apenas executar uma sequência errada. Era executar a sequência correta num sistema que já não correspondia ao cenário para o qual ela havia sido escrita.

Proteções que perderam função

Para realizar o teste, alguns sistemas automáticos e permissivos estavam fora da configuração normal. Nem todos tiveram o mesmo peso causal, mas o conjunto revela uma operação progressivamente dependente de menos barreiras.

Esse detalhe importa. Um protocolo não é uma lista de passos independentes. É uma arquitetura de proteção. Retirar uma defesa pode parecer aceitável quando as demais continuam disponíveis. Retirar várias transforma uma condição anormal em aposta.

A equipe ainda possuía instrumentos, alarmes e o botão de parada. Mas a segurança já dependia de que cada elemento restante funcionasse exatamente como se imaginava.

O teste avançou com uma margem que existia mais no procedimento do que no reator real.

O teste começou

Pouco depois da 1h23, o fluxo de vapor para as turbinas foi interrompido. Elas começaram a perder velocidade, exatamente como o ensaio previa.

As bombas passaram a receber menos energia. O fluxo de água diminuiu. Mais vapor se formou no núcleo. Naquele projeto, a formação de vapor aumentava a reatividade.

À 1h23min40s, a equipe acionou o AZ-5, o comando que deveria inserir as barras de controle e parar o reator. O motivo do acionamento não foi estabelecido pela investigação reproduzida no INSAG-7.

As barras começaram a descer. O que ocorreu nos primeiros instantes revelou um defeito que a própria operação não compreendia plenamente.

O botão que deveria salvar

As barras de controle possuíam pontas de grafite. Ao entrar no núcleo, essas pontas deslocavam água antes que a parte absorvedora ocupasse o mesmo espaço.

Em condições normais, o efeito inicial era limitado. Na configuração extrema daquela madrugada, ele acrescentou reatividade exatamente quando o sistema precisava retirá-la.

A potência aumentou de forma abrupta. Canais de combustível se romperam, a pressão cresceu e o reator foi destruído.

Isso impede a explicação confortável de que bastaria um operador mais atento. A equipe cometeu violações e decisões inadequadas. O sistema, porém, também escondia fragilidades capazes de transformar essas decisões em catástrofe.

A primeira versão da culpa

A explicação inicial concentrou a responsabilidade nos operadores. Eles haviam ultrapassado limites, retirado barras e conduzido o teste fora das condições previstas. Parte dessa descrição era verdadeira.

Era também insuficiente. Anos depois, a revisão internacional conhecida como INSAG-7 ampliou a análise. O projeto do reator, as informações incompletas, a regulamentação e a cultura de segurança passaram a ocupar o centro da explicação.

EXPLICAÇÃO RÁPIDA	EXPLICAÇÃO SISTÊMICA
Os operadores descumpriram o procedimento e provocaram o acidente.	Decisões operacionais inadequadas encontraram um projeto perigoso, informações insuficientes, barreiras reduzidas e governança incapaz de impedir a sequência.

Onde a história poderia ter terminado

A sequência poderia ter sido interrompida quando a rede atrasou o teste. Poderia ter terminado quando a potência caiu muito abaixo da faixa planejada. Poderia ter sido encerrada quando a margem de controle deixou de atender aos limites.

Nenhuma dessas decisões exigia antecipar cada detalhe do comportamento do RBMK. Exigia reconhecer que o experimento já não estava sendo realizado nas condições que justificavam sua execução.

Adiar custaria uma nova preparação, mais tempo de parada e explicações. Continuar preservava o objetivo imediato: concluir o ensaio antes do fim do turno.

A primeira quebra ocorreu quando terminar recebeu mais autoridade do que estabilizar.

O PONTO DE RUPTURA

PROTOCOLO

Interromper o teste quando o reator deixasse a faixa estável e somente retomá-lo após restabelecer as condições operacionais previstas e as barreiras necessárias.

PRIMEIRA QUEBRA

A queda extrema de potência não encerrou o ensaio. A operação continuou numa configuração que já não correspondia ao plano seguro.

CONSEQUÊNCIA

O aumento abrupto de potência destruiu o reator, iniciou incêndios e liberou grande quantidade de material radioativo.

SE FOSSE CUMPRIDO

O teste seria adiado, o reator estabilizado ou desligado e a cadeia daquela madrugada seria interrompida.

VEREDITO

O teste não precisava terminar naquela noite. A primeira quebra ocorreu quando concluí-lo passou a valer mais do que recuperar o controle.

Nota documental: IAEA, INSAG-7 (1992), incluindo a revisão das causas e a incerteza sobre o motivo do acionamento do AZ-5. Ver ND-05, p. 137.

A falha física destruiu o reator. A quebra de protocolo permitiu que um teste substituísse a obrigação de manter o processo sob controle.

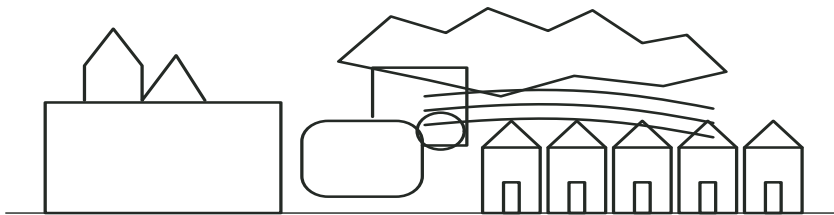
PARTE II

BARREIRAS, MARGENS E SINAIS

Um sistema não está protegido porque possui muitas barreiras. Está protegido quando cada uma consegue perceber a falha da anterior.



A cidade que dormia ao lado do perigo



3 de dezembro de 1984. A cidade dormia. Nas casas próximas à fábrica de pesticidas da Union Carbide, milhares de pessoas encerravam mais um domingo sem saber que uma reação já avançava dentro da unidade.

Não havia uma informação clara capaz de dizer o que estava escapando, para onde correr ou como proteger a família. Pouco depois da meia-noite, moradores acordaram tossindo e saíram às ruas procurando ar.

| A população descobriu o perigo quando já estava dentro dele.

O tanque 610

Dentro da fábrica, a temperatura e a pressão do tanque 610 começaram a subir. O reservatório continha isocianato de metila, conhecido pela sigla MIC, uma substância usada na fabricação de pesticidas e altamente reativa com água.

Água entrou no sistema e iniciou uma reação intensa. O calor acelerou a reação. A reação produziu mais calor. O MIC vaporizou, a pressão aumentou e a válvula de segurança abriu.

Mais de quarenta toneladas de material tóxico escaparam. Como o vapor permaneceu próximo do solo, a nuvem avançou sobre bairros densamente ocupados. Milhares de pessoas morreram nas primeiras horas e nos dias seguintes. Centenas de milhares foram expostas.

A rota exata pela qual a água alcançou o tanque permanece discutida. Essa dúvida importa para reconstruir o evento iniciador. Não altera, porém, a pergunta central deste livro: por que uma contaminação encontrou tão pouco para detê-la?

O perigo já tinha manual

O MIC não era uma substância misteriosa. Sua reação com água, a geração de calor e a facilidade de vaporização eram conhecidas. Por isso, o armazenamento precisava ser limitado, refrigerado e cercado por defesas capazes de ganhar tempo.

A refrigeração não impediria toda contaminação. Reduziria a velocidade da reação e ampliaria o intervalo disponível para reconhecer o problema, transferir o produto ou conter a liberação.

O sistema de refrigeração, contudo, estava fora de operação havia meses. O MIC permanecia próximo da temperatura ambiente. Durante esse período, a fábrica não sofreu uma grande liberação.

Esse silêncio ensinou a lição errada. A proteção começou a parecer cara e dispensável justamente porque continuava cumprindo sua função de forma invisível.

Quando a barreira foi retirada, a organização não economizou somente energia. Reduziu o tempo entre o primeiro desvio e a perda do controle.

As barreiras que existiam no desenho

A refrigeração era apenas uma camada. Um lavador deveria neutralizar vapores. Uma torre de queima deveria destruir o material que ainda escapasse. Um tanque de reserva deveria permitir a transferência em emergência. Uma cortina de água poderia limitar pequenas liberações.

Naquela noite, as proteções não estavam disponíveis para o cenário real. A torre de queima estava fora de serviço. O lavador não possuía capacidade para a descarga. O tanque de emergência não estava livre. A água lançada do lado de fora não alcançava adequadamente o ponto de emissão.

A unidade possuía equipamentos de segurança registrados em desenhos, inventários e inspeções. Não possuía, porém, um sistema de segurança capaz de responder à combinação que ocorria.

Redundância não é contar quantos dispositivos aparecem no fluxograma. É demonstrar que cada defesa continua disponível, possui capacidade suficiente e não depende do mesmo ponto de falha das demais.

Economizar onde ninguém vê

Barreiras críticas possuem uma característica ingrata: quando funcionam, não produzem espetáculo. A produção segue, o produto sai e o acidente não acontece. Por isso, manutenção, treinamento e disponibilidade podem ser tratados como custos que não entregam resultado visível.

Reconstruções do desastre apontaram degradação da manutenção, redução de pessoal e perda de capacidade operacional. Nenhuma dessas condições, isoladamente, liberou a nuvem. Juntas, diminuíram a probabilidade de reconhecer, conter e responder ao evento.

A organização continuava armazenando uma substância extremamente perigosa, mas já não sustentava a mesma capacidade técnica que justificara aquela operação. O risco permaneceu. As condições para controlá-lo encolheram.

O problema não é economizar. Toda organização precisa escolher onde investir. A quebra ocorre quando a redução de custo altera uma defesa crítica sem uma nova prova de que o risco continua controlado.

A cidade sem protocolo

Do lado de fora dos muros, a comunidade também dependia de barreiras. Moradores precisavam saber que risco existia, como reconhecer um alarme, para onde se deslocar e que orientação seguir. Hospitais precisavam conhecer o agente e preparar uma resposta compatível.

Bhopal mostrou que um plano de emergência não pode começar na portaria da fábrica. Quando a consequência atravessa o limite da propriedade, informação, comunicação e coordenação pública passam a integrar o mesmo sistema de controle.

Naquela madrugada, a população recebeu o evento antes de receber a explicação. Pessoas correram em direções diferentes. Serviços de saúde enfrentaram uma emergência sem informação proporcional à velocidade da exposição.

A obrigação de prevenir não termina onde começa a comunidade. Quanto maior a consequência possível, maior deve ser a independência entre prevenção interna, alerta externo e resposta pública.

Não foi uma única quebra

Seria confortável reduzir a história à entrada de água. Um evento iniciador possui utilidade porque localiza o começo físico da reação. Mas não explica por que a reação atravessou todas as defesas e alcançou uma cidade inteira.

O operador controla tarefas específicas. Não decide sozinho quanto produto será armazenado, quais sistemas permanecerão disponíveis, quantas pessoas estarão no turno, que manutenção será adiada ou que informação chegará à comunidade.

Essas condições pertencem a uma arquitetura de autoridade. Direção, engenharia, manutenção, operação, segurança e governo possuem deveres diferentes. A análise sistêmica não dissolve responsabilidade. Ela a distribui até o nível em que cada condição foi criada, aceita ou mantida.

Quando uma investigação termina em “erro operacional”, ela pode registrar a ação final e perder as decisões que tornaram aquela ação capaz de atravessar o conjunto inteiro.

Onde a história poderia ter terminado

A unidade poderia reduzir o estoque de MIC. Poderia interromper o armazenamento enquanto a refrigeração e as defesas estivessem indisponíveis. O tanque de emergência poderia permanecer livre. A comunidade poderia receber informação e exercícios de resposta.

Nenhuma dessas medidas tornaria a substância inofensiva. Esse não é o objetivo de um protocolo. Um protocolo não elimina a realidade física. Cria limites para que uma falha encontre outra defesa antes de alcançar a consequência.

Parar custaria produção. Reduzir estoque exigiria outra logística. Restaurar equipamentos consumiria dinheiro. Informar a comunidade exporia a existência do risco. Todos esses custos eram visíveis.

O custo do desastre permanecia abstrato, distante e difícil de colocar numa planilha. Até deixar de ser.

O PONTO DE RUPTURA

PROTOCOLO

Manter o MIC refrigerado, limitar o estoque e garantir que neutralização, queima, transferência, contenção e resposta de emergência estivessem disponíveis.

PRIMEIRA QUEBRA

A unidade continuou armazenando grande quantidade de MIC enquanto a refrigeração e outras barreiras críticas estavam indisponíveis ou insuficientes.

CONSEQUÊNCIA

A entrada de água iniciou uma reação descontrolada. Sem contenção eficaz, material tóxico escapou e alcançou a população vizinha.

SE FOSSE CUMPRIDO

A operação seria interrompida ou o estoque reduzido até a restauração das defesas. A reação encontraria tempo e sistemas capazes de limitá-la.

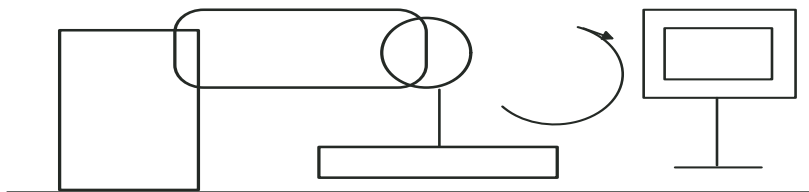
VEREDITO

A água iniciou a reação. A primeira quebra retirou as barreiras que impediriam a reação de alcançar a cidade.

Nota documental: Bloch e Jung, análise técnica publicada pela IChemE (2014). A rota exata de entrada da água permanece controversa. Ver ND-06, p. 138.

Uma organização não possui uma barreira porque a comprou. Possui quando consegue demonstrar que ela estará disponível no pior momento.

A máquina disse que estava tudo bem



21 de março de 1986. A sala de tratamento estava fechada. No East Texas Cancer Center, em Tyler, uma técnica corrigiu rapidamente no terminal a modalidade de radioterapia.

A tela confirmou os parâmetros e declarou que o Therac-25 estava pronto. Pouco depois da ativação, surgiu uma mensagem curta e pouco esclarecedora: “Malfunction 54”.

A máquina interrompeu o tratamento. O sistema, porém, não explicou por quê.

O painel dizia que quase nada havia acontecido

A tela informava que apenas uma pequena fração da dose havia sido aplicada. O comando para continuar permanecia disponível. A operadora, experiente e acostumada a mensagens de baixa gravidade, retomou o tratamento.

O paciente percebeu imediatamente uma sensação intensa e tentou sair da posição. O vídeo e o áudio da sala não funcionavam. A pessoa que comandava o equipamento não podia ver nem ouvir com clareza o que acontecia do outro lado da parede.

O painel oferecia uma realidade. O paciente experimentava outra. Entre as duas, o sistema escolheu acreditar em si mesmo.

Uma mensagem de falha não é uma barreira completa. Precisa indicar gravidade, bloquear a sequência apropriada e conduzir a uma reação compatível com a incerteza.

A falha que só aparecia nas mãos de alguém competente

Engenheiros não conseguiram reproduzir o problema. A máquina voltou ao serviço. Três semanas depois, a mesma clínica registrou uma ocorrência semelhante.

A causa estava ligada à velocidade com que uma operadora experiente corrigia os dados. Uma sequência rápida de comandos podia deixar o software numa configuração interna incompatível com aquilo que a tela mostrava.

Nos testes, os comandos eram introduzidos lentamente. Na rotina, profissionais treinados trabalhavam com rapidez. O equipamento fora validado numa realidade diferente daquela em que seria usado.

Isso muda a pergunta sobre treinamento. Competência não é apenas executar o procedimento como foi imaginado pelo projetista. É operar no ritmo real sem que a habilidade se transforme numa condição não prevista pelo sistema.

O software que conferia a própria resposta

Modelos anteriores da família possuíam intertravamentos físicos. No Therac-25, parte dessas proteções foi retirada e o software assumiu funções de comando, verificação e defesa.

O mesmo sistema que definia a configuração também confirmava que ela estava correta. Quando uma falha lógica alterava o estado interno, várias camadas podiam concordar com a mesma informação errada.

Isso parecia redundância. Era repetição da mesma dependência. Um sensor independente, um circuito elétrico separado ou um bloqueio mecânico não precisam ser mais inteligentes do que o software. Precisam apenas impedir que um erro digital atravessasse sozinho o caminho até o mundo físico.

A primeira ocorrência deveria retirar a máquina de serviço

Entre 1985 e 1987, seis exposições graves foram associadas ao Therac-25. As circunstâncias não foram idênticas, mas a repetição mostrou falhas de projeto, mensagens pouco claras, investigação fragmentada e retorno prematuro ao uso.

Em produtos críticos, uma falha não compreendida não pode ser tratada como evento encerrado apenas porque não foi reproduzida no laboratório. A incapacidade de repetir a anomalia aumenta a incerteza. Não reduz sua gravidade.

Reclamações, eventos de campo e relatos de usuários são sensores externos do projeto. Quando chegam, a organização precisa reuni-los, compará-los e procurar o padrão que cada unidade isolada pode esconder.

O recall, a correção de campo ou a retirada temporária possuem custo imediato. Continuar em operação transfere esse custo para pessoas que não participaram da decisão.

O PONTO DE RUPTURA

PROTOCOLO

Manter intertravamentos físicos independentes, validar o software sob condições reais e bloquear o equipamento diante de falhas não compreendidas.

PRIMEIRA QUEBRA

O projeto concentrou no software as funções de controle, verificação e proteção, sem preservar todas as barreiras independentes dos modelos anteriores.

CONSEQUÊNCIA

Falhas de sincronização permitiram configurações incompatíveis. Mensagens pouco claras e retorno prematuro ao serviço permitiram repetição.

SE FOSSE CUMPRIDO

Uma barreira independente impediria a ativação incorreta. A primeira ocorrência retiraria os equipamentos de serviço até a correção comprovada.

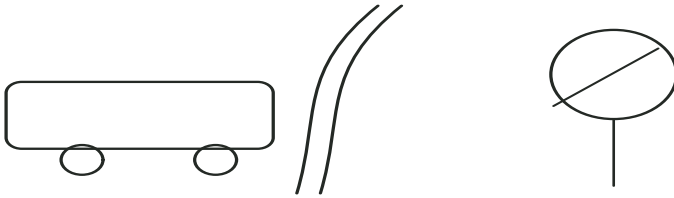
VEREDITO

O software executou o comando perigoso. A primeira quebra ocorreu quando o projeto retirou as barreiras capazes de impedir que o erro digital alcançasse o mundo físico.

Nota documental: Leveson e Turner, Computer (1993). As seis ocorrências tiveram circunstâncias distintas; registros regulatórios são acessados por intermédio do estudo. Ver ND-07, p. 138.

Bhopal mostrou barreiras indisponíveis. O Therac-25 mostrou algo igualmente perigoso: várias proteções que dependiam da mesma verdade errada.

Quando uma pessoa vira a última barreira



A curva que dependia da memória

Angrois, Espanha, 24 de julho de 2013

O trem aproximava-se de uma curva limitada a 80 quilômetros por hora. Vinha de um trecho percorrido a velocidade muito superior. Na cabine, uma chamada operacional fez o maquinista perder a referência de sua posição por alguns instantes.

Quando reconheceu a proximidade da curva, acionou o freio de emergência. Era tarde. O trem entrou rápido demais e descarrilou. O acidente provocou 80 mortes.

A distração foi real e a responsabilidade do condutor não desaparece. A quebra anterior estava numa transição crítica sem proteção automática capaz de impor a redução caso a ação humana chegasse tarde.

LIMITE: Uma redução crítica deveria ser supervisionada e, se necessário, executada automaticamente.

QUEBRA: A última defesa foi transferida à memória e à atenção de uma única pessoa.

CONSEQUÊNCIA: Uma chamada operacional transformou o atraso da frenagem em descarrilamento.

A troca de turno que perdeu a verdade

Piper Alpha, Mar do Norte, 6 de julho de 1988

Uma bomba de condensado estava em manutenção. Sua válvula de segurança havia sido removida, e a abertura permanecia fechada apenas por uma vedação temporária. A intervenção não terminara. A bomba não poderia ser acionada.

Segundo a reconstrução mais provável do inquérito Cullen, a condição não chegou com clareza ao turno da noite. Quando a outra bomba parou, o equipamento em manutenção foi acionado. O vazamento iniciou a sequência que, ampliada por outras falhas, causou 167 mortes.

A permissão de trabalho existia. O bloqueio não atravessou a troca de turno como uma verdade inequívoca no campo, no painel e na documentação.

LIMITE: Equipamento desmontado deve permanecer fisicamente e administrativamente indisponível.

QUEBRA: A condição crítica ficou separada da decisão de partida.

CONSEQUÊNCIA: Uma bomba em manutenção voltou à operação e abriu caminho para o desastre.

Nota documental: Inquérito Cullen (1990), v. 1 e 2. A sequência da bomba é a reconstrução considerada mais provável; outras falhas ampliaram o desastre. Ver ND-09, p. 139.

O teste que provou a condição errada

Lac-Mégantic, Canadá, 6 de julho de 2013

Um trem carregado com petróleo bruto foi estacionado num trecho inclinado. Sete freios manuais foram aplicados. O teste indicou que a composição permanecia imóvel e o resultado foi aceito como prova de segurança.

Mais tarde, a locomotiva foi desligada durante o combate a um incêndio. A pressão dos freios pneumáticos diminuiu. Os freios manuais não sustentaram o peso. O trem desceu sem ninguém a bordo e descarrilou no centro da cidade, causando 47 mortes.

O teste preservava a ajuda pneumática que deveria remover. Confirmou a estabilidade de uma configuração diferente daquela em que o trem seria deixado.

LIMITE: O teste deveria liberar todos os freios pneumáticos e provar a capacidade dos freios manuais isoladamente.

QUEBRA: A verificação não separou as barreiras e ocultou a insuficiência da defesa permanente.

CONSEQUÊNCIA: Quando a pressão desapareceu, a gravidade encontrou o caminho livre.

O mesmo erro em três sistemas

Um trem de passageiros, uma plataforma de petróleo e uma composição de carga parecem histórias distantes. Nas três, porém, uma pessoa ou um teste tornou-se a última defesa porque o sistema não sustentou uma barreira independente.

CASO	ÚLTIMO ELO VISÍVEL	BARREIRA QUE FALTOU
Angrois	Condutor distraído	Proteção automática da redução crítica
Piper Alpha	Operador que iniciou a bomba	Bloqueio inequívoco e passagem de turno
Lac-Mégantic	Teste aceito como suficiente	Verificação isolada dos freios manuais

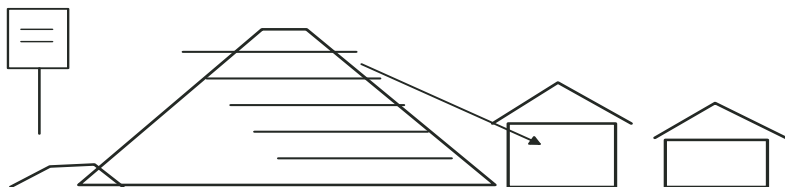
Pessoas erram, esquecem, interpretam e se distraem. Um sistema robusto não nega essa realidade. É construído para que uma única ação não atravesse sozinha todas as defesas.

Essa não é uma defesa da irresponsabilidade individual. É uma exigência de responsabilidade organizacional. A pessoa responde pelo que fez. A liderança responde pelo sistema que permitiu que aquele gesto fosse suficiente para produzir a consequência.

A próxima pergunta do livro será ainda mais incômoda: o que acontece quando os alertas existem, mas a organização aprende a não ouvi-los?

Fontes dos casos deste interlúdio: ND-08, p. 139; ND-09, p. 139; ND-10, p. 140.

A barragem que já não podia confiar nos próprios sinais



25 de janeiro de 2019. Era hora do almoço na Mina Córrego do Feijão. Caminhões circulavam, equipes atravessavam os prédios administrativos e trabalhadores ocupavam o refeitório instalado abaixo da Barragem I.

Às 12h28, a estrutura perdeu estabilidade. A massa de rejeitos avançou com velocidade sobre instalações, veículos, vegetação e comunidades. Em poucos minutos, a rotina desapareceu sob a lama.

O rompimento tirou 272 vidas, incluindo dois nascituros. Muitas vítimas estavam onde o alerta de emergência já não poderia alcançá-las a tempo.

A estabilidade que existia no documento

A Barragem I estava inativa para recebimento de rejeitos havia anos. Isso não a tornava um objeto imóvel. Barragens continuam mudando depois do último alteamento: água se desloca, materiais se adensam, tensões se redistribuem e pequenos movimentos podem anunciar uma condição diferente daquela descrita no projeto.

O sistema de controle reunia inspeções, instrumentos, relatórios e declarações periódicas de estabilidade. Esses elementos produziam uma conclusão formal: a barragem podia permanecer na condição em que estava.

Uma declaração, porém, não estabiliza uma estrutura. Ela apenas registra que, com base nos dados, critérios e interpretações utilizados, alguém considerou a estabilidade demonstrada.

Quando a realidade muda mais rápido do que o método de avaliação consegue reconhecer, o papel continua válido por algum tempo. A estrutura, não.

O modo de falha que não pede licença

O painel técnico que investigou as causas concluiu que a ruptura ocorreu por liquefação estática. Em termos simples, materiais que pareciam sustentar a barragem perderam resistência e passaram a se comportar como uma massa fluida.

A falha foi súbita para quem a observou em vídeo. Não necessariamente para o material. As análises posteriores identificaram condições formadas ao longo do tempo: geometria íngreme, rejeitos vulneráveis, estado de tensões elevado e água suficiente para reduzir a resistência disponível.

O colapso começou perto da crista e se propagou rapidamente pela estrutura. Não houve uma sequência lenta, visível e generosa, capaz de permitir evacuação depois do primeiro grande movimento.

Esperar uma confirmação inequívoca de instabilidade pode parecer prudência técnica. Em certos sistemas, significa esperar o instante em que já não existe decisão útil.

Os sinais que não formaram uma decisão

A investigação posterior encontrou pequenas deformações externas medidas por dados de satélite desde meados de 2015. Isoladamente, movimentos discretos podem ter explicações diferentes. O problema não é exigir que cada sinal anuncie sozinho uma catástrofe. É deixar de reuni-los numa pergunta suficientemente incômoda.

Instrumentos produzem números. Engenheiros produzem interpretações. Gestores produzem decisões. Entre medir e parar existe uma cadeia inteira de critérios, responsabilidades, independência e autoridade.

O monitoramento pode falhar de três maneiras. Pode não medir. Pode medir sem compreender. Ou pode compreender uma incerteza relevante e ainda assim não alterar o plano.

Em Brumadinho, o sistema continuou produzindo estabilidade administrativa enquanto a estrutura acumulava uma condição que os métodos utilizados não transformaram em interdição.

A certificação que precisava discordar

Grandes organizações recorrem a especialistas externos para acrescentar independência. O princípio é correto: quem avalia uma condição crítica deve possuir liberdade técnica para contrariar a área que deseja continuar operando.

A independência, contudo, não nasce apenas de um contrato ou de uma assinatura profissional. Depende de acesso completo aos dados, critérios conservadores, ausência de pressão indevida e consequências claras quando a evidência não é suficiente.

Uma certificação perde sua função quando se torna uma etapa necessária para manter o calendário. Nesse momento, a pergunta deixa de ser “a segurança foi demonstrada?” e passa a ser “o que falta para emitir o documento?”

A barragem possuía avaliações. O desastre demonstrou que o conjunto de verificações não foi capaz de produzir a única conclusão que teria protegido as pessoas: não permanecer abaixo dela enquanto a segurança não estivesse demonstrada.

O refeitório dentro da consequência

Mesmo uma barragem considerada estável possui uma zona de inundação potencial. O plano de emergência existe porque a organização admite que a prevenção pode falhar e precisa proteger as pessoas da consequência.

Em Córrego do Feijão, instalações administrativas e o refeitório estavam na trajetória direta dos rejeitos. A sirene não ofereceria tempo suficiente para retirar centenas de pessoas depois do início do rompimento. A última barreira dependia de um aviso que chegaria tarde demais para quem estava mais exposto.

Localizar pessoas na mancha de inundação não é uma decisão neutra. Significa aceitar que a segurança delas dependerá da estabilidade permanente da estrutura ou de um sistema de alerta mais rápido do que o próprio desastre.

A ausência de tempo não foi criada no minuto do rompimento. Foi incorporada ao sistema quando atividades permanentes permaneceram dentro da área que a própria análise de consequências reconhecia como perigosa.

O segundo aviso nacional

Quatro anos antes, o rompimento da Barragem de Fundão, em Mariana, já havia demonstrado a dimensão humana, ambiental e institucional de uma falha em estruturas de rejeitos.

Os dois casos não possuem a mesma causa técnica e não devem ser tratados como cópias. Compartilham, porém, uma obrigação gerencial evidente: depois de um desastre de grande escala, todas as estruturas comparáveis precisam ser reavaliadas com um nível de dúvida maior do que aquele que existia antes.

Aprender não é publicar uma nova norma, formar um comitê ou acrescentar uma assinatura. É alterar decisões, critérios, localizações, recursos e prazos de modo que a repetição se torne menos provável.

A reincidência sistêmica não exige repetir o mesmo mecanismo físico. Basta repetir a incapacidade de transformar conhecimento disponível em uma barreira real.

O que quebrou primeiro?

A causa física foi uma perda rápida de resistência associada à liquefação estática. Essa conclusão explica como a barragem se rompeu. Não explica, sozinha, por que 272 pessoas permaneceram expostas a uma estrutura cuja falha não ofereceria tempo útil de fuga.

A quebra sistêmica ocorreu na distância entre possuir informações e produzir uma decisão conservadora. Avaliações, instrumentos e documentos não convergiram para interdição. O plano de emergência não compensava a localização das instalações. A arquitetura dependia de a barragem continuar estável porque, se não continuasse, a resposta chegaria tarde.

É possível discutir quais dados eram conclusivos antes do rompimento. Não é necessário inventar um alarme perfeito para reconhecer uma falha de

governança: um sistema de consequências catastróficas precisa ser capaz de agir diante da incerteza, não apenas depois da certeza.

O PONTO DE RUPTURA

PROTOCOLO

Barragens críticas devem ter segurança demonstrada por avaliação tecnicamente independente, monitoramento capaz de detectar mudanças relevantes e planos de emergência compatíveis com o tempo real de resposta.

PRIMEIRA QUEBRA

O sistema aceitou estabilidade formal sem transformar sinais, incertezas e consequências em interdição ou retirada das pessoas da zona de impacto.

CONSEQUÊNCIA

A ruptura por liquefação estática avançou sobre instalações e comunidades, tirou 272 vidas e espalhou rejeitos pela bacia do Rio Paraopeba.

SE FOSSE CUMPRIDO

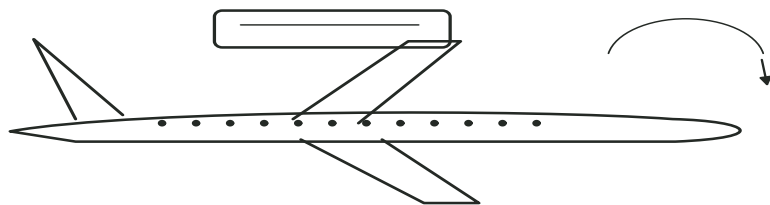
A ausência de segurança demonstrada levaria à evacuação preventiva, à retirada permanente de instalações da mancha de inundação ou à desativação controlada da estrutura.

VEREDITO

A liquefação explica o mecanismo. A quebra do sistema de decisão explica por que tantas vidas permaneceram dependentes de uma barragem que não poderia falhar.

Nota documental: Painel técnico de 2019, CPI da ALMG e documentação estadual. O painel foi contratado por assessoria jurídica externa da Vale. A contagem de 272 vidas inclui dois nascituros. Ver ND-11, p. 140.

O avião que sabia mais que o piloto



29 de outubro de 2018. O voo Lion Air 610 decolou de Jacarta com 189 pessoas a bordo. Pouco depois, o nariz do Boeing 737 MAX começou a baixar repetidamente, como se o avião insistisse numa verdade que a tripulação não conseguia enxergar.

Os pilotos puxavam. O sistema voltava a comandar o estabilizador. Alarmes, indicações conflitantes e forças crescentes ocupavam a cabine. Treze minutos depois da decolagem, a aeronave atingiu o mar.

O sistema que pretendia ajudar o piloto tornou-se o risco que ele precisava descobrir durante a emergência.

Um avião novo com aparência familiar

O 737 MAX foi desenvolvido como evolução de uma família conhecida por companhias e pilotos. Motores maiores e sua nova posição alteraram características aerodinâmicas em determinadas condições. Para preservar uma resposta semelhante à dos modelos anteriores, foi criado o MCAS, um sistema automático capaz de comandar o estabilizador e baixar o nariz.

Adicionar automação não é uma quebra. Sistemas automáticos podem ampliar segurança e reduzir carga de trabalho. A quebra aparece quando a autoridade concedida ao software é maior do que a transparência, a redundância e o treinamento concedidos às pessoas que precisarão enfrentá-lo.

O MCAS não ocupava posição proporcional nos materiais e no treinamento inicial dos pilotos. Um avião vendido como continuação familiar carregava uma lógica nova capaz de agir sobre um comando essencial.

Quando uma mudança é escondida para preservar simplicidade, a organização economiza treinamento e transfere complexidade para o pior momento possível: a falha.

Uma verdade entregue por um único sensor

Embora a aeronave possuísse dois sensores de ângulo de ataque, o MCAS podia ser acionado a partir da informação de apenas um deles. Se esse sensor enviasse um valor incorreto, o sistema poderia interpretar que o avião se aproximava de uma condição perigosa e comandar o nariz para baixo.

A análise de segurança pressupunha que os pilotos reconheceriam e corrigiriam rapidamente um comando indesejado do estabilizador. Essa expectativa parecia razoável nos modelos, nos testes e nos tempos assumidos.

Na cabine real, porém, a falha não chegava com uma etiqueta dizendo “MCAS”. Chegava misturada a alarmes, forças no manche, indicações discordantes e repetição do comando automático.

A redundância aparente desapareceu no ponto crítico. Dois sensores existiam. Uma única leitura possuía autoridade para iniciar a sequência.

Depois do primeiro acidente

A queda do Lion Air transformou uma hipótese de projeto em acontecimento real. A partir daquele momento, a pergunta já não era se uma leitura incorreta poderia ativar o sistema. Era como impedir que isso voltasse a ocorrer antes que a causa estivesse completamente corrigida.

Foram emitidas orientações para que pilotos reconhecessem e respondessem a um movimento indesejado do estabilizador. A frota permaneceu em operação enquanto a investigação avançava e alterações de software eram preparadas.

Uma orientação pode ser uma contenção adequada quando a condição é compreendida, a resposta é simples e o risco residual está demonstrado. Torna-se frágil quando exige que pessoas compensem, sob pressão, uma arquitetura que ainda conserva o mesmo poder de produzir a falha.

O sistema ganhou uma explicação. Ainda não ganhou todas as barreiras necessárias.

Cinco meses depois

Em 10 de março de 2019, o voo Ethiopian Airlines 302 decolou de Adis Abeba. Pouco depois, a tripulação enfrentou outra sequência de comandos de nariz para baixo. O avião caiu seis minutos após a partida. As 157 pessoas a bordo morreram.

Os dois acidentes mataram 346 pessoas. Só depois do segundo a frota mundial foi imobilizada. A correção exigiu mudanças no software, na utilização dos sensores, na autoridade do MCAS, nos procedimentos e no treinamento.

A indústria chamou o resultado de recertificação. O aprendizado mais profundo não estava apenas no código. Estava na relação entre pressão comercial, classificação de risco, delegação regulatória, comunicação com pilotos e confiança excessiva em suposições sobre desempenho humano.

Um sistema automático não elimina o erro humano. Pode apenas deslocá-lo para quem especifica, programa, valida, certifica e decide continuar.

O PONTO DE RUPTURA

PROTOCOLO

Mudanças com autoridade sobre controles críticos devem ser avaliadas com análise de perigos conservadora, redundância real, informação clara aos usuários, treinamento adequado e certificação independente.

PRIMEIRA QUEBRA

O MCAS recebeu autoridade relevante, dependia de uma única leitura e foi integrado a um avião apresentado como familiar sem comunicação e treinamento proporcionais ao risco.

CONSEQUÊNCIA

Ativações indevidas contribuíram para os acidentes dos voos Lion Air 610 e Ethiopian 302, nos quais morreram 346 pessoas.

SE FOSSE CUMPRIDO

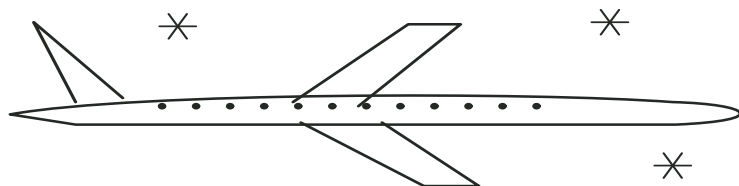
O sistema utilizaria sensores comparados, teria autoridade limitada, falharia de forma transparente e exigiria treinamento antes da entrada em serviço. Após o primeiro acidente, a frota seria contida até a barreira estar demonstrada.

VEREDITO

O sensor forneceu a informação errada. A quebra ocorreu quando o sistema recebeu poder para acreditar nela mais rapidamente do que o piloto conseguia compreender e contrariar.

Nota documental: Relatórios KNKT e EAIB, recomendações do NTSB e relatório parlamentar dos EUA. As divergências do NTSB sobre ET302 são explicitadas na nota. Ver ND-12, p. 141.

O alerta que perdeu autoridade



9 de agosto de 2024. O voo 2283 da Voepass deixou Cascavel com destino a Guarulhos. A bordo do ATR 72-500, matrícula PS-VPB, estavam 58 passageiros e quatro tripulantes.

Durante o cruzeiro, a aeronave encontrou condições meteorológicas associadas à formação severa de gelo. O acúmulo aumentou o arrasto, reduziu a velocidade e degradou o desempenho até o estol. A queda, em Vinhedo, encerrou a vida das 62 pessoas a bordo.

O gelo produziu o mecanismo físico. A perda de autoridade das barreiras permitiu que o voo chegasse até ele.

A pane que desapareceu do sistema

O Relatório Final do CENIPA registrou que o sistema Airframe De-Icing, responsável por remover gelo de superfícies críticas da estrutura, apresentara falhas anteriores. Essas ocorrências não foram formalmente incorporadas ao Diário Técnico de Bordo.

A informação existia entre pessoas. Não existia, porém, no mecanismo que obrigaria manutenção, operações e despacho a reagir. Sem o registro, a pane não gerava avaliação pela lista de equipamentos mínimos, correção técnica, substituição da aeronave ou restrição proporcional ao risco.

Quando uma falha não é registrada, ela não desaparece da aeronave. Desaparece apenas do sistema encarregado de impedir que a falha avance.

O voo começou sem a barreira

A síntese oficial é direta: a aeronave foi despachada com o sistema de degelo da estrutura inoperante e, durante o cruzeiro, encontrou condições adversas de gelo severo. O planejamento colocou uma proteção degradada exatamente no ambiente em que ela seria mais necessária.

Havia ainda uma falha no limpador de para-brisa que, segundo a investigação, já impediria o despacho, embora não tenha contribuído diretamente para o acidente. O detalhe importa porque revela uma disciplina operacional

enfraquecida antes da decolagem. O problema não era apenas uma peça. Era a facilidade com que condições impeditivas deixavam de impedir.

Quando o alerta vira ruído

Durante o voo, o sistema de monitoramento de desempenho emitiu repetidos avisos de velocidade de cruzeiro baixa. Também apareceu o alerta de desempenho degradado. A tripulação comentou o gelo e a anomalia do sistema, mas as respostas previstas não foram executadas com a rapidez e a consistência necessárias.

O relatório discutiu fenômenos como cegueira e surdez por desatenção. Sob carga elevada, uma pessoa pode olhar para um sinal sem integrá-lo à decisão. Essa explicação não elimina responsabilidade. Mostra por que sistemas críticos não podem depender apenas de percepção individual no momento de maior pressão.

Um alerta só é uma barreira quando possui significado conhecido, procedimento praticável e autoridade para mudar a ação. Quando avisos semelhantes se repetem sem consequência ou quando a organização aprende a conviver com anomalias, o som permanece. O poder de interromper desaparece.

Da exceção à cultura

A investigação descreveu uma cultura de informalidade. Pilotos e mecânicos deixavam de registrar problemas para permitir que aeronaves continuassem operando. Uma exceção parecia resolver o dia seguinte. Na realidade, retirava do sistema a memória necessária para reconhecer recorrência, acumular evidência e impor correção.

Esse mecanismo é conhecido. O desvio ocorre uma vez e nada acontece. Repete-se, continua sem consequência e passa a parecer aceitável. Depois, a ausência de acidente é tratada como demonstração de segurança. A organização confunde sorte acumulada com controle comprovado.

A espiral final foi rápida. A construção da vulnerabilidade não foi.

Não houve uma única quebra

O registro técnico perdeu eficácia. A manutenção não recebeu a verdade completa. O despacho não conteve a aeronave. O planejamento não reconciliou condição técnica e meteorologia. Alertas não produziram mudança suficiente. A supervisão organizacional e a vigilância regulatória não restabeleceram as barreiras antes do voo.

Nenhuma dessas camadas, isoladamente, explica toda a ocorrência. Juntas, porém, mostram por que a análise não pode terminar na cabine. O piloto executa a última decisão visível. A organização decide quais informações chegarão até ele, quais panes serão tratadas, quais desvios serão tolerados e quanto risco será transferido para o momento em que já não existe margem.

O CENIPA não atribui culpa civil ou penal. Seu trabalho identifica fatores contribuintes e recomenda prevenção. A leitura sistêmica acrescenta outra pergunta: em qual momento ainda existia uma escolha capaz de impedir que o gelo se transformasse em destino?

A resposta aparece antes da formação do estol. Aparece no primeiro problema que não entrou no registro formal e, por isso, não encontrou uma organização obrigada a parar.

O PONTO DE RUPTURA

PROTOCOLO

Falhas técnicas devem ser registradas no Diário Técnico de Bordo, avaliadas pela manutenção e pela lista de equipamentos mínimos, confrontadas com a meteorologia e transformadas em restrição, correção ou impedimento de despacho.

PRIMEIRA QUEBRA

Falhas anteriores do sistema Airframe De-Icing não foram formalmente registradas. A realidade técnica deixou de produzir uma reação obrigatória do sistema.

CONSEQUÊNCIA

A aeronave foi despachada com uma barreira crítica degradada, encontrou gelo severo, perdeu desempenho, entrou em estol e evoluiu para perda de controle em voo.

SE FOSSE CUMPRIDO

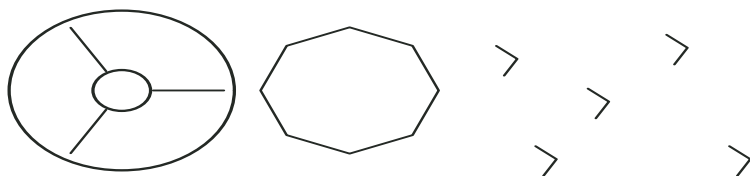
O registro acionaria manutenção e despacho. A aeronave seria reparada, substituída ou impedida de operar em condições de gelo. Durante o voo, os alertas produziram saída imediata da condição degradada e declaração proporcional à emergência.

VEREDITO

O gelo foi o agente físico. A quebra começou quando uma pane conhecida pôde permanecer fora do sistema formal e terminou quando alertas sucessivos já não conseguiram mudar a decisão.

Nota documental: CENIPA, A-116/CENIPA/2024, publicado em 23 jul. 2026. Identificação e publicação confirmadas; a nota informa o limite de acesso ao inteiro teor. Finalidade preventiva. Ver ND-13, p. 142.

Quando o desvio chega ao público



O airbag que se transformou em perigo

Takata, recall global O airbag existe para se abrir em frações de segundo e proteger o ocupante. Em milhões de veículos, infladores fabricados pela Takata podiam fazer o contrário: romper-se durante o acionamento e lançar fragmentos metálicos dentro da cabine.

A degradação estava associada, especialmente, à exposição prolongada a calor e umidade em infladores com propelente de nitrato de amônio estabilizado sem agente dessecante. O risco aumentava com o tempo e com o ambiente.

O desafio deixou de ser apenas fabricar corretamente. Passou a ser identificar veículos, priorizar os mais expostos, comunicar proprietários e substituir uma barreira de segurança distribuída por diferentes marcas e gerações.

LIMITE: Um componente de proteção deve permanecer seguro durante toda a vida prevista e ser rastreável quando sua condição muda.

QUEBRA: A barreira se degradou no campo e a reação precisou alcançar uma população dispersa antes do próximo acionamento.

CONSEQUÊNCIA: O airbag criado para reduzir a consequência tornou-se uma fonte adicional de dano.

Quando encontrar Listeria não foi suficiente

Blue Bell Creameries, 2015

Sorvete é consumido pronto. Não existe uma etapa doméstica de cozimento capaz de corrigir aquilo que saiu da fábrica. Por isso, a última barreira precisa funcionar antes da embalagem.

Em 2015, uma investigação relacionou produtos da Blue Bell a um surto de listeriose. Dez pessoas foram incluídas na contagem final do surto e três morreram. Análises de amostras de produto e do ambiente encontraram *Listeria monocytogenes* em instalações da empresa.

O caso mostrou a diferença entre detectar e controlar. Um resultado microbiológico só se torna barreira quando produz bloqueio, investigação do nicho, higienização eficaz, verificação e decisão de não liberar até que a causa esteja dominada.

LIMITE: Achados ambientais e de produto devem interromper a liberação e iniciar uma investigação capaz de eliminar a fonte.

QUEBRA: A presença do microrganismo atravessou equipamentos, ambiente, produto e resposta antes que toda a produção fosse retirada.

CONSEQUÊNCIA: Alimentos prontos chegaram ao consumo e o controle microbiológico tornou-se um recall nacional.

A água que obedecia ao sistema e falhava para a população

Flint, Michigan, 2014-2016

Em abril de 2014, Flint mudou sua fonte de abastecimento para o rio Flint. A água distribuída sem controle de corrosão adequado atacou tubulações e conexões. O chumbo não precisava estar em alta concentração na saída da estação: podia ser liberado dentro da rede e das próprias casas.

Moradores reclamaram de cor, odor e sabor. Amostras e alertas técnicos passaram a indicar um problema maior. Ainda assim, falhas de amostragem, interpretação, fiscalização e coordenação entre autoridades atrasaram a resposta.

O indicador podia parecer administrável enquanto a exposição real variava de residência para residência. A crise não mostrou apenas água inadequadamente tratada. Mostrou um sistema incapaz de representar com rapidez aquilo que chegava à torneira.

LIMITE: Mudanças de fonte exigem tratamento de corrosão, amostragem representativa e reação imediata a sinais de exposição.

QUEBRA: O processo avaliou conformidade por dados que não capturavam adequadamente a condição real da rede e das casas.

CONSEQUÊNCIA: A população permaneceu exposta ao chumbo enquanto instituições discutiam responsabilidade e interpretação.

Quando a falha atravessa o último limite

Uma barragem, um avião, um airbag, uma fábrica de sorvetes e uma rede pública de água não compartilham o mesmo mecanismo físico. Compartilham o instante em que o risco deixa de pertencer à organização e passa a ser entregue a quem confiava nela.

CASO	O PÚBLICO RECEBEU	O SISTEMA DEVERIA TER INTERROMPIDO
Brumadinho	Rejeitos e destruição	Permanência de pessoas sem segurança demonstrada
737 MAX	Aeronave com risco não plenamente comunicado	Liberação e continuidade da frota
Takata	Componente de proteção degradado	Circulação sem correção rastreável
Blue Bell	Alimento pronto contaminado	Liberação diante de sinais microbiológicos
Flint	Água que liberava chumbo da rede	Mudança sem controle de corrosão e medição real

O desvio deixa de ser interno quando atravessa o último limite da organização. A partir desse momento, trabalhador, cliente ou sociedade passam a experimentar aquilo que o sistema deveria ter contido.

A gravidade pública não começa no contato com a vítima. Começa quando uma organização perde a capacidade de impedir que sua incerteza, seu defeito ou sua contaminação saiam por seus portões.

O próximo passo será examinar um mecanismo ainda mais difícil de admitir: situações em que os sinais eram conhecidos, mas a organização escolheu uma explicação que permitia continuar.

Fontes dos casos deste interlúdio: ND-14, p. 142; ND-15, p. 143; ND-16, p. 143.

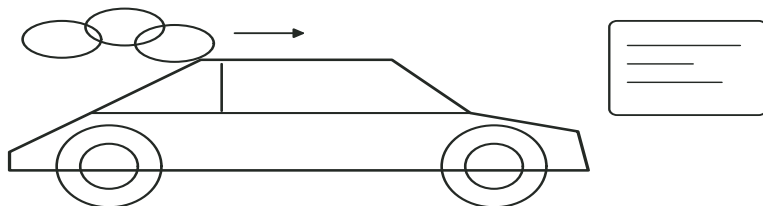
PARTE III

QUANDO O SISTEMA APRENDE A PARECER CORRETO

A aparência de controle pode sobreviver por muito tempo depois que o controle real desapareceu.



O carro que reconhecia o laboratório



18 de setembro de 2015. A notificação da Agência de Proteção Ambiental dos Estados Unidos não descrevia um defeito comum. Os veículos não estavam falhando por incapacidade de controlar emissões. Estavam reconhecendo quando precisavam parecer capazes.

O software identificava condições compatíveis com o teste oficial e acionava uma estratégia de controle mais rigorosa. Fora do laboratório, durante a condução normal, o comportamento mudava e as emissões de óxidos de nitrogênio aumentavam.

O carro não apenas violava o limite. Aprendia a demonstrar que o havia cumprido.

Dois carros dentro do mesmo carro

Todo veículo moderno depende de software. Sensores informam velocidade, posição do volante, pressão, temperatura e centenas de outras condições. O programa decide como motor, transmissão, freios e sistemas de emissões devem responder.

Essa capacidade não é um problema. Torna o veículo mais eficiente e seguro. A quebra ocorreu quando a inteligência destinada a controlar o produto passou a controlar a aparência do produto diante da fiscalização.

No ensaio, o carro se comportava de uma maneira. Na estrada, sob circunstâncias que o software reconhecia como uso comum, adotava outra calibração. O mesmo produto possuía uma versão para ser medido e outra para ser utilizado.

A conformidade existia no cenário em que seria verificada. O cliente, a cidade e o meio ambiente recebiam a condição que permanecia fora da sala de ensaio.

Quando o protocolo vira adversário

Um teste regulatório é uma barreira. Ele não foi criado para atrapalhar a engenharia, mas para representar uma exigência pública: o produto deve controlar emissões dentro de limites conhecidos.

Organizações saudáveis usam o resultado para corrigir o produto. Organizações em ruptura começam a tratar o resultado como obstáculo comercial. O objetivo deixa de ser cumprir o requisito e passa a ser obter o documento que afirma que ele foi cumprido.

Essa inversão é sutil porque os mesmos recursos continuam existindo. Há especificações, laboratórios, certificados, auditorias e assinaturas. A diferença está no objeto protegido. O sistema já não protege o cliente ou o ambiente. Protege a aprovação.

Em A Farsa, amostras que deveriam preservar a verdade deixaram de representá-la. No Dieselgate, o próprio produto aprendeu a oferecer ao ensaio uma realidade preparada.

A discrepância que insistia em existir

Testes em estrada realizados por pesquisadores encontraram emissões muito superiores às observadas no laboratório. A diferença poderia ter várias explicações: condição de uso, temperatura, desgaste, calibração ou falha de componentes.

Por meses, explicações técnicas e tentativas de correção ocuparam o espaço entre a evidência e a admissão. Atualizações e um recall não eliminaram a discrepância. Os reguladores passaram a exigir uma resposta capaz de explicar por que os veículos se comportavam de forma tão diferente fora do ciclo oficial.

A insistência da medição externa foi decisiva. O sistema interno tinha autoridade para produzir certificados. A verificação independente tinha liberdade para perguntar se o certificado representava o que acontecia na rua.

Sem essa possibilidade, a revisão apenas confirma a narrativa construída por quem precisa que o projeto avance.

A fraude que precisava de uma organização

Um código não se projeta, testa, integra, certifica, produz e vende sozinho. O escândalo não pode ser entendido como a ação abstrata de um computador. O software apenas executou uma decisão humana transformada em lógica.

Para chegar ao mercado, motores foram calibrados, documentos foram preparados, resultados foram apresentados, campanhas prometeram desempenho ambiental e veículos foram distribuídos durante anos. Cada etapa podia ter formulado uma pergunta simples: a condição aprovada representa o uso real?

Sistemas complexos também diluem a responsabilidade. Cada pessoa enxerga uma parte. Quem programa pode não assinar a certificação. Quem certifica pode não conhecer o código. Quem vende pode confiar no documento. Essa

fragmentação exige um protocolo superior capaz de reunir as partes e testar a verdade do conjunto.

O cliente comprou uma promessa

O comprador não adquiriu apenas um motor. Adquiriu a promessa de desempenho, economia e menor impacto ambiental. A certificação pública transformava essa promessa em confiança comercial.

Por isso, o dano não terminou no excesso de emissões. A fraude atingiu a relação entre informação e escolha. Consumidores pagaram por uma característica que acreditavam receber. Reguladores autorizaram produtos com base em resultados que não representavam o funcionamento normal.

Qualidade não é somente entregar o que pode ser medido no fim da linha. É garantir que aquilo que a organização declara sobre o produto permaneça verdadeiro quando ninguém está preparando o cenário para observá-lo.

Quando essa equivalência se rompe, a não conformidade técnica torna-se também uma quebra ética e comercial.

O custo que o teste havia escondido

Depois da admissão, vieram paralisações de vendas, recalls, recompras, acordos, processos e reformas de conformidade. Nos Estados Unidos, o esquema alcançou aproximadamente 590 mil veículos a diesel e produziu compromissos bilionários.

O valor financeiro foi extraordinário, mas não foi o primeiro custo. Antes dele, a organização havia gasto competência técnica para manter uma solução que não poderia ser defendida publicamente. Pessoas capazes de melhorar o produto foram mobilizadas para melhorar a aparência do teste.

Esse é um desperdício difícil de registrar. Quando a inteligência da empresa trabalha para contornar o limite, o sistema transforma talento em mecanismo de ocultação.

O benefício inicial foi preservar o produto, o cronograma e a promessa comercial. A consequência foi descobrir que a aprovação obtida não possuía valor quando a verdade se tornou pública.

O que quebrou primeiro?

A primeira quebra não foi a descoberta do software. Tampouco foi o momento em que um regulador publicou a notificação. A sequência começou quando o requisito ambiental perdeu autoridade sobre o projeto e passou a ser tratado como uma condição que precisava ser superada apenas durante o ensaio.

Depois vieram quebras adicionais: validação sem representar o uso real, certificação de uma condição preparada, comunicação comercial incompatível com o produto e demora em reconhecer aquilo que os dados externos já mostravam.

O Dieselgate acrescenta uma camada à tese deste livro. Às vezes, o protocolo não é ignorado nem executado de forma deficiente. Ele é estudado com precisão para que o sistema aprenda a aparentar conformidade.

Nesse momento, auditoria, ensaio e certificado deixam de ser barreiras e tornam-se cenografia.

O PONTO DE RUPTURA

PROTOCOLO

Veículos devem cumprir os limites de emissões durante o uso representativo, e a certificação deve refletir o comportamento real do produto.

PRIMEIRA QUEBRA

O requisito passou a ser tratado como uma condição de teste. O software reconhecia o laboratório e alterava o controle de emissões para obter aprovação.

CONSEQUÊNCIA

Veículos foram vendidos com emissões reais muito superiores às demonstradas, clientes e reguladores receberam informação falsa e a confiança na marca foi atingida.

SE FOSSE CUMPRIDO

A discrepância entre laboratório e estrada teria bloqueado a liberação. O projeto precisaria ser corrigido, reposicionado ou retirado antes da comercialização.

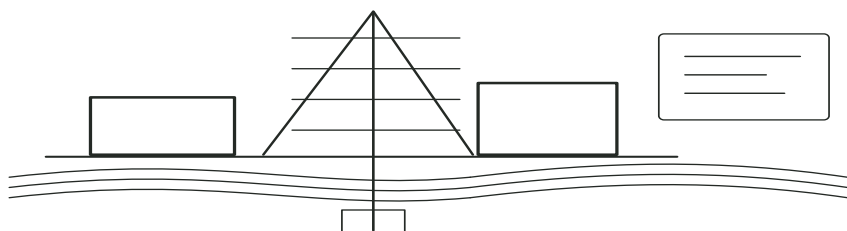
VEREDITO

O produto não falhou em compreender o teste. A organização falhou porque ensinou o produto a vencê-lo.

Nota documental: Comunicações oficiais da EPA (2015) e do DOJ (2017). O recorte de aproximadamente 590 mil veículos refere-se aos Estados Unidos. Ver ND-17, p. 144.

No Dieselgate, a conformidade deixou de ser uma condição do produto e tornou-se uma apresentação preparada para o fiscal.

O teste aprovado pelo desejo de terminar



20 de abril de 2010. A Deepwater Horizon estava concluindo o poço Macondo, no Golfo do México. O trabalho principal de perfuração havia terminado. Restava preparar o poço para uma suspensão temporária e liberar a plataforma para o próximo serviço.

Antes de retirar parte da pressão exercida pelo fluido pesado, a equipe precisava demonstrar que as barreiras do poço suportariam a formação. O teste deveria responder a uma pergunta binária: o poço está isolado ou existe comunicação com o reservatório?

O teste não precisava mostrar que o trabalho podia continuar. Precisava ter poder para impedir que continuasse.

A barreira que ninguém podia ver

Milhares de metros abaixo da plataforma, o cimento deveria vedar o espaço entre revestimentos e formação. A barreira não era observável diretamente. Sua existência precisava ser inferida por projeto, execução e testes.

Essa característica torna a disciplina ainda mais importante. Quando uma proteção está escondida, o sistema depende da qualidade da evidência que demonstra sua integridade. Não basta acreditar que o cimento foi colocado. É necessário confirmar que isolou os fluidos sob as condições reais do poço.

O plano de abandono temporário também modificava o equilíbrio. Lama pesada seria substituída por água do mar em parte do sistema. Ao reduzir a pressão hidrostática, a operação passaria a depender mais das barreiras mecânicas e do cimento.

O risco não surgiu porque a pressão foi reduzida. Surgiu quando a redução avançou sem uma demonstração inequívoca de que o poço permanecia isolado.

O teste que produziu duas respostas

Durante o teste de pressão negativa, as leituras não formaram uma história coerente. Uma linha indicava ausência de fluxo. Outra apresentava pressão elevada que retornava depois de ser aliviada.

Resultados conflitantes não são um detalhe inconveniente. São o próprio resultado do teste. Quando dois indicadores que deveriam descrever a mesma condição discordam, a única conclusão segura é que o sistema ainda não compreendeu o que está medindo.

Naquela noite, a pressão foi explicada como um efeito conhecido como bladder effect. A interpretação permitiu classificar o teste como satisfatório e prosseguir com o deslocamento da lama.

A primeira resposta estava nos instrumentos. A segunda nasceu da necessidade de fazer os instrumentos caberem no plano.

Quando continuar organiza a interpretação

Nenhuma decisão operacional acontece fora do contexto. O poço estava atrasado, a plataforma tinha compromissos seguintes e cada hora possuía custo. Isso não prova que alguém tenha escolhido conscientemente um acidente. Mostra por que critérios objetivos de parada são indispensáveis.

Sem um limite inequívoco, pessoas competentes podem interpretar a ambiguidade na direção que preserva a tarefa. A pressão não precisa aparecer como ordem. Pode surgir como familiaridade com o plano, desejo de concluir, confiança na experiência e resistência em reabrir uma etapa que parecia encerrada.

Relatórios oficiais descreveram uma sequência de decisões de diferentes empresas, falhas de comunicação e uma cultura de gerenciamento de risco incapaz de tratar o poço como um sistema integrado.

As últimas barreiras receberam o problema tarde demais

Depois que a lama foi deslocada, hidrocarbonetos entraram no poço e subiram em direção à plataforma. Sinais de fluxo e variações nos volumes não produziram reação a tempo de recuperar o controle.

Quando o influxo alcançou a superfície, a equipe tentou desviar a mistura para equipamentos que não foram capazes de conter a vazão. Gás espalhou-se pela plataforma, encontrou fontes de ignição e explodiu.

O preventor de explosão, última barreira mecânica no fundo do mar, não conseguiu selar o poço. Onze trabalhadores morreram. A plataforma afundou, e o vazamento continuou por meses, produzindo um desastre ambiental de enorme escala.

A explosão recebeu as imagens. A quebra decisiva permaneceu no teste que deveria ter interrompido o abandono temporário.

O PONTO DE RUPTURA

PROTOCOLO

Antes de reduzir a pressão hidrostática, o teste de pressão negativa deveria demonstrar de forma coerente que as barreiras do poço estavam íntegras.

PRIMEIRA QUEBRA

Leituras conflitantes foram interpretadas como teste satisfatório, permitindo que a operação prosseguisse sem prova inequívoca de isolamento.

CONSEQUÊNCIA

Hidrocarbonetos entraram no poço, alcançaram a plataforma, incendiaram-se e superaram as defesas finais. Onze trabalhadores morreram e ocorreu um grande derramamento.

SE FOSSE CUMPRIDO

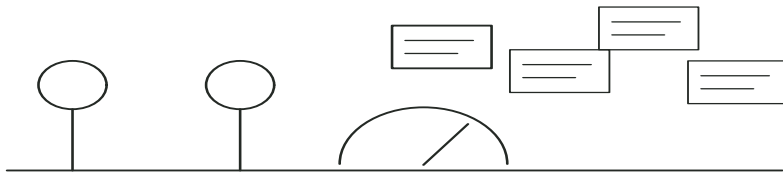
A discrepância bloquearia o deslocamento da lama. O poço seria estabilizado, o teste repetido e a integridade das barreiras investigada antes de prosseguir.

VEREDITO

O reservatório forneceu a pressão. A quebra transformou um teste ambíguo em autorização para retirar a margem que ainda protegia o sistema.

Nota documental: Comissão presidencial (2011), CSB (2014) e BP (2010). O relatório da BP é identificado como investigação empresarial. Ver ND-18, p. 144.

Quando a aparência substitui o controle



Quando a meta aprendeu a criar o cliente

Wells Fargo, 2002 a 2016

O discurso dizia vender de acordo com a necessidade. A rotina premiava volume. Metas agressivas, acompanhamento constante e incentivos transformaram produtos financeiros em números que precisavam existir, mesmo quando o cliente não os havia pedido.

Funcionários abriram contas e solicitaram cartões sem autorização, criaram registros e movimentaram recursos para fazer produtos parecerem utilizados. A meta não descrevia o serviço prestado. Passou a fabricar a evidência de que o serviço havia sido prestado.

Milhares de empregados foram responsabilizados ao longo dos anos, mas autoridades concluíram que a prática era sistêmica, ligada ao modelo de vendas, aos incentivos e a falhas de supervisão e auditoria.

LIMITE: Metas comerciais devem permanecer subordinadas ao consentimento, à necessidade do cliente e à integridade dos registros.

QUEBRA: O sistema recompensou volume e tratou sinais de fraude como problemas individuais, sem corrigir a arquitetura que os produzia.

CONSEQUÊNCIA: Milhões de contas e produtos foram abertos sob falsas premissas ou sem autorização, destruindo confiança e gerando sanções bilionárias.

O prédio que mostrou a rachadura

Rana Plaza, Bangladesh, 2013

No dia anterior ao colapso, rachaduras apareceram no edifício que abrigava fábricas de roupas. Bancos e lojas suspenderam atividades. Trabalhadores temeram entrar. A estrutura havia produzido um sinal visível, compreensível e impossível de reduzir a um número abstrato.

Na manhã seguinte, milhares de pessoas voltaram ao prédio. A produção foi retomada. Pouco depois, a estrutura desabou. Mais de 1.100 trabalhadores morreram e mais de 2.500 ficaram feridos.

O caso não exige uma teoria sofisticada sobre detecção. O risco foi visto. A quebra ocorreu quando a autoridade econômica de continuar foi maior do que a autoridade técnica de interditar.

LIMITE: Rachaduras relevantes exigem evacuação, inspeção independente e proibição de ocupação até demonstração de segurança.

QUEBRA: O sinal foi reconhecido, mas trabalhadores retornaram e a produção recebeu prioridade sobre a incerteza estrutural.

CONSEQUÊNCIA: O edifício colapsou com milhares de pessoas no interior, tornando-se um símbolo mundial da fragilidade nas cadeias de fornecimento.

O açúcar que se acumulava à vista de todos

Imperial Sugar, 2008

Açúcar parece inofensivo sobre uma mesa. Disperso em partículas finas, acumulado em superfícies e suspenso no ar, pode alimentar explosões violentas. A fábrica conhecia poeira, vazamentos e depósitos como parte da rotina.

Uma esteira havia sido enclausurada para conter derramamentos. O fechamento, porém, também criou um volume onde a poeira podia se concentrar. A investigação concluiu que uma ignição provável dentro desse espaço iniciou a explosão primária. A onda levantou depósitos espalhados pelo prédio e alimentou explosões secundárias muito maiores.

Quatorze trabalhadores morreram e dezenas ficaram feridos. O combustível não estava escondido. Estava sobre equipamentos, pisos e estruturas, normalizado pela convivência diária.

LIMITE: Projeto, ventilação, coleta e limpeza devem impedir acúmulos perigosos de poeira combustível.

QUEBRA: Equipamentos inadequados e housekeeping insuficiente permitiram que o combustível se acumulasse, enquanto o enclausuramento criou uma nova condição de confinamento.

CONSEQUÊNCIA: Uma ignição localizada propagou explosões secundárias por grandes áreas da refinaria.

Quando o indicador começa a mentir

Os cinco casos desta parte parecem pertencer a mundos incompatíveis. Um motor, um poço marítimo, um banco, um edifício e uma refinaria de açúcar. Em todos, porém, a organização recebeu uma evidência que ameaçava a continuidade e encontrou uma forma de preservar a aparência necessária para seguir.

CASO	A REALIDADE	A APARÊNCIA ACEITA
Dieselgate	Emissões elevadas na condução real	Aprovação obtida no ciclo de teste
Macondo	Teste com leituras incompatíveis	Interpretação de barreira íntegra
Wells Fargo	Produtos sem necessidade ou consentimento	Meta comercial registrada como venda
Rana Plaza	Rachaduras e incerteza estrutural	Retorno tratado como condição aceitável
Imperial Sugar	Poeira combustível acumulada	Acúmulo tratado como parte da rotina

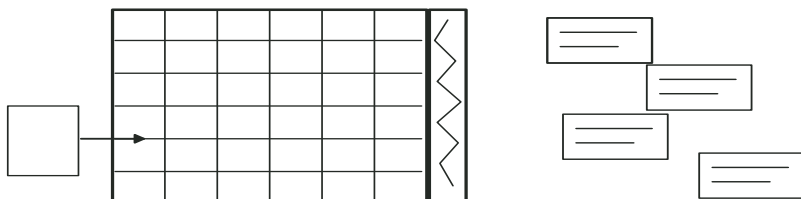
O sistema começa a quebrar quando a evidência deixa de servir para interromper a decisão e passa a ser administrada para permitir que ela continue.

Nem toda aparência falsa nasce de fraude deliberada. Algumas surgem de interpretação conveniente, metas mal desenhadas ou normalização. O efeito é o mesmo: o indicador permanece verde enquanto a realidade já saiu do controle.

A próxima parte deverá olhar para organizações que receberam oportunidades explícitas de aprender após o primeiro evento e, ainda assim, permitiram que o mesmo mecanismo voltasse a alcançar pessoas, clientes e comunidades.

Fontes dos casos deste interlúdio: ND-19, p. 145; ND-20, p. 145; ND-21, p. 146.

A torre que já havia sido avisada



14 de junho de 2017. A primeira ligação chegou pouco antes da uma da manhã. O fogo havia começado numa cozinha da Grenfell Tower, em Londres. A lógica de segurança dizia que um incêndio doméstico deveria permanecer no apartamento de origem.

Poucos minutos depois, as chamas alcançaram a fachada. O edifício passou a conduzir o fogo por fora da compartimentação que deveria proteger quem permanecia dentro.

O refrigerador iniciou o incêndio. A reforma decidiu até onde ele poderia chegar.

O incêndio que deveria permanecer comum

Edifícios altos não dependem de uma única defesa. Portas resistentes, paredes, lajes, selagens e rotas de fuga trabalham juntas para que um foco localizado não se transforme em ameaça para toda a torre.

Essa arquitetura sustenta a estratégia de permanecer no apartamento quando o incêndio está em outra unidade. A orientação não é uma regra abstrata. Depende de uma premissa física: cada residência precisa continuar oferecendo proteção enquanto os bombeiros controlam o foco.

Em Grenfell, a premissa deixou de existir. O fogo saiu pela janela, encontrou o sistema externo e subiu rapidamente. Depois retornou a outros apartamentos, ocupou áreas comuns e tornou a única escada progressivamente mais difícil de usar.

O problema não estava apenas no comportamento da madrugada. Estava no fato de o edifício reformado ainda ser administrado como se fosse o edifício anterior.

A reforma que mudou a natureza do risco

A torre recebeu uma nova fachada durante a reforma concluída no ano anterior ao incêndio. Revestimento, isolamento, cavidades, janelas e barreiras formavam um sistema único, embora contratos, fornecedores e documentos tratassem cada elemento em pedaços.

Uma mudança estética e térmica também é uma mudança de segurança. Ao cobrir a parede externa, a obra alterou caminhos de calor, ventilação, fumaça e propagação. Isso exigia demonstrar que o conjunto preservava a compartimentação e não criava uma rota vertical para o fogo.

A investigação final concluiu que o desastre resultou de falhas acumuladas ao longo de muitos anos, envolvendo produtos, testes, certificação, projeto, fiscalização, gestão do edifício e resposta pública. Não existiu uma decisão isolada capaz de explicar tudo.

A primeira quebra editorialmente relevante ocorreu quando a segurança do conjunto foi presumida a partir de componentes, certificados e responsabilidades fragmentadas.

Componentes aprovados, sistema não demonstrado

Conformidade por componentes oferece conforto. Cada material possui ficha, classificação ou ensaio. Cada fornecedor responde por uma parte. O conjunto parece protegido pela soma dos documentos.

Incêndios, porém, não leem certificados separados. Encontram a configuração real: juntas, espaços vazios, fixações, membranas, barreiras de cavidade, janelas e materiais que interagem sob calor crescente.

O relatório da investigação apontou falhas graves no regime de testes e na orientação regulatória. Métodos disponíveis não forneciam aos projetistas a informação necessária para avaliar adequadamente a propagação em paredes externas, e classificações usadas durante anos eram inadequadas para aquele propósito.

O protocolo correto não era colecionar documentos. Era provar, em configuração representativa, que a fachada real manteria o fogo onde a estratégia do edifício esperava encontrá-lo.

A cavidade que virou caminho

Fachadas ventiladas possuem espaços que cumprem funções úteis. Permitem drenagem, equalização e desempenho térmico. Também podem criar fluxo vertical se barreiras internas não interromperem o caminho.

Uma barreira de cavidade não precisa impedir todo aquecimento. Precisa dividir o percurso, limitar a circulação de chamas e fumaça e preservar a separação entre pavimentos. Sua eficácia depende de posição, instalação e continuidade.

Em Grenfell, a fachada ofereceu uma rota exterior que contornou as defesas internas. A velocidade da propagação não foi produzida por um único material,

mas por um sistema no qual combustibilidade, geometria e falhas de compartimentação passaram a trabalhar na mesma direção.

Quando a consequência percorre uma rota inesperada, a investigação deve perguntar qual mudança abriu o caminho e por que nenhum teste obrigou o sistema a demonstrar que conseguiria fechá-lo.

A estratégia que dependia de um prédio que já não existia

A orientação de permanecer nos apartamentos funcionava enquanto a compartimentação permanecesse confiável. Quando o fogo e a fumaça alcançaram vários pavimentos, essa estratégia precisava ser revista com velocidade.

A investigação da primeira fase analisou a resposta na noite do incêndio e a demora em abandonar a orientação geral. Mas culpar apenas a mensagem final seria outra forma de começar tarde. O comando recebeu uma situação que o edifício não deveria ter produzido.

Uma estratégia de emergência precisa possuir gatilhos de mudança. Se a premissa falha, a orientação deve mudar. Para isso, quem decide precisa receber informação confiável, reconhecer o novo cenário e possuir meios de comunicação e evacuação compatíveis.

A ruptura da fachada retirou tempo. As falhas posteriores consumiram parte do tempo restante. Camadas diferentes, responsabilidades diferentes, uma mesma sequência.

Os moradores que não conseguiam transformar preocupação em decisão

Antes do incêndio, moradores haviam manifestado preocupações sobre segurança e gestão. Reclamações não são sempre prova técnica de perigo, mas são sensores distribuídos por toda a operação. Revelam portas, elevadores, rotas, alarmes e comportamentos que relatórios periódicos podem não enxergar.

O sistema precisa separar ruído de sinal sem transformar o mensageiro em problema. Quando a organização aprende a defender-se das reclamações, perde uma fonte barata de conhecimento sobre a realidade cotidiana.

Em edifícios residenciais, essa assimetria é profunda. O morador vive o risco, mas não controla especificações, contratos, inspeções ou decisões de investimento. Sua proteção depende de instituições que não podem exigir dele a linguagem necessária para ser levado a sério.

A quebra também ocorre quando o canal existe, recebe a preocupação e não consegue convertê-la em investigação, resposta e correção.

Responsabilidade dividida, risco inteiro

O relatório final distribuiu críticas por uma rede extensa: fabricantes, empresas de teste e certificação, projetistas, contratadas, autoridades locais, governo central, gestão do edifício e serviços de resposta. Essa amplitude não dilui a responsabilidade. Mostra como o perigo atravessou fronteiras organizacionais.

Cada participante controlava uma parte. Nenhum podia controlar sozinho o incêndio. Justamente por isso, o protocolo precisava conectar as partes e exigir uma prova comum: a torre reformada continuava segura como sistema?

Fragmentação transforma dúvidas em espaços vazios. O fornecedor presume que o projetista avaliará o uso. O projetista presume que o certificado cobre o produto. A fiscalização presume que os documentos representam a instalação. O gestor presume que a estratégia antiga continua válida.

A ausência dessa função permite que cada decisão pareça defensável isoladamente e o resultado coletivo se torne indefensável.

O PONTO DE RUPTURA

PROTOCOLO

Toda reforma de fachada deve ser avaliada como sistema completo, com materiais, cavidades, janelas, barreiras e estratégia de emergência demonstrando segurança na configuração real.

PRIMEIRA QUEBRA

A alteração foi aceita por uma cadeia fragmentada de aprovações sem prova confiável de que o edifício reformado preservava a compartimentação e impediria propagação rápida entre pavimentos.

CONSEQUÊNCIA

O fogo alcançou a fachada, espalhou-se pela torre e contribuiu para 72 mortes, enquanto a estratégia de permanência perdeu a premissa física que a sustentava.

SE FOSSE CUMPRIDO

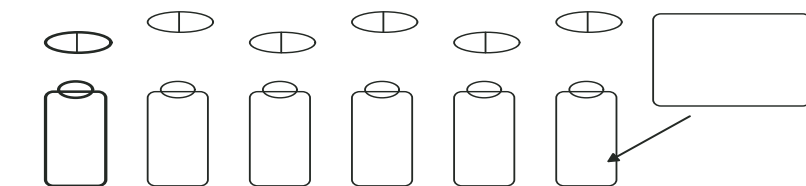
O sistema externo seria rejeitado ou redesenhado. Mesmo diante do incêndio inicial, a propagação vertical seria limitada e a resposta teria mais tempo e condições.

VEREDITO

O refrigerador iniciou o incêndio. A primeira quebra ocorreu quando uma reforma que alterava o risco foi tratada como componentes conformes, sem que o edifício real precisasse provar que continuava seguro. Grenfell mostra uma mudança que avançou antes da prova. O caso seguinte mostra algo ainda mais direto: a prova existia, mas o lote avançou apesar dela.

Nota documental: Grenfell Tower Inquiry, Fases 1 (2019) e 2 (2024). Conclusões do inquérito público são distintas de condenações criminais. Ver ND-22, p. 146.

O resultado que não podia atrasar o lote



Estados Unidos, 2008 e 2009. O problema não começou quando pessoas adoeceram. Começou quando a fábrica recebeu resultados que deveriam bloquear produto e passou a tratá-los como obstáculos de expedição.

A Peanut Corporation of America fabricava ingredientes usados por muitas outras empresas. Um único lote podia desaparecer dentro de biscoitos, barras, doces e produtos distribuídos por cadeias extensas.

Na indústria de alimentos, liberar antes da prova transforma o consumidor na última etapa do controle.

O lote que esperava o caminhão, não o resultado

Análise microbiológica exige tempo. A amostra entra no laboratório, o ensaio segue etapas e o lote precisa permanecer retido até que o resultado permita a liberação. A espera não é atraso inútil. É a barreira que separa o risco invisível do mercado.

Documentos do processo criminal mostraram situações em que produtos foram enviados antes da conclusão dos testes. Em outras, resultados positivos para *Salmonella* foram seguidos por novos ensaios até surgir um resultado negativo que permitisse tratar o material como aceitável.

Retestar pode ser tecnicamente legítimo quando existe investigação de método, amostragem ou erro comprovado. Torna-se quebra quando sua função é substituir uma evidência incômoda por outra mais conveniente, sem eliminar a causa.

O protocolo não era obter um papel negativo. Era demonstrar que o produto e o processo estavam sob controle.

Retestar até o problema desaparecer

Microrganismos não se distribuem de forma perfeitamente uniforme. Uma amostra pode capturar contaminação e outra, retirada do mesmo lote, não. Por isso, um resultado positivo não é equilibrado por um resultado negativo como se fossem votos opostos.

A pergunta correta é causal: de onde veio a contaminação, quais lotes podem estar envolvidos, o ambiente permanece afetado e que evidência demonstra que a fonte foi eliminada? Sem essa investigação, o novo resultado apenas mede outro ponto de um sistema ainda desconhecido.

Quando a organização premia expedição e pune retenção, o laboratório deixa de ser proteção e passa a ser negociador. A análise continua existindo, mas sua autoridade depende de coincidir com a necessidade comercial.

A primeira quebra não foi microbiológica. Foi gerencial: permitir que a pressão por entrega decidisse qual evidência merecia representar a realidade.

O certificado que não representava o produto

Clientes industriais raramente acompanham cada lote dentro da fábrica do fornecedor. Recebem especificações, certificados de análise e garantias de que o sistema de segurança funcionou. A cadeia depende da integridade dessa representação.

No caso PCA, a Justiça dos Estados Unidos concluiu que resultados foram falsificados e que produtos contaminados foram enviados. Certificados e comunicações deixaram de descrever o estado do material e passaram a proteger a venda.

Isso multiplica o alcance da quebra. O cliente usa o ingrediente acreditando que a barreira já foi cumprida. Pode incorporá-lo a outro produto, distribuí-lo nacionalmente e descobrir o problema apenas quando a epidemiologia conecta pessoas distantes à mesma origem.

Quando o dado perde integridade, controles posteriores trabalham com uma realidade fabricada e podem concluir, com rigor, algo que nunca foi verdadeiro.

O consumidor como laboratório

O surto foi associado a mais de setecentas infecções notificadas e nove mortes. A extensão real pode ter sido maior, porque nem toda doença é diagnosticada, comunicada ou conectada à fonte.

Para encontrar o problema, autoridades precisaram combinar entrevistas, padrões de doença, rastreabilidade, inspeções e resultados laboratoriais. O sistema aprendeu depois que o produto havia sido ingerido.

Esse é o fracasso mais profundo de um programa de segurança de alimentos: o consumidor torna-se a etapa de detecção que a fábrica deveria ter mantido dentro de seus muros. A reclamação, o hospital e a vigilância epidemiológica passam a fazer o trabalho que retenção, higiene e investigação não fizeram.

O recall retira produto. Não devolve a condição anterior. Depois da distribuição, a organização controla apenas parte da velocidade e da eficácia da reação.

A fraude que precisou de uma cadeia

Fraude operacional raramente permanece numa única mentira. Para liberar um lote adverso, é preciso neutralizar retenção. Para explicar a liberação, é preciso alterar registro. Para preservar o cliente, é preciso emitir documento. Para enfrentar a investigação, é preciso sustentar a narrativa anterior.

Cada nova etapa cria testemunhas, mensagens, decisões e inconsistências. A organização passa a gastar energia protegendo a primeira quebra, enquanto o problema físico continua disponível para repetir-se.

A condenação criminal dos dirigentes da PCA foi incomum pela severidade e pelo reconhecimento de que segurança de alimentos também depende de integridade deliberada. Não era apenas uma falha de limpeza ou laboratório. Era a transformação consciente do sistema de controle em instrumento de venda.

O caso mostra por que Qualidade, laboratório e cadeia de custódia precisam de independência suficiente para bloquear produto mesmo quando a decisão ameaça receita e prazo.

O PONTO DE RUPTURA

PROTOCOLO

Reter lotes até resultado satisfatório, investigar qualquer detecção de patógeno, preservar registros e emitir certificados que representem fielmente produto e processo.

PRIMEIRA QUEBRA

Produtos foram enviados antes da conclusão de testes ou após resultados adversos neutralizados por retestes e registros que não demonstravam eliminação da causa.

CONSEQUÊNCIA

Ingredientes contaminados alcançaram uma cadeia ampla, contribuindo para mais de setecentas infecções notificadas e nove mortes, além de recall e colapso empresarial.

SE FOSSE CUMPRIDO

Os lotes permaneceriam bloqueados, a fonte seria investigada e clientes receberiam informação verdadeira para impedir distribuição e transformação do ingrediente.

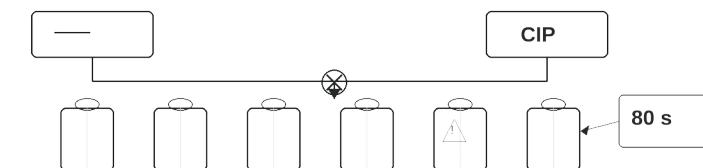
VEREDITO

A Salmonella criou o perigo. A primeira quebra ocorreu quando o resultado laboratorial perdeu autoridade para interromper a expedição.

Nota documental: Comunicados oficiais do DOJ sobre o veredito de 2014 e as sentenças de 2015. As condutas e condenações variam entre os envolvidos. Ver ND-23, p. 147.

Na PCA, o teste foi vencido pela expedição. No caso seguinte, a linha permitiria que limpar e envasar ocupassem a mesma sequência.

Os oitenta segundos que a fábrica não conteve



25 de fevereiro de 2013. Em uma das linhas de produção da Unilever em Pouso Alegre, Minas Gerais, o lote AGB25 de AdeS sabor maçã, em embalagens de 1,5 litro, estava terminando. O tanque que alimentava o envase já tinha pouco produto, condição que antecedia o ciclo automático de limpeza. Era exatamente o momento em que duas operações deveriam permanecer separadas: produzir e higienizar.

Durante o ciclo de limpeza CIP, a linha foi acionada novamente para envase. A solução que circulava pelo equipamento continha hidróxido de sódio a 2,5%. Como ainda havia embalagens disponíveis, 96 unidades receberam a solução de limpeza no lugar da bebida. A inspeção sanitária registrou ainda um fato mais importante que o número: o desvio não foi constatado antes da liberação e o produto chegou ao mercado.

O produto de limpeza não chegou ao consumidor porque o CIP existia. Chegou porque uma condição que deveria impedir o envase continuou operacional.

Quando limpeza e produção dividiram a mesma linha

CIP é uma barreira de higiene. Usa agentes químicos justamente porque precisa remover resíduos e devolver o equipamento a uma condição sanitária conhecida. Por isso, o mesmo sistema que protege o alimento durante a limpeza precisa impedir que a limpeza seja confundida com produção.

A Unilever atribuiu o episódio a uma combinação de falha humana e mecânica. Em entrevista posterior, o presidente da empresa afirmou que o equipamento não deveria ter aceitado o comando de envase naquela condição. Essa declaração desloca a pergunta para um ponto anterior ao gesto do operador: por que uma ação humana inadequada ainda tinha caminho físico para colocar solução de limpeza dentro da embalagem?

Um processo robusto não depende de uma única pessoa reconhecer, em poucos segundos, qual fluido ocupa a tubulação. Ele transforma estados incompatíveis em comandos incompatíveis. Se a linha está em limpeza, produzir deveria ser tecnicamente impossível ou, no mínimo, exigir uma liberação independente que prove a condição segura.

Noventa e seis embalagens, nenhuma barreira final

A sequência durou cerca de oitenta segundos, segundo a própria empresa. Curta demais para parecer um evento de processo. Longa o bastante para criar 96 embalagens capazes de causar queimaduras. O tamanho da janela ajuda a entender por que o caso é relevante: falhas transitórias são justamente aquelas que um plano de controle por amostragem pode não enxergar.

Na audiência pública da Câmara, um executivo da Unilever explicou que as amostras mantidas na fábrica não haviam capturado as unidades produzidas naquele intervalo. O produto amostrado estava normal e a produção foi liberada. A amostragem não criou a contaminação, mas também não funcionou como barreira de escape.

A resposta da Vigilância Sanitária mineira revela, pela própria natureza das correções exigidas, quais defesas precisavam ser fortalecidas. A linha só poderia voltar após revisão de equipamentos, sensores e software, aumento das amostras de envase, alteração do período de retenção do produto acabado, revisão do procedimento de liberação após o CIP e criação de um dossiê diário de qualidade com liberação formal assinada pela gestão.

Quando a correção exige intertravamento, amostragem, retenção e assinatura de liberação, o problema já não cabe na expressão “erro do operador”.

A fábrica soube depois do consumidor

O produto havia sido fabricado em 25 de fevereiro. Segundo relato público do presidente da Unilever, o SAC recebeu em 7 de março uma mensagem de consumidor descrevendo ardência na boca. A empresa levou alguns dias para obter a amostra e confirmar a alteração. O recall do lote foi anunciado em 14 de março.

Esse intervalo não transforma automaticamente a reação da empresa em omissão. Uma reclamação isolada precisa ser verificada. O ponto sistêmico é outro: a primeira evidência eficaz do desvio veio de fora da fábrica. O consumidor passou a cumprir a função que intertravamento, inspeção, amostragem, retenção e liberação deveriam ter cumprido antes da expedição.

Até 15 de março, ao menos 14 pessoas haviam relatado reações ao serviço de atendimento, segundo informações divulgadas à época. A Anvisa advertiu que o consumo poderia causar queimaduras e recomendou que o produto não fosse ingerido. Dias depois, a empresa ainda procurava parte das 96 unidades distribuídas em São Paulo, Rio de Janeiro e Paraná.

Depois que o produto sai, o controle muda de natureza. A fábrica deixa de bloquear e passa a procurar. Cada unidade não localizada representa uma barreira que já não está sob comando da operação.

A suspensão que ampliou o raio

Em 18 de março, a Anvisa suspendeu, por precaução, a fabricação, a distribuição, a comercialização e o consumo de todos os alimentos com soja produzidos na linha TBA3G, abrangendo todos os sabores. A medida não significava que toda a linha estivesse contaminada. Significava que, naquele momento, a extensão real da falha ainda precisava ser demonstrada.

A inspeção realizada entre 18 e 22 de março permitiu reduzir a incerteza. Em 8 de abril, a Anvisa informou que a falha operacional havia atingido apenas o AdeS maçã de 1,5 litro do lote AGB25 e liberou os demais produtos da linha, mantendo a proibição sobre o lote afetado. O episódio, portanto, foi pontual na extensão física. Isso não o torna pequeno na arquitetura de controle.

Três camadas da mesma ocorrência

A origem física é clara: solução de hidróxido de sódio a 2,5% circulava durante a limpeza e foi envasada quando a linha voltou à função de produção. O escape organizacional veio depois: a condição não foi bloqueada pelo equipamento, não foi segregada de forma eficaz e não foi capturada pelos controles que antecederiam a liberação. A escalada sistêmica apareceu quando o consumidor se tornou a fonte da evidência que obrigou a organização a reconstruir o que havia ocorrido.

Essa separação evita duas simplificações. A primeira seria chamar o caso apenas de “contaminação por soda cáustica”, como se o produto químico explicasse por que chegou ao mercado. A segunda seria encerrá-lo em “falha humana”, como se a função de um sistema industrial fosse apenas registrar o erro depois que alguém aperta o botão errado.

Na lógica de A Quebra, a investigação procura o primeiro limite que perdeu autoridade. Aqui, a leitura mais consistente com os fatos públicos é que a função de envase permaneceu disponível quando a linha ainda estava em uma condição de higienização. Depois disso, outras barreiras também falharam: percepção do desvio, segregação, amostragem, retenção e liberação.

A primeira quebra não foi a queimadura relatada pelo consumidor. Foi permitir que limpar e envasar pudessem ocupar a mesma sequência sem uma barreira capaz de tornar a combinação impossível.

O erro do operador não encerra a investigação

A inspeção sanitária confirmou a falha de processo, mas as fontes públicas não oferecem base para atribuir, sozinhas, toda a responsabilidade causal a uma pessoa. A própria empresa descreveu uma combinação de fatores mecânicos e humanos. Isso importa porque acidentes de processo raramente precisam de menos controle depois que um operador erra. Precisam de mais.

A correção tecnicamente madura não é pedir apenas que o próximo operador preste mais atenção. É reduzir a quantidade de atenção necessária para impedir o evento. Intertravamentos, liberação pós-CIP, retenção e critérios formais de qualidade existem para que um lapso não atravessasse todas as camadas até o consumidor. Oitenta segundos bastaram para produzir o desvio; foram necessários dias, inspeções, recall e novas regras para reconstruir a barreira.

O PONTO DE RUPTURA

PROTOCOLO

Produção e CIP devem ser estados mutuamente exclusivos. O envase precisa permanecer bloqueado enquanto houver solução de limpeza no circuito e só pode ser retomado após verificação formal da condição da linha. O produto acabado deve permanecer retido até que os critérios de liberação demonstrem segurança.

PRIMEIRA QUEBRA

Durante a limpeza, a linha pôde ser reativada para envase enquanto a solução de hidróxido de sódio ainda ocupava o sistema. Nenhum bloqueio automático ou liberação independente impediu que 96 embalagens fossem produzidas nessa condição.

CONSEQUÊNCIA

Unidades do lote AGB25 chegaram ao mercado com solução de limpeza, houve relatos de reações e risco de queimaduras, foi realizado recall e a Anvisa suspendeu preventivamente todos os produtos fabricados na linha TBA3G até delimitar a extensão da falha.

SE FOSSE CUMPRIDO

O comando de envase permaneceria inibido até o fim comprovado do CIP e a liberação da linha. Mesmo se o acionamento indevido ocorresse, as unidades produzidas na janela seriam segregadas ou permaneceriam retidas antes de alcançar o mercado.

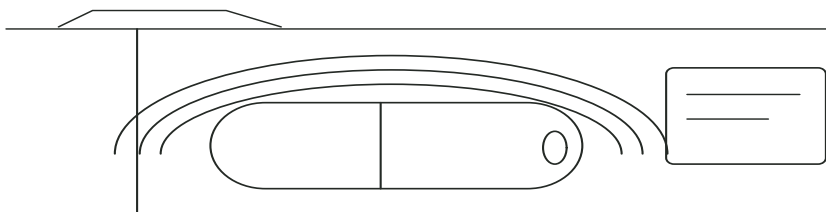
VEREDITO

A soda cáustica criou o perigo. A primeira quebra ocorreu quando duas condições que deveriam ser incompatíveis — limpar e envasar — puderam coexistir sem uma barreira capaz de impedir ou reter o resultado.

***Nota documental:** a inspeção sanitária confirmou o lote AGB25, a linha TBA3G, o envase de 96 unidades com solução de hidróxido de sódio a 2,5% e a falha em detectar o desvio antes do mercado. A duração aproximada de 80 segundos e a combinação entre falha humana e mecânica são declarações públicas da Unilever reproduzidas pela imprensa. A análise de “primeira quebra” é interpretação organizacional. Ver ND-32, p. 151.*

No AdeS, a barreira deveria ter tornado dois estados incompatíveis. No caso seguinte, a própria exigência de provar segurança seria tratada como obstáculo à inovação.

A inovação que dispensou a prova



18 de junho de 2023. O Titan iniciou a descida rumo aos destroços do Titanic levando cinco pessoas. A comunicação desapareceu durante o mergulho. O submersível havia sido perdido no Atlântico Norte.

Durante dois anos, a investigação da Guarda Costeira dos Estados Unidos examinou projeto, manutenção, inspeção, cultura, regulação e alertas anteriores. Em 2025, concluiu que a perda era evitável.

A profundidade não criou a fragilidade. Apenas aplicou a carga que o projeto prometia suportar.

A pressão que não negocia

A quase quatro mil metros, a água exerce uma pressão externa extrema. O casco precisa suportar repetidos ciclos de compressão sem perder geometria, aderência ou resistência. Não existe espaço para uma margem baseada em esperança.

Submersíveis tripulados tradicionais usam materiais, geometrias e processos com histórico amplo, além de classificação, ensaios e inspeções independentes. Inovar é possível, mas cada afastamento do conhecimento consolidado aumenta a obrigação de produzir prova equivalente ou superior.

O Titan combinava uma seção cilíndrica de compósito de fibra de carbono com extremidades metálicas. A proposta buscava reduzir peso e ampliar capacidade. A mesma escolha introduzia questões difíceis sobre fabricação, união entre materiais e comportamento após ciclos repetidos.

A engenharia não proíbe a novidade. Proíbe tratar desconhecimento como margem.

Um casco fora da tradição

Materiais compósitos podem oferecer excelente relação entre resistência e peso. Também apresentam modos de dano menos intuitivos do que metais homogêneos. Fibras, matriz, vazios, delaminações e interfaces podem degradar-se sem produzir a mesma assinatura visual de uma deformação metálica.

Isso não torna o compósito inadequado por definição. Torna indispensáveis um processo de fabricação controlado, critérios de aceitação, ensaios representativos, rastreabilidade e um programa de vida útil capaz de relacionar cada ciclo à condição estrutural real.

A investigação apontou inadequações no projeto e nos processos de certificação, manutenção e inspeção. O problema não era simplesmente usar um material novo. Era transportar pessoas antes que o sistema de evidências fosse proporcional à novidade e à consequência.

Quando a tecnologia se afasta do caminho conhecido, a independência da verificação torna-se parte do projeto, não uma etapa opcional depois dele.

A certificação tratada como obstáculo

Classificação independente não garante que nada falhará. Sua função é obrigar o projeto a explicar materiais, cálculos, ensaios, fabricação, inspeção e limites a especialistas que não dependem do cronograma comercial.

A OceanGate operou o Titan sem a classificação convencional do veículo completo. A justificativa pública associava a escolha à velocidade da inovação e às limitações de regras criadas para tecnologias tradicionais.

Esse argumento contém uma verdade parcial. Normas podem atrasar mudanças e não antecipam todo projeto. Mas a conclusão correta seria construir um caminho alternativo de verificação igualmente independente e rigoroso. Não eliminar a discordância externa.

O protocolo superior não exige obedecer cegamente a qualquer padrão. Exige demonstrar, diante de terceiros competentes, por que a solução diferente protege melhor ou com segurança equivalente.

Os avisos e a cultura

Advertências internas e externas questionaram o projeto, os ensaios e a maneira de comunicar riscos. A investigação da Guarda Costeira descreveu uma cultura de trabalho tóxica e um processo de denúncia ineficaz.

O alerta técnico raramente chega com autoridade própria. Precisa de um canal que proteja quem fala, registre a questão, imponha avaliação independente e mantenha a operação parada até que a dúvida seja resolvida.

Em organizações dominadas pela figura do fundador, discordar pode ser interpretado como falta de visão ou incapacidade de compreender a inovação. A lealdade à missão passa a ser medida pela disposição de continuar.

O problema deixa de ser a qualidade do argumento e passa a ser quem possui autoridade para defini-lo como válido. Nesse ambiente, o protocolo existe apenas enquanto coincide com a convicção central.

O monitoramento que não substitui prova

O Titan usava monitoramento acústico para acompanhar sinais do casco durante os mergulhos. Sensores podem ampliar conhecimento e detectar mudanças. Mas um alarme não prova, por si, que existe tempo suficiente entre detectar e perder a estrutura.

Monitoramento é barreira quando a organização conhece o que o sinal significa, possui limites validados e reage antes que a condição se torne irreversível. Sem isso, o sistema apenas acompanha a aproximação do perigo.

A tentação é usar o sensor como autorização para reduzir ensaios, inspeções ou margens. A lógica se inverte: em vez de confirmar que o projeto é seguro e monitorar sua preservação, a operação confia que o monitor avisará quando deixar de ser.

Barreiras preventivas precisam permanecer antes das barreiras de detecção. Tecnologia de alerta não pode receber sozinha a responsabilidade de corrigir um projeto ainda incerto.

Ciclos, reparos e memória estrutural

Cada descida e subida submetia o casco a um novo ciclo de pressão. Um sistema desse tipo precisa conhecer sua história: fabricação, ensaios, mergulhos, anomalias, reparos, armazenamento e critérios de retirada.

Vida útil não pode ser uma impressão acumulada de sucesso. O fato de um mergulho terminar bem informa que a estrutura sobreviveu àquela exposição. Não demonstra automaticamente quanto dano interno permaneceu ou quantos ciclos seguros ainda existem.

Depois de um sinal anormal ou dano relevante, a resposta precisa reconstruir a condição de projeto. Reparar não significa restaurar sem prova. O sistema deve demonstrar que a intervenção devolveu integridade e que os critérios de inspeção conseguem enxergar o modo de falha esperado.

A normalização nasce quando cada sobrevivência reduz o peso do desconhecido, embora a carga continue acumulando-se no material.

A operação que dependia de uma exceção regulatória

A investigação também identificou lacunas na estrutura regulatória nacional e internacional para submersíveis experimentais e veículos de desenho novo. Lacuna legal, porém, não é ausência de dever técnico.

Quando a regra específica não alcança uma tecnologia, o protocolo recua um nível: identificar riscos, buscar revisão independente, definir critérios

conservadores, registrar incertezas e impedir transporte de pessoas até que a segurança seja demonstrada.

Operar dentro de um espaço não claramente proibido pode ser juridicamente diferente de demonstrar que a operação é segura. Confundir essas perguntas transforma ausência de fiscalização em aprovação implícita.

Organizações maduras tratam a lacuna como razão para aumentar a prudência. Organizações capturadas pela missão tratam a lacuna como oportunidade para avançar antes que alguém consiga detê-las.

O PONTO DE RUPTURA

PROTOCOLO

Projeto tripulado inovador deve demonstrar integridade por ensaios representativos, certificação ou revisão independente, controle de fabricação, inspeção, vida útil e reação protegida a alertas.

PRIMEIRA QUEBRA

O Titan transportou pessoas sem um processo de projeto, certificação, manutenção e inspeção proporcional ao risco, enquanto advertências técnicas perderam autoridade.

CONSEQUÊNCIA

O submersível foi perdido durante a descida ao Titanic em junho de 2023, causando a morte das cinco pessoas a bordo.

SE FOSSE CUMPRIDO

A operação comercial não começaria antes da validação independente. Dúvidas sobre casco, ciclos e reparos manteriam o veículo fora de serviço até demonstração de integridade.

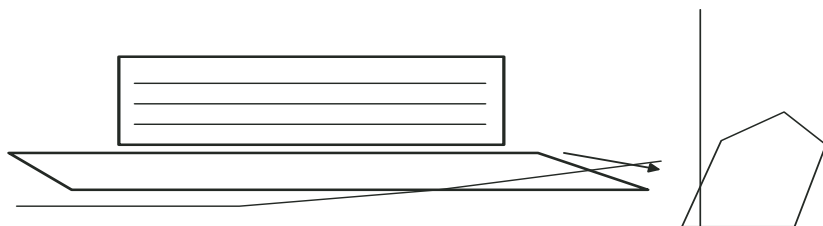
VEREDITO

A pressão aplicou a carga. A primeira quebra ocorreu quando inovação foi usada como argumento para dispensar a prova que deveria autorizar o transporte de pessoas.

Nota documental: Marine Board of Investigation, USCG (2025). Relatório de investigação e recomendações, distinto de decisão judicial. Ver ND-24, p. 147.

O Titan avançou porque a prova independente foi afastada. O Costa Concordia avançou porque uma rota segura foi substituída por uma decisão pessoal.

O desvio que virou espetáculo



13 de janeiro de 2012. O Costa Concordia havia deixado Civitavecchia com mais de quatro mil pessoas a bordo. A rota planejada mantinha o navio afastado da Ilha de Giglio. Naquela noite, a embarcação aproximou-se da costa.

Às 21h45, o casco atingiu uma formação rochosa. A água comprometeu energia e estabilidade. A evacuação terminou com 32 mortes.

| A rocha abriu o casco. O espetáculo retirou a margem.

A rota que existia para não depender de habilidade extraordinária

Rotas marítimas não são linhas decorativas no mapa. Incorporam profundidade, distância de perigos, velocidade, capacidade de manobra e espaço para corrigir desvios. Sua função é transformar conhecimento coletivo em um caminho que não dependa de improviso.

A aproximação à ilha não era necessária para chegar ao destino. Produzia visibilidade, proximidade e uma experiência para quem observava de terra e do navio. O benefício aparecia imediatamente. A margem retirada permanecia invisível.

Quando um desvio é repetido sem consequência, pode ganhar o status de tradição informal. A prática passa a parecer controlada porque alguém já a executou antes. O precedente substitui a avaliação atual.

O protocolo deveria exigir autorização, avaliação e distância suficiente. A autoridade pessoal transformou o caminho validado em sugestão.

O passadiço que não conseguiu contestar

A navegação de um grande navio é trabalho de equipe. Cartas, radares, sistemas eletrônicos, oficiais e procedimentos existem para detectar divergências antes que a embarcação alcance uma condição sem recuperação.

Essa redundância só funciona quando o grupo possui permissão real para questionar a decisão superior. Se a hierarquia converte discordância em desafio pessoal, vários profissionais podem observar o mesmo risco sem produzir uma correção efetiva.

No Costa Concordia, a investigação descreveu falhas de planejamento, condução e coordenação no passado. O problema não foi falta absoluta de informação. Foi a incapacidade de transformar informação disponível em contestação e mudança de rumo com antecedência.

Protocolos de comunicação precisam definir palavras, gatilhos e obrigações que sobrevivam à diferença de cargo. Caso contrário, a última decisão continua concentrada no mesmo ponto que criou o risco.

Depois do impacto, outra margem começou a desaparecer

O choque não encerrou as oportunidades de proteção. A partir dele, a prioridade deveria ser reconhecer a extensão do dano, comunicar a emergência, organizar o abandono e reduzir o tempo de exposição.

A demora em compreender e declarar a gravidade consumiu minutos preciosos. Passageiros receberam informações tranquilizadoras enquanto a condição de energia e estabilidade se deteriorava.

Organizações frequentemente resistem a nomear a emergência porque a palavra produz custos, autoridades externas e perda de controle narrativo. Enquanto o evento ainda pode ser chamado de falha elétrica ou dificuldade técnica, existe a tentação de administrá-lo internamente.

A primeira quebra foi o desvio. A segunda foi permitir que a necessidade de preservar normalidade atrasasse a resposta à realidade já criada.

Evacuação como última margem

Abandonar um navio com milhares de pessoas exige iluminação, comunicação, tripulação treinada, rotas acessíveis e tempo. Quando a embarcação aderna, tarefas simples tornam-se progressivamente mais difíceis.

A evacuação não foi projetada para compensar qualquer decisão de navegação. Era a última barreira, destinada a proteger quando camadas anteriores já haviam falhado. Recebeu um cenário agravado por atraso, perda de energia e inclinação crescente.

É um erro comum avaliar a última defesa como se tivesse enfrentado a ocorrência original. Na realidade, ela enfrenta tudo o que decisões anteriores deixaram passar. Quanto mais tarde é acionada, menos capacidade conserva.

Mesmo depois da primeira quebra, declarar cedo, organizar o abandono e comunicar com clareza poderiam reduzir a consequência. A responsabilidade permanece em camadas.

O PONTO DE RUPTURA

PROTOCOLO

Manter a rota planejada e autorizar qualquer aproximação apenas com avaliação formal de distância, profundidade, velocidade, correção e coordenação da equipe de ponte.

PRIMEIRA QUEBRA

O navio deixou a rota regular para uma passagem próxima à Ilha de Giglio sem necessidade operacional, tornando a segurança dependente de uma manobra pessoal.

CONSEQUÊNCIA

O casco foi rompido, energia e estabilidade foram comprometidas e uma evacuação tardia contribuiu para 32 mortes.

SE FOSSE CUMPRIDO

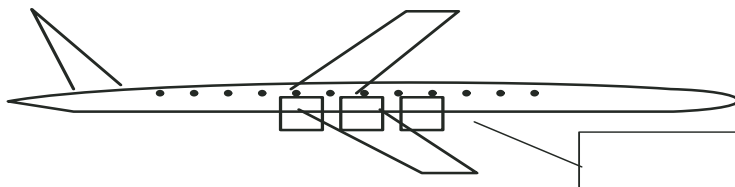
A embarcação permaneceria afastada das rochas. Mesmo após o impacto, comunicação e abandono imediatos preservariam mais tempo e capacidade de resposta.

VEREDITO

A rocha abriu o casco. A primeira quebra ocorreu quando uma rota criada para proteger milhares de pessoas foi substituída por uma aproximação criada para impressionar. No Costa Concordia, o risco recebeu o nome de espetáculo. No ValuJet 592, recebeu um nome ainda mais eficiente: carga vazia.

Nota documental: Relatório da investigação técnica de segurança marítima italiana (2013), preservando a distinção entre navegação e evacuação. Ver ND-25, p. 148.

O perigo embarcado como carga comum



11 de maio de 1996. O voo 592 deixou Miami para Atlanta com 110 pessoas a bordo. Pouco depois da decolagem, a tripulação informou fumaça e tentou retornar. A aeronave caiu nos Everglades cerca de dez minutos após partir.

No compartimento dianteiro estavam caixas descritas como recipientes de oxigênio vazios. Dentro delas havia geradores químicos ainda capazes de produzir oxigênio e intenso calor.

O perigo não desapareceu. Apenas recebeu um nome que impediu o sistema de reconhecê-lo.

O dispositivo que parecia consumido

Geradores químicos de oxigênio serviam ao sistema de emergência dos passageiros. Quando acionados, produziam oxigênio por reação interna e alcançavam temperaturas elevadas. Retirá-los da aeronave não retirava automaticamente a energia que permanecia dentro deles.

Os dispositivos haviam chegado ao fim de sua vida de serviço e foram removidos durante manutenção. Alguns não haviam sido ativados. Deveriam receber tampas de segurança ou ser neutralizados de maneira controlada antes de qualquer transporte.

As tampas não foram instaladas, embora formulários indicassem a conclusão das tarefas. O risco atravessou manutenção e inspeção com uma aparência administrativa de serviço terminado.

O protocolo de descarte precisa começar reconhecendo que um componente pode deixar de ser útil e continuar plenamente capaz de produzir energia, reação, pressão ou contaminação.

A palavra que apagou o risco

Os geradores foram colocados em caixas e descritos na documentação como recipientes de oxigênio vazios. Para quem recebeu a carga, a expressão indicava objetos inertes, sem conteúdo e sem exigência especial.

Se o documento dissesse geradores químicos não acionados, surgiriam perguntas: foram neutralizados? Possuem tampas? Podem viajar por via aérea? Qual embalagem e identificação são exigidas?

A descrição incorreta retirou essas perguntas da cadeia. Agentes de rampa e tripulação receberam caixas que pareciam comuns porque o sistema anterior havia eliminado a informação necessária para reconhecê-las como perigosas.

Classificação é uma barreira. Quando o nome não representa a condição física, todos os controles seguintes podem funcionar exatamente como foram desenhados e ainda assim conduzir o perigo até a operação.

Terceirização que fragmentou a responsabilidade

A manutenção havia sido executada por empresa contratada. Terceirizar trabalho não transfere automaticamente o dever de assegurar que riscos, competências, materiais, registros e resultados permaneçam sob controle.

A investigação do NTSB atribuiu falhas à empresa de manutenção na preparação, embalagem e identificação dos geradores. Também apontou falhas da companhia aérea na supervisão do programa de manutenção contratada e na garantia de conformidade com regras de materiais perigosos.

Manutenção, almoxarifado, expedição e operação aérea pareciam processos separados. Para o gerador, eram uma única viagem. Cada área presumiu que a anterior havia tornado o objeto seguro ou descrito corretamente sua condição.

O protocolo precisa atravessar empresas. Deve definir quem verifica, quem aceita, que evidência acompanha o item e quem pode interromper o embarque.

O compartimento que não poderia conter aquele incêndio

Os geradores provavelmente foram acionados por movimento durante o carregamento ou a decolagem. O calor encontrou embalagens e pneus, enquanto o oxigênio produzido alimentou o incêndio.

O compartimento de carga não possuía sistema de detecção e supressão capaz de controlar rapidamente aquele cenário. A tripulação recebeu o alerta quando a condição já avançava fora de sua visão e com pouco tempo para retorno.

A última barreira foi obrigada a compensar erros de manutenção, inspeção, classificação, embalagem, aceitação e supervisão. Nenhum piloto poderia reconstruir, em minutos, a informação que vários processos haviam apagado antes do voo.

O incêndio foi o gatilho visível. A cadeia começou quando o componente ativo foi autorizado a viajar como carga comum e cada etapa seguinte recebeu uma versão menos perigosa da realidade.

O PONTO DE RUPTURA

PROTOCOLO

Neutralizar ou proteger geradores não acionados, classificá-los como material perigoso, embalar e documentar corretamente, além de verificar manutenção terceirizada e aceitação da carga.

PRIMEIRA QUEBRA

Componentes ainda ativos foram tratados como serviço concluído e descritos como recipientes vazios, apagando o perigo da documentação e da decisão de embarque.

CONSEQUÊNCIA

Um incêndio alimentado pelos geradores atingiu o compartimento de carga e a aeronave caiu, causando a morte das 110 pessoas a bordo.

SE FOSSE CUMPRIDO

Os dispositivos seriam neutralizados, segregados ou recusados para transporte. Mesmo um erro de manutenção seria capturado pela classificação e aceitação da carga.

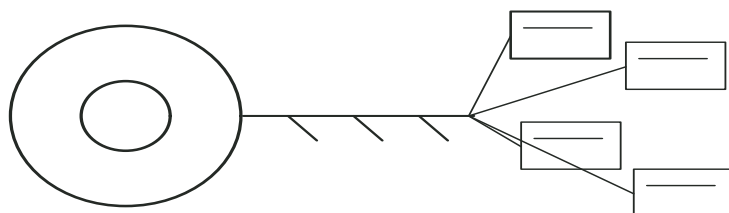
VEREDITO

O fogo derrubou o avião. A primeira quebra ocorreu quando um componente ainda perigoso atravessou a cadeia recebendo um nome mais inofensivo do que sua condição real.

Nota documental: NTSB/AAR-97/06 (1997). A investigação trata de geradores de oxigênio, manutenção contratada, supervisão e proteção da carga. Ver ND-26, p. 148.

Os casos examinados receberam avisos, resultados, rotas, relatórios ou classificações capazes de interromper a sequência. O capítulo seguinte examina o que acontece quando o defeito já possui nome e histórico, mas ainda não recebe uma decisão.

O defeito que viajou entre departamentos



General Motors, 2002 a 2014. O interruptor de ignição era pequeno, barato e capaz de mover-se da posição de funcionamento para acessório ou desligado. Quando isso ocorria, o motor podia parar e os airbags frontais podiam não ser acionados em determinados acidentes.

O defeito não permaneceu invisível. Testes, reclamações, paradas de motor, investigações e acidentes produziram informação durante anos. O problema foi fazer essa informação chegar a uma decisão de recall.

O conhecimento existia em partes. A responsabilidade pelo todo não conseguiu encontrá-lo a tempo.

Uma peça pequena com efeito sistêmico

O interruptor precisava manter posição diante do peso do chaveiro, vibração e movimentos normais. Protótipos apresentaram torque abaixo da própria especificação interna antes da produção, mas a peça foi aprovada.

Mover-se para acessório ou desligado não significava apenas perder potência. Em certos modelos, podia interromper sistemas elétricos e impedir o acionamento dos airbags frontais. Uma falha discreta no comando da ignição alterava o comportamento de diversas barreiras do veículo.

Essa é uma característica de componentes críticos: seu preço ou tamanho não mede sua importância. O valor da barreira depende da função que controla e da consequência de perder autoridade.

Quando a especificação falha antes da produção, o protocolo deveria bloquear o lançamento ou exigir redesign. Aprovar cria uma dívida técnica que cada veículo leva para a estrada.

O sinal que mudava de nome

Nos primeiros anos, relatos de desligamento foram tratados como problema de conveniência, experiência do usuário ou peso excessivo no chaveiro. A classificação inicial decidiu a velocidade da resposta.

Se o evento é chamado de incômodo, a solução pode ser um aviso ao cliente. Se é classificado como defeito de segurança, exige investigação regulatória, comunicação e recall. O mesmo fenômeno físico recebe rotas diferentes dentro da organização conforme o nome administrativo que lhe é atribuído.

Em 2004 e 2005, a empresa considerou mudanças, mas decidiu que a condição não representava risco de segurança. Recomendações de uso ocuparam o lugar de uma correção estrutural.

A primeira quebra organizacional ocorreu quando um resultado fora da especificação e desligamentos reais foram enquadrados abaixo do nível capaz de acionar o sistema de segurança.

O conhecimento que não conseguia formar uma história

Engenharia conhecia a resistência insuficiente. Assistência via desligamentos. Jurídico acompanhava ocorrências. Investigadores de acidentes encontravam airbags não acionados. Cada área possuía fragmentos, mas o sistema não os reuniu cedo o bastante.

Organizações complexas dependem de processos que conectem dados de garantia, reclamações, acidentes, testes, fornecedores e mudanças de projeto. Sem uma função de integração, cada departamento pode concluir que sua evidência é insuficiente e esperar que outro enxergue o padrão.

A investigação mostrou que, em 2012, pessoas dentro da GM já conheciam a ligação entre o interruptor e a não ativação de airbags em alguns veículos. A comunicação ao regulador e ao público ocorreu apenas em fevereiro de 2014.

A ausência de um dono do risco permite que muitos profissionais façam seu trabalho localmente e o sistema falhe globalmente.

O recall que precisava chegar pronto

O Departamento de Justiça afirmou que o processo interno atrasou a decisão enquanto a empresa buscava empacotar, explicar e administrar o problema. A investigação foi mantida fora do fluxo regular de recall em parte do período.

Essa é uma tentação recorrente. A organização deseja compreender toda a população afetada, preparar peças, prever custos e controlar a comunicação antes de reconhecer publicamente a condição. O problema é que veículos continuam em uso durante a busca pela resposta perfeita.

Protocolos de emergência devem permitir decisões parciais e conservadoras. Quando existe evidência suficiente para identificar um grupo de risco, a proteção desse grupo não pode esperar que todas as perguntas estejam resolvidas.

Recall não é cerimônia final de uma investigação. É uma barreira de contenção que precisa começar enquanto a investigação continua.

O PONTO DE RUPTURA

PROTOCOLO

Bloquear componente fora de especificação, integrar testes, reclamações e acidentes, classificar rapidamente qualquer risco de segurança e comunicar o defeito ao regulador dentro do prazo.

PRIMEIRA QUEBRA

O interruptor foi aprovado apesar de desempenho abaixo da especificação, e sinais posteriores foram classificados e fragmentados de forma que não produziram correção e recall tempestivos.

CONSEQUÊNCIA

Veículos permaneceram em circulação com possibilidade de desligamento e não acionamento de airbags, contribuindo para mortes e lesões, além de recalls amplos e sanções.

SE FOSSE CUMPRIDO

A peça seria redesenhada antes da produção ou retirada do mercado quando surgiram os primeiros sinais, preservando airbags e reduzindo a população exposta.

VEREDITO

O interruptor desligava o veículo. A primeira quebra ocorreu quando uma peça fora da especificação foi autorizada a entrar em produção e o conhecimento posterior não encontrou um processo capaz de transformá-lo em recall.

Nota documental: Comunicado oficial do DOJ (2015), que descreve admissões e acordo de diferimento da persecução penal. Não se apresenta o acordo como julgamento de todos os envolvidos. Ver ND-27, p. 149.

O protocolo de reconhecer um defeito

Empresas costumam possuir procedimentos para desenvolver, testar e liberar produtos. Menos visível é o protocolo que começa depois da venda: como uma reclamação se transforma em sinal, como sinais formam um padrão e como o padrão ganha autoridade para retirar o produto do mercado.

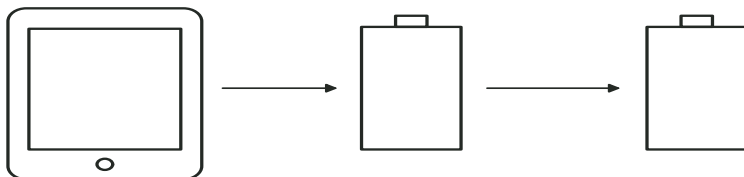
Esse sistema precisa responder a cinco perguntas simples. Quem reúne as fontes? Quem classifica o risco? Que evidência é suficiente para agir? Quem pode ordenar recall? Quanto tempo a organização aceita permanecer em dúvida?

ETAPA	O PROTOCOLO PRECISA ASSEGURAR
DETECÇÃO	Teste, reclamação, incidente, garantia ou informação externa.
INTEGRAÇÃO	Dados diferentes são conectados ao mesmo modo de falha.
CLASSIFICAÇÃO	A consequência potencial define prioridade e prazo.
CONTENÇÃO	Venda, uso ou distribuição são interrompidos antes da conclusão total.
APRENDIZAGEM	Projeto, processo, fornecedores e critérios são corrigidos e verificados.

Quando uma dessas etapas não possui dono, o defeito viaja pela organização procurando alguém que tenha informação e autoridade ao mesmo tempo.

A pior forma de desconhecimento é aquela produzida por uma empresa que sabe tudo em departamentos separados.

Três produtos, três verdades adiadas



O telefone substituído que também precisou ser recolhido

Samsung Galaxy Note7, 2016

Relatos de superaquecimento e incêndio levaram ao primeiro recall do Galaxy Note7. Consumidores receberam reembolso ou aparelhos de substituição. O problema parecia contido.

Novos incidentes envolveram também unidades substitutas. A solução criada para restaurar confiança precisava ser recolhida. A autoridade americana ampliou o recall e orientou todos os usuários a desligar os aparelhos.

O caso mostra uma regra desconfortável: ação corretiva não é eficaz porque foi executada rapidamente ou em grande escala. Precisa demonstrar que eliminou o modo de falha. Quando a segunda população repete o perigo, o protocolo deve voltar ao início, não defender a primeira solução.

LIMITE: Recall e substituição devem depender de causa compreendida, solução validada e verificação da nova população.

QUEBRA: A primeira resposta colocou no mercado aparelhos substitutos antes de demonstrar que todas as causas relevantes estavam controladas.

CONSEQUÊNCIA: O recall precisou ser ampliado para incluir os aparelhos originais e os de substituição, encerrando o produto.

A correção conhecida que não encontrou o sistema

Equifax, 2017

Uma vulnerabilidade crítica no Apache Struts foi divulgada em março de 2017. A política interna exigia aplicação do patch em 48 horas. O sistema vulnerável permaneceu sem correção até a descoberta da invasão meses depois.

O ataque expôs dados de aproximadamente 148 milhões de consumidores. O relatório do Congresso americano considerou a violação totalmente evitável e mostrou que havia política, alertas e responsabilidades descritas, mas faltavam proprietários claramente designados, redundância e confirmação de execução.

O e-mail avisou. O procedimento definiu prazo. O controle falhou porque ninguém conseguiu provar que cada ativo relevante havia sido identificado, corrigido e verificado.

LIMITE: Vulnerabilidade crítica exige inventário confiável, responsável nomeado, correção no prazo e varredura de confirmação.

QUEBRA: A política existia, mas a execução dependia de um sistema de honra, sem designação clara e sem redundância suficiente.

CONSEQUÊNCIA: Uma falha conhecida permaneceu aberta e permitiu uma das maiores exposições de dados pessoais registradas nos Estados Unidos.

A demonstração que não precisava medir

Theranos

A empresa prometia realizar numerosos exames com pequenas quantidades de sangue por meio de tecnologia própria. A narrativa era simples, poderosa e difícil de verificar porque a operação permanecia protegida por segredo.

A acusação criminal descreveu demonstrações nas quais investidores acreditavam que o equipamento analisava sangue quando executava um protocolo nulo. Também alegou o uso de analisadores comerciais enquanto a empresa dizia empregar tecnologia própria. A nota ND-30 distingue essas alegações dos resultados dos julgamentos.

O caso não é apenas sobre mentira. É sobre uma organização que retirou os protocolos capazes de confrontar a promessa: validação independente, transparência técnica, comparação com método de referência e liberdade para especialistas discordarem.

LIMITE: Tecnologia diagnóstica deve demonstrar precisão, validação clínica, rastreabilidade e limites antes de orientar decisões médicas.

QUEBRA: A narrativa comercial avançou enquanto demonstrações e informações não permitiam verificar a capacidade real da tecnologia.

CONSEQUÊNCIA: Investidores foram fraudados e médicos e pacientes receberam afirmações e resultados que o sistema não conseguia sustentar com prova adequada.

O momento em que saber deixa de ser desculpa

Os dez casos — Grenfell a Theranos, atravessam moradia, alimentos, exploração submarina, navegação, aviação, automóveis, eletrônicos, cibersegurança e diagnóstico. A diversidade mostra que a quebra não pertence a uma tecnologia específica.

CASO	O SINAL	O QUE DEVERIA PARAR
Grenfell	Mudança, testes e alertas	Fachada sem prova do sistema
PCA	Resultados de Salmonella	Liberação e expedição
AdeS	CIP ativo e envase reaberto	Produção durante higienização
Titan	Advertências e incerteza estrutural	Mergulhos tripulados
Costa	Rota e proximidade da costa	Desvio para espetáculo
ValuJet	Componente ativo e sem tampas	Aceitação como carga comum
GM	Especificação, desligamentos e acidentes	Produção e demora no recall
Note7	Incidentes em originais e substitutos	Continuidade do produto
Equifax	Alerta de vulnerabilidade crítica	Sistema sem patch
Theranos	Validação insuficiente	Venda da promessa como prova

O aviso muda de nome, o resultado é relativizado e a dúvida é empurrada para outra área. A quebra acontece quando saber deixa de produzir a obrigação de parar.

Com os 31 casos apresentados até aqui, o leitor já pode reconhecer essa arquitetura. O Qantas 32 completará os 32 casos desta edição. O próximo movimento organiza as formas de quebra, mostra quem responde por cada camada e prepara o caminho para interromper a corrente.

Fontes dos casos deste interlúdio: ND-28, p. 149; ND-29, p. 150; ND-30, p. 150.

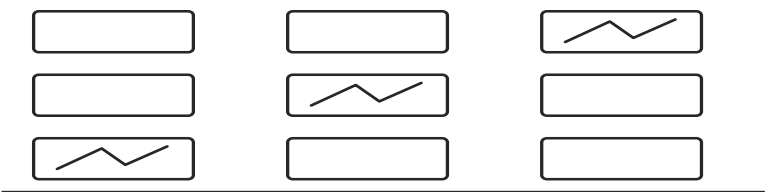
PARTE IV

ANATOMIA DA QUEBRA

Depois dos casos, o padrão já não precisa de outra tragédia para se tornar visível.



As nove formas de quebrar um protocolo



O documento pode existir e o controle já ter desaparecido.

Na sala de reunião, o procedimento estava projetado na tela. Tinha código, revisão, responsáveis e uma lista de assinaturas. Ninguém poderia dizer que a empresa não possuía regra.

Na operação, porém, a regra era outra. O equipamento não permitia executar todas as etapas no tempo previsto. O supervisor conhecia o atalho. O gerente conhecia o atraso que o cumprimento produziria. A auditoria conhecia apenas o documento.

O caso não cabia na divisão confortável entre “há protocolo” e “não há protocolo”. Havia papel. Faltava autoridade.

Um protocolo quebra sempre que deixa de controlar o risco para o qual foi criado.

As nove formas, em uma visão única

1. Não existe	2. É inadequado	3. Está desatualizado
4. É impraticável	5. Não foi treinado	6. Não foi executado
7. Não foi verificado	8. Não gerou reação	9. Não incorporou aprendizado

1. O protocolo não existe

A forma mais visível da quebra é a ausência. O risco está presente, mas nenhuma regra, barreira, especificação ou critério de parada foi criado para controlá-lo.

Em uma pequena organização, a ausência pode resultar de desconhecimento. Em sistemas complexos, ela costuma revelar uma falha anterior. Processos de

gestão de risco, controle de mudanças, aprendizagem com incidentes e revisão de projeto deveriam identificar a necessidade de proteção.

Quando o controle específico não existe, a investigação precisa subir um nível. Quem deveria reconhecer o risco? Qual fórum deveria convertê-lo em requisito? Por que a experiência disponível não produziu uma regra?

Não criar um protocolo necessário também é uma decisão organizacional, mesmo quando ninguém se reuniu para tomá-la.

2. O protocolo é inadequado. 3. Está desatualizado

Uma regra pode existir e ainda assim controlar o risco errado. Ela cobre a situação normal, mas não a condição extrema. Exige uma inspeção visual onde seria necessário medir. Define uma reserva que já não corresponde à rota. Prescreve uma barreira dimensionada para uma carga que o processo deixou para trás.

Também pode ter sido correta no passado. A matéria-prima mudou, o software foi atualizado, o equipamento envelheceu, o volume cresceu ou a legislação evoluiu. O documento permaneceu intacto enquanto o processo se transformava.

Esse tipo de quebra é silencioso porque a conformidade continua possível. As pessoas cumprem exatamente aquilo que está escrito e ainda assim deixam o risco avançar.

A pergunta decisiva não é “o procedimento foi seguido?” É “o procedimento ainda representa o processo real?”

4. O protocolo é impraticável. 5. Não foi treinado

Há regras escritas para um mundo que não existe. Exigem tempo indisponível, ferramentas que não chegam ao turno, sistemas que ficam fora do ar ou um número de pessoas diferente daquele que a escala oferece.

Quando cumprir se torna incompatível com entregar, a operação aprende a escolher. Primeiro pede autorização. Depois comunica. Em seguida, apenas repete o atalho que todos conhecem.

Outra regra pode ser tecnicamente adequada e operacionalmente executável, mas nunca ter sido convertida em competência. Ler um procedimento não equivale a treinar. Assinar presença não demonstra que alguém consegue reconhecer a condição, executar a resposta e explicar por que ela existe.

Treinamento real aparece no momento da pressão. A pessoa identifica o sinal, sabe o que fazer e possui confiança para interromper a sequência.

6. O protocolo não é executado. 7. Não é verificado

A sexta forma é a mais conhecida: a regra existe, funciona e foi compreendida, mas alguém decide não cumpri-la. Às vezes por pressa. Às vezes por conveniência. Às vezes porque a experiência anterior terminou bem.

A sétima forma explica por que a sexta sobrevive. O sistema não observa a rotina, não testa a barreira, não confronta dados independentes e não reage aos desvios. A organização depende da declaração de que tudo foi feito.

Verificar não é procurar culpados. É comparar a prática com o padrão antes que a consequência faça essa comparação de maneira irreversível.

Sem verificação, o procedimento se torna uma promessa privada. Cada turno decide quanto dele continua obrigatório.

8. O protocolo não é corrigido. 9. Não é aperfeiçoado

Uma barreira pode falhar e o sistema responder com um documento adicional, uma assinatura e uma data de conclusão. A causa permanece. A ação fecha.

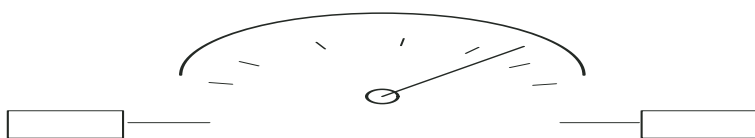
Não corrigir significa conhecer a deficiência e permitir que ela continue. Não aperfeiçoar é algo diferente. O controle ainda funciona, mas sinais, incidentes e mudanças mostram que sua margem está diminuindo. A organização espera a falha para atualizar aquilo que já poderia melhorar.

Os trinta e um casos deste livro cabem em combinações dessas nove formas. Em alguns, o protocolo não existia. Em outros, estava desligado, era incapaz, não foi executado ou não produziu reação. Quase nunca houve apenas uma forma.

A utilidade da classificação não é simplificar a história. É impedir que a investigação termine na frase confortável: “o procedimento não foi seguido”.

FORMA	O QUE REALMENTE SE PERDE
1. Inexistente	O risco não recebeu controle específico.
2. Inadequado	A barreira não controla a condição real.
3. Desatualizado	O processo mudou e a regra ficou.
4. Impraticável	Cumprir exige condições que não existem.
5. Não treinado	A regra não virou competência.
6. Não executado	O limite foi conscientemente ultrapassado.
7. Não verificado	A prática não é confrontada com evidência.
8. Não corrigido	A deficiência conhecida permanece.
9. Não aperfeiçoado	O aprendizado não amplia a margem.

Quando a meta derrota o limite



O número não precisa mandar. Basta que todos acreditem que ele manda.

A reunião começava sempre pela mesma tela. Produção, custo, entrega, perdas, segurança. Quase tudo estava verde. Um item permanecia amarelo, mas o fechamento do mês estava próximo.

A decisão não foi anunciada como quebra de protocolo. Foi descrita como recuperação de resultado. O risco continuaria por mais um turno. Depois seria tratado.

Quando a meta ganhou a disputa, ninguém precisou ordenar o desvio. A organização já havia ensinado qual número protegia carreiras e qual limite produzia explicações.

Metas orientam o esforço. Tornam-se perigosas quando recebem poder para suspender as condições de operação.

A meta é direção, não licença

Uma meta legítima indica aonde a organização pretende chegar. Um protocolo define as condições mínimas para percorrer o caminho. Os dois instrumentos deveriam se complementar.

O conflito aparece quando o resultado é tratado como obrigação absoluta e o limite como variável negociável. A produção precisa atingir cem. A entrega não pode atrasar. O custo precisa cair. Se o processo real não comporta a exigência, alguém precisa decidir entre revelar a incapacidade ou esconder o desvio.

Sistemas maduros aceitam que uma meta pode ser perdida para preservar um limite. Sistemas frágeis interpretam qualquer parada como incompetência. A mensagem parece motivadora, mas produz uma operação incapaz de admitir que não possui condições para continuar.

A meta deixa de ser instrumento de gestão e vira autorização silenciosa para transferir risco ao futuro.

O indicador verde que esconde o risco

Indicadores não são a realidade. São uma representação escolhida dela. Podem mostrar volume sem mostrar margem, prazo sem mostrar atalhos, acidente sem mostrar quase acidente, reclamação sem mostrar o cliente que desistiu de reclamar.

A Farsa começou quando eventos deixaram de ser registrados. O painel melhorou porque a operação perdeu memória. Wells Fargo transformou metas em

pressão. Dieselgate transformou teste em teatro. Theranos transformou demonstração em promessa.

O problema não está no número. Está na distância entre aquilo que ele afirma e aquilo que a decisão precisa conhecer.

Todo indicador crítico deveria possuir uma pergunta de integridade: que comportamento ele pode induzir e qual parte da realidade ele permite esconder?

Incentivos ensinam antes dos treinamentos

Uma organização pode repetir que segurança vem primeiro e promover quem entrega apesar das condições. Pode defender qualidade e premiar quem reduz bloqueios. Pode falar em transparência e punir quem leva um problema à direção.

As pessoas aprendem rapidamente qual mensagem é institucional e qual é decorativa. O bônus, a promoção, o silêncio do gestor e a reação ao atraso formam um currículo mais convincente que qualquer apresentação.

Incentivos não precisam ser financeiros. Prestígio, acesso, proteção, exposição e estabilidade também selecionam comportamentos. Quando o herói é sempre quem “faz acontecer”, a prudência começa a parecer falta de compromisso.

A cultura real aparece na carreira de quem parou a operação quando o protocolo exigiu.

Como proteger a meta do próprio excesso

Metas precisam de limites explícitos. A organização deve declarar quais condições não podem ser negociadas para entregar o resultado. Deve também separar o desempenho de quem cumpre o plano do desempenho de quem preserva o sistema.

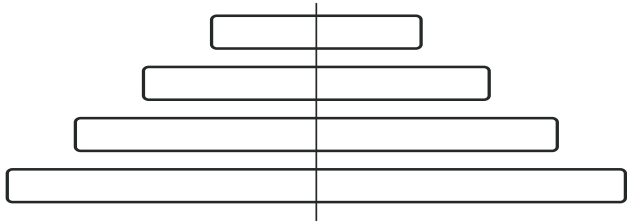
Um atraso causado por falha de planejamento não pode ser transferido ao operador como obrigação de arriscar. Uma parada necessária deve aparecer no resultado com a causa correta, não como fracasso de quem interrompeu.

Reuniões de desempenho precisam perguntar não apenas “quanto entregamos?”, mas “o que foi sacrificado para entregar?” Atalhos, retrabalho, horas excessivas, testes adiados e sinais ignorados são dívidas operacionais. O painel deve torná-las visíveis.

A meta continua importante. Apenas deixa de ocupar o lugar da realidade.

PERGUNTA	O PAINEL TAMBÉM PRECISA MOSTRAR
Resultado	O que foi entregue?
Margem	Que capacidade de absorver imprevistos permaneceu?
Integridade	Que informação foi omitida, reclassificada ou adiada?
Sustentação	O desempenho pode ser repetido sem novos atalhos?

Quem responde pelo sistema



A última pessoa visível raramente é a única pessoa com poder de evitar a sequência.

Depois do colapso, a câmera procura um rosto. O operador que acionou, o piloto que continuou, o técnico que assinou, o funcionário que não percebeu.

A investigação organizacional precisa fazer outra coisa. Precisa reconstruir onde estavam a informação, a autoridade, os recursos e o dever de agir.

Responsabilidade não desaparece porque está distribuída. Mas também não pode ser atribuída apenas a quem tocou o último controle.

A pergunta correta não é somente “quem fez?” É “quem podia impedir, quem deveria saber e quem desenhou as condições da decisão?”

QUEM RESPONDE PELO SISTEMA

DIREÇÃO

prioridades, recursos, incentivos, governança e consequências

GERÊNCIA

existência, adequação, verificação e aperfeiçoamento do sistema

SUPERVISÃO

treinamento, observação, diagnóstico e reação

OPERAÇÃO

execução, percepção e relato

Responsabilidade organizacional não é culpa jurídica automática. É a reconstrução de onde estavam informação, autoridade, recursos e dever de agir.

Responsabilidade em camadas

O operador responde por executar, interromper e relatar. O supervisor responde por treinar, observar, remover obstáculos e reagir. O gerente responde por garantir que o sistema exista, possua recursos, seja verificado e aprenda. A direção responde por prioridades, incentivos, governança e tolerâncias.

Essas camadas não competem. Uma ação direta inadequada pode coexistir com supervisão fraca, protocolo impraticável e metas incompatíveis. Reconhecer o sistema não absolve a decisão individual. Impede apenas que a organização troque uma pessoa e preserve a arquitetura.

Em alguns casos, a pessoa na ponta viola uma regra clara com condições suficientes para cumpri-la. Em outros, executa aquilo que a rotina, os recursos e a liderança transformaram em única opção prática.

A análise séria precisa distinguir as duas situações.

CAMADA	RESPONSABILIDADE PRINCIPAL
Operação	Executar, interromper, registrar e comunicar.
Supervisão	Treinar, observar, diagnosticar e reagir.
Gerência	Assegurar padrão, recursos, verificação e correção.
Direção	Definir prioridades, incentivos, governança e consequências.

A pergunta que muda a investigação

Culpa jurídica depende de lei, jurisdição, conhecimento, nexo causal e prova. Responsabilidade organizacional começa antes. Pergunta quem possuía capacidade de intervenção e que mecanismo deveria usar.

Uma matriz simples ajuda. Quem sabia? Quem deveria saber? Quem podia parar? Quem controlava recursos? Quem validou a mudança? Quem verificava a barreira? Quem recebeu o alerta e qual reação era esperada?

Quando as respostas apontam para muitas áreas, isso não significa que ninguém responde. Significa que o protocolo de integração também precisa ser investigado.

O risco mais difícil é aquele que viaja entre departamentos. Cada área enxerga um fragmento, enquanto nenhuma possui o quadro completo e a autoridade para agir.

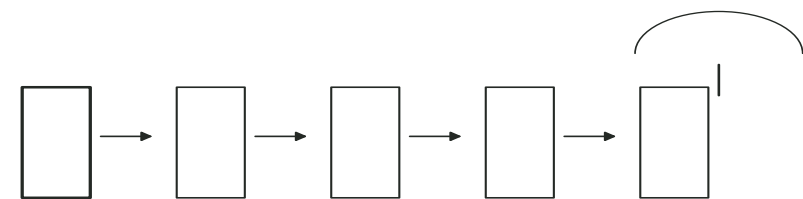
PARTE V

ANTES QUE QUEBRE

Prevenir não é imaginar todos os acidentes. É impedir que o primeiro desvio perca o poder de interromper a sequência.



O protocolo que funciona



A regra só existe de verdade quando continua valendo no pior momento.

O operador segurava a etiqueta vermelha. Atrás dele, a linha acumulava produto, o telefone tocava e o prazo já havia sido perdido.

A inspeção encontrara uma condição fora do limite. Parar era tecnicamente simples e organizacionalmente difícil.

Ele bloqueou o equipamento. O supervisor chegou, confirmou a condição e protegeu a decisão. Ninguém chamou o ato de heroísmo. Era apenas o sistema funcionando.

Um bom protocolo transforma coragem individual em rotina organizacional.

Escrito, compreendido e executável

O primeiro requisito é clareza. A pessoa precisa reconhecer quando a regra se aplica, qual ação executar e que condição permite retomar. Ambiguidade pode parecer flexibilidade, mas transfere a decisão crítica para o momento de maior pressão.

O segundo requisito é compreensão. Não basta decorar etapas. Quem executa precisa entender o risco que cada etapa controla. Esse conhecimento permite reagir quando a situação real não coincide exatamente com o exemplo do treinamento.

O terceiro requisito é viabilidade. Ferramentas, tempo, acesso, pessoal, sistemas e peças devem existir. Quando a organização não fornece condições, o descumprimento deixa de ser surpresa e vira desenho operacional.

A melhor regra é curta o suficiente para ser usada e robusta o suficiente para proteger.

Autoridade e recursos

Um critério de parada sem autoridade produz hesitação. A pessoa sabe o que deveria fazer, mas teme não conseguir sustentar a decisão diante da pressão.

Por isso, protocolos críticos precisam declarar quem pode bloquear, quem pode liberar e que evidência é necessária. A liberação não pode pertencer à mesma pressão que desejava continuar.

Também precisam proteger tempo e recursos. Uma ação que depende de autorização distante, sistema indisponível ou especialista que nunca está presente já nasce enfraquecida.

Autoridade não significa liberdade sem controle. Significa que a primeira resposta segura pode ocorrer antes da negociação econômica.

Verificação, reação e aprendizagem

O protocolo funciona quando deixa evidência. A inspeção registra a condição real. O bloqueio pode ser rastreado. A liberação demonstra que o risco foi removido. A supervisão observa a prática, não apenas o formulário.

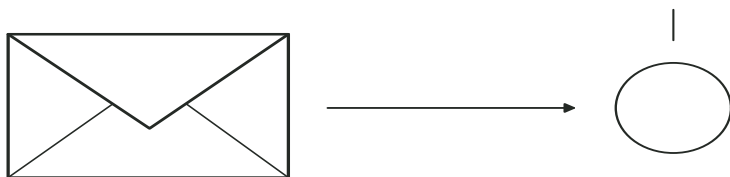
Quando aparece um desvio, a reação precisa ser proporcional. Corrigir o sintoma pode devolver a operação, mas a organização ainda deve perguntar por que a barreira permitiu a condição e onde ela pode se repetir.

Depois, o aprendizado volta ao padrão. Procedimentos, treinamentos, projetos, indicadores e planos de manutenção são atualizados. A ação só termina quando a nova proteção pode ser verificada na rotina.

Esse ciclo transforma o protocolo em sistema vivo.

ELEMENTO	COMO O PROTOCOLO GANHA AUTORIDADE
Clareza	A condição e a resposta são inequívocas.
Competência	A pessoa reconhece, executa e explica.
Condições	Recursos, tempo e ferramentas existem.
Autoridade	Parar e bloquear são decisões protegidas.
Evidência	A execução e a liberação podem ser provadas.
Aprendizagem	O desvio modifica o sistema, não apenas o formulário.

O mensageiro não é o problema



A organização aprende com aquilo que permite chegar inteiro até a decisão.

A primeira reclamação parecia exagerada. O primeiro quase acidente parecia falta de atenção. O primeiro resultado anormal parecia erro de amostragem.

Cada explicação era possível. O perigo estava em usar a possibilidade para encerrar a pergunta.

Sinais chegam incompletos. A função do sistema não é exigir que o mensageiro traga a causa pronta. É preservar o alerta até que a investigação produza evidência.

Quem comunica um problema entrega uma oportunidade de correção.

Punir o mensageiro devolve o risco ao processo.

A organização aprende com aquilo que não pune

Pessoas observam o destino de quem relata. Se o alerta gera investigação, respeito e retorno, outros sinais aparecem. Se gera exposição, ironia, perda de espaço ou questionamento de lealdade, a informação aprende a desaparecer.

O silêncio pode ser confundido com estabilidade. Na realidade, talvez a organização tenha apenas treinado as pessoas a resolver sozinhas, adaptar números ou esperar que o problema alcance outra área.

Liderança receptiva não significa aceitar toda interpretação como correta. Significa separar o valor do sinal da precisão da hipótese. A pessoa pode estar errada sobre a causa e certa ao perceber que algo mudou.

O protocolo de comunicação precisa proteger essa diferença.

Do alerta à decisão

Um canal de denúncia ou uma caixa de sugestões não constitui sistema de reação. O alerta precisa de classificação, responsável, prazo, critério de escalonamento e retorno a quem informou.

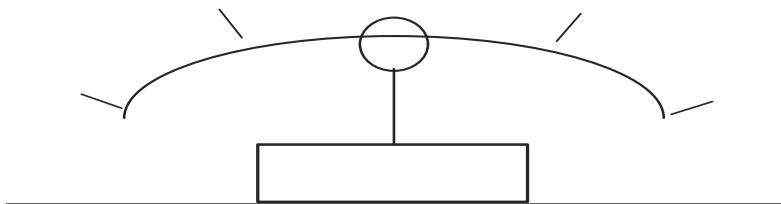
Sinais críticos não podem permanecer presos à hierarquia local. Quando a própria liderança é parte do risco, deve existir rota independente para qualidade, segurança, compliance, engenharia ou conselho.

O fechamento precisa demonstrar evidência. “Orientado”, “treinado” e “conscientizado” não bastam quando o risco envolve projeto, capacidade, conflito de incentivo ou barreira física ausente.

Por fim, o sistema precisa procurar padrões. Uma reclamação isolada pode ser ruído. Dez reclamações isoladas em bancos de dados diferentes podem ser o defeito tentando formar uma história.

ETAPA	O ALERTA PRECISA PRODUZIR
Receber	Preservar o relato sem exigir conclusão pronta.
Classificar	Avaliar gravidade, recorrência e potencial.
Escalonar	Levar o sinal a quem possui autoridade independente.
Investigar	Proteger evidências e testar hipóteses.
Responder	Corrigir, comunicar e verificar eficácia.
Aprender	Conectar casos e atualizar o sistema.

A decisão de parar



Interromper a sequência é uma competência gerencial, não uma derrota operacional.

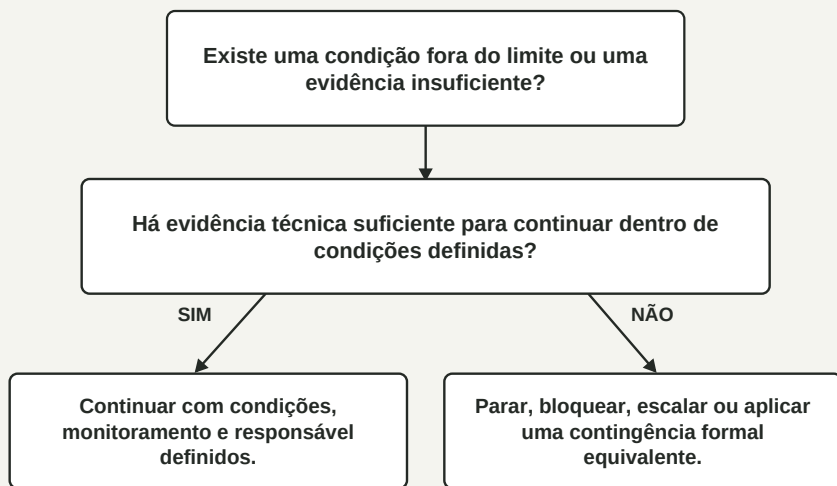
O gerente recebeu a ligação antes do amanhecer. A matéria-prima estava fora da condição, o cliente esperava o lote e a equipe já havia preparado a linha.

A pergunta veio na forma habitual: “dá para continuar com acompanhamento?”

Ele poderia pedir mais uma amostra, reduzir a velocidade ou prometer uma verificação posterior. Em vez disso, perguntou qual evidência autorizava produzir. Não havia. A linha permaneceu parada.

Parar não exige certeza de que o pior acontecerá. Exige reconhecer que a organização perdeu a prova necessária para continuar.

A DECISÃO DE PARAR



A dúvida não autoriza continuar por padrão. Ela exige uma decisão explícita sobre quem aceita o risco e com base em qual evidência.

Parar tem custo. Continuar tem aposta

A parada apresenta imediatamente seus efeitos: produção perdida, atraso, horas adicionais, reclamação e explicações. A continuidade oferece um benefício agora e distribui o risco num futuro incerto.

Essa assimetria favorece a decisão insegura. O custo de cumprir é contabilizado. O custo de romper aparece apenas como probabilidade.

A gestão madura corrige essa comparação. Reconhece que continuar sem barreira é uma aposta feita com ativos que não pertencem apenas a quem decide: pessoas, clientes, comunidade, reputação e futuro da organização.

O protocolo de parada existe para impedir que a pressão transforme incerteza em autorização.

Crítérios antes da pressão

As melhores decisões de parada são construídas antes do evento. Limites, alarmes, intertravamentos e condições de liberação precisam estar definidos enquanto a organização ainda consegue pensar sem prazo sobre a mesa.

Também é necessário prever zonas cinzentas. Quem decide quando o dado é inconclusivo? Qual margem conservadora se aplica? Que especialista precisa participar? Quanto tempo a operação pode permanecer sob condição provisória?

Quando tudo depende de uma reunião improvisada, o resultado costuma refletir quem possui mais poder, não quem possui melhor evidência.

Crerios prvrios no eliminam julgamento. Impedem que o julgamento comece sem limites.

CONDICAO	RESPOSTA PREDEFINIDA
Fora de especificacao	Bloquear atd demonstrar restauracao.
Barreira indisponivel	Parar ou aplicar contingencia formal equivalente.
Dado inconclusivo	Assumir condicao conservadora e investigar.
Mudanca no validada	No liberar atd concluir avaliacao proporcional ao risco.
Sinal recorrente	Escalonar alem da correcao local.
Emergencia	Proteger pessoas antes de preservar ativo ou producao.

O que a lideranca precisa dizer

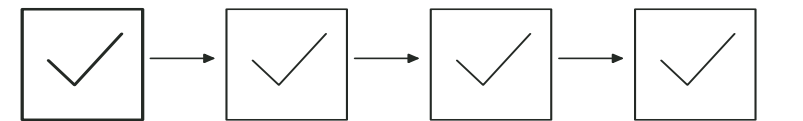
A autoridade do protocolo aparece na linguagem. “Faça o possivel para no parar” produz uma regra. “Pare quando perdermos a condicao e me chame” produz outra.

A lideranca deve declarar que uma parada tecnicamente correta no sera tratada como falha de compromisso. Deve pedir a verdade antes do plano de recuperacao e impedir que a urgencia do cliente recaia sobre quem controla a ultima barreira.

Depois, precisa agir de acordo. Defender a pessoa que interrompeu, investigar a causa da condicao e cobrar a restauracao do sistema. Caso contrario, a mensagem publica sera anulada pela experiencia privada.

A organizacao aprende quando ve que a regra continua valendo diante da perda real.

Como verificar uma barreira

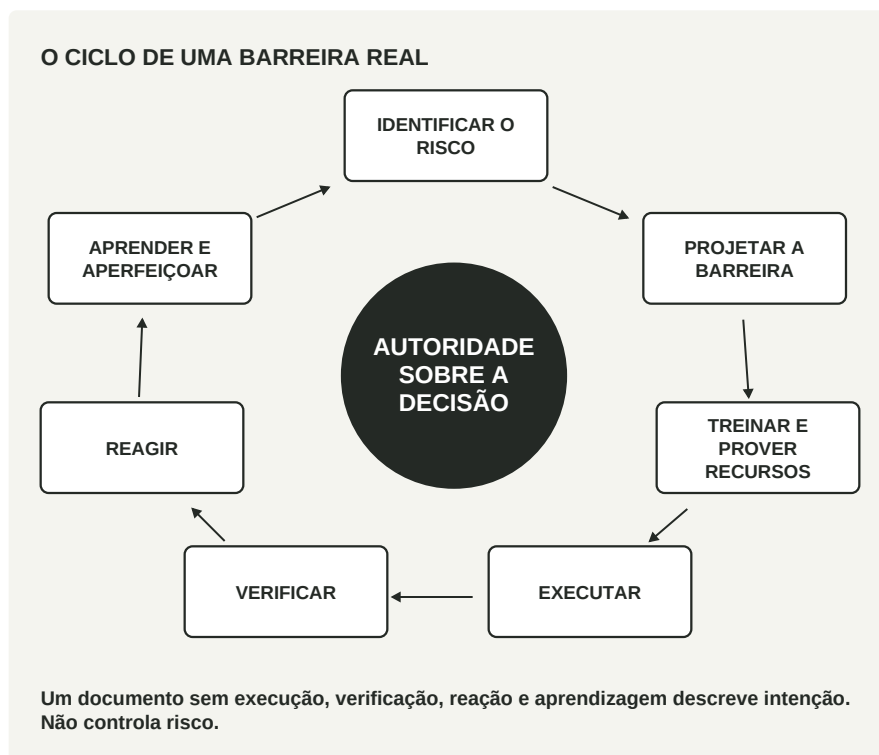


Uma proteção não deve ser avaliada pela intenção com que foi criada, mas pela evidência de que funciona.

A luz verde acendeu. O teste foi registrado. O equipamento voltou ao serviço. Horas depois, descobriu-se que o ensaio havia confirmado outra coisa. A condição usada no teste não representava aquela em que a barreira seria necessária.

Lac-Mégantic mostrou um trem imóvel durante uma configuração que mascarava a capacidade real dos freios. Therac-25 mostrou software confirmando a própria lógica. A verificação precisa ser capaz de contrariar o sistema que avalia.

Testar não é produzir um resultado favorável. É criar uma oportunidade honesta para a barreira falhar diante de nós.



Teste representativo

Uma barreira deve ser testada na condição em que precisa proteger. Pressão, temperatura, carga, velocidade, sequência de comandos, envelhecimento e falhas simultâneas podem alterar completamente a resposta.

Ensaio fáceis produzem confiança barata. A condição real exige perguntas incômodas: o instrumento mede aquilo que importa? A amostra representa o produto? A contingência funciona sem energia? O alarme chega quando a equipe está reduzida?

O teste também precisa definir antecipadamente o que constitui aprovação. Ajustar critérios depois de conhecer o resultado transforma validação em negociação.

Representatividade é o elo entre o laboratório e o mundo que a organização pretende controlar.

Independência, frequência e prova

Independência significa que a verificação não depende da mesma hipótese, do mesmo sensor ou do mesmo interesse que produziu a condição. Em riscos críticos, uma camada deve conseguir discordar da outra por princípio diferente.

Frequência significa acompanhar a velocidade de degradação. Um teste anual pode ser adequado para uma condição estável e inútil para um componente que mudou após manutenção, atualização ou incidente.

Prova significa registrar dados suficientes para reconstruir o que foi feito, por quem, em qual configuração e com qual resultado. Uma assinatura sem rastreabilidade demonstra apenas que alguém assinou.

Por fim, a verificação precisa produzir reação. Encontrar a falha e manter a decisão transforma o teste em testemunha, não em barreira.

DIMENSÃO	PERGUNTA DE VERIFICAÇÃO
Representatividade	O teste reproduz a condição relevante?
Independência	Pode detectar a falha da camada que verifica?
Frequência	A periodicidade acompanha a degradação?
Rastreabilidade	É possível reconstruir configuração e resultado?
Critério	A aprovação foi definida antes do resultado?
Reação	A falha modifica imediatamente a decisão?

QF32: quando uma falha não vira colapso

Uma barreira falhou. As demais impediram que a anomalia se transformasse em tragédia.

Em 4 de novembro de 2010, o Airbus A380 do voo Qantas 32 decolou de Singapura com 469 pessoas a bordo. Poucos minutos depois, o motor número 2 sofreu uma falha não contida. Fragmentos atingiram a asa e danificaram sistemas elétricos, hidráulicos e de combustível. A cabine recebeu uma quantidade extraordinária de alertas.

A falha existiu. Não foi imaginária, pequena ou plenamente prevista. A investigação do Australian Transport Safety Bureau identificou uma trinca por fadiga em um tubo de alimentação de óleo, associada a um problema de fabricação. Uma camada importante do sistema havia falhado antes da decolagem.

O que aconteceu depois, porém, diferencia uma anomalia grave de um colapso. A aeronave conservou capacidade de controle. A tripulação não tentou responder a todos os alarmes ao mesmo tempo. Ganhou tempo, organizou prioridades, trabalhou com listas, comunicou-se com o controle e preparou uma volta para Singapura sob condições degradadas.

O pouso exigiu uma velocidade superior ao normal e consumiu grande parte da pista. Depois da parada, um dos motores não respondeu ao comando de desligamento e houve vazamento de combustível. Ainda assim, passageiros e tripulantes deixaram a aeronave sem ferimentos.

QF32: QUANDO UMA FALHA NÃO ATRAVESSA TODAS AS BARREIRAS**1 FALHA DO MOTOR**

Uma barreira de fabricação falhou.

2 REDUNDÂNCIA

Sistemas remanescentes preservaram controle.

3 DISCIPLINA

A tripulação ganhou tempo e priorizou.

4 COMUNICAÇÃO

Cabine, controle e equipes coordenaram.

5 POUSO

469 pessoas saíram sem ferimentos.

A anomalia ocorreu. O colapso não. O caso demonstra que a tese não exige perfeição: exige camadas capazes de perceber, conter e reagir.

O contraponto necessário

O caso não contradiz a tese deste livro. Ele impede que ela se torne simplista. Nem toda falha física nasce de quebra deliberada, e nenhum sistema consegue prometer ausência absoluta de anomalias. O que se pode exigir é que uma falha não encontre todas as portas abertas.

No QF32, uma barreira de fabricação falhou. Outras camadas permaneceram capazes de perceber, absorver, coordenar e reagir. O protocolo não eliminou o evento inicial. Criou tempo e alternativas suficientes para que o evento não definisse sozinho o desfecho.

A prova de um sistema robusto não é nunca falhar. É impedir que uma falha isolada atravesse toda a organização.

Nota documental: ATSB, investigação AO-2010-089, relatório final de 27 jun. 2013. A ocorrência é de 4 nov. 2010. Ver ND-31, p. 151.

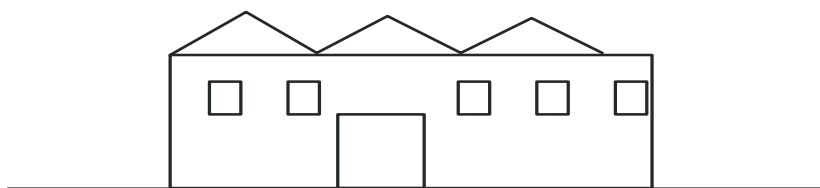
PARTE VI

O CAMINHO QUE AINDA EXISTE

*Toda quebra possui um momento anterior em que
outra decisão ainda era possível.*



A fábrica que ainda poderia ter sido salva



Voltemos ao portão.

Na história real, ele foi fechado depois de anos de perda de confiança, volume, competitividade e capacidade de reação. O último dia apenas tornou visível um processo que começara muito antes.

Mas uma investigação não serve apenas para explicar o caminho que aconteceu. Serve para localizar as saídas que permaneceram abertas e foram ultrapassadas.

Aquela fábrica não precisava conhecer o futuro. Precisava obedecer ao primeiro limite que já conhecia.

O dia em que a água mudou

Quando a condição da água ultrapassou a capacidade do tratamento, a organização ainda possuía uma escolha simples e cara: parar.

A parada revelaria fragilidade, ameaçaria a entrega e exigiria comunicação com o cliente. Também preservaria o produto, as evidências e a possibilidade de resolver o problema sem transformar uma condição temporária em crise de confiança.

O caminho alternativo começaria com uma frase: “não temos prova de que podemos produzir”. A partir dela, engenharia avaliaria a fonte, qualidade definiria critérios, operação preservaria equipamentos e liderança negociaria o impacto comercial.

Talvez o cliente se irritasse. Talvez o mês fosse perdido. A fábrica continuaria possuindo algo mais valioso que o volume: credibilidade para explicar o que acontecera.

A primeira reclamação

Mesmo depois da produção, ainda existia outra saída. A reclamação poderia ter sido registrada por inteiro, conectada ao período da alteração e tratada como sinal de sistema.

Registrar não significa admitir culpa antes da investigação. Significa impedir que a memória seja editada pela conveniência. Frequência, lote, data, condição de processo e amostra testemunha formariam uma história que poderia ser testada.

O cliente receberia uma resposta talvez incompleta, mas verdadeira: reconhecemos o sinal, bloqueamos a repetição e estamos preservando evidências.

A confiança não exige perfeição. Exige a certeza de que a falha não será escondida para proteger a aparência.

A amostra que precisava permanecer intacta

As amostras testemunhas existiam para permitir que o passado fosse examinado. Preservá-las seria proteger a própria organização contra conclusões precipitadas, inclusive contra acusações injustas.

Quando a evidência perde integridade, todas as partes perdem. O cliente deixa de confiar. A investigação deixa de aprender. Pessoas que poderiam esclarecer ficam expostas a narrativas impossíveis de verificar.

No caminho alternativo, a custódia das amostras seria independente. O acesso ficaria registrado. Resultados divergentes provocariam nova coleta, comparação com método de referência e comunicação transparente.

A verdade poderia ser desagradável. Ainda seria administrável.

A liderança que poderia mudar o método

Depois do primeiro episódio, novos treinamentos e documentos só teriam valor se a liderança alterasse aquilo que realmente selecionava comportamentos.

Quem registrasse problema precisaria receber proteção. Indicadores deveriam recuperar eventos omitidos. Auditorias não seriam preparadas como palco, mas usadas para encontrar a diferença entre o papel e a rotina.

Metas de volume seriam acompanhadas por margem, integridade de dados e recorrência. Uma parada correta deixaria de aparecer como fracasso do turno e passaria a revelar uma condição que a gestão precisava corrigir.

A mudança mais importante não seria anunciar tolerância zero. Seria mostrar, em decisões repetidas, que a verdade continuava valendo quando custava dinheiro.

O cliente que ainda poderia permanecer

Clientes estratégicos não comprem apenas especificação. Compram previsibilidade, reação e confiança na informação. Quando essas dimensões existem, um incidente pode fortalecer a relação porque demonstra capacidade de enfrentar a realidade.

A fábrica ainda poderia apresentar o problema, o bloqueio, a causa em investigação e as ações provisórias. Poderia convidar o cliente a verificar a evidência, estabelecer marcos e compartilhar o risco de retomada.

Talvez perdesse volume temporariamente. Mas a relação não precisaria terminar no momento em que a primeira falha apareceu.

O contrato foi perdido quando o cliente deixou de acreditar que receberia a verdade. Esse era o ativo que o protocolo deveria preservar.

O fechamento que não precisava acontecer

Não existe garantia de que o caminho alternativo salvaria a unidade para sempre. Mercados mudam, custos aumentam, tecnologias envelhecem e decisões corporativas podem encerrar operações competentes.

A tese é mais precisa. A condição da água não precisava transformar-se em perda de verdade. A reclamação não precisava destruir a memória. A investigação não precisava virar encenação. A perda do cliente não precisava resultar de um sistema incapaz de reconhecer a própria falha.

A fábrica fechou muito depois de ter quebrado. O que poderia ter sido salvo primeiro era a autoridade dos limites. Com ela, talvez viessem a confiança, o aprendizado e o tempo necessário para reconstruir competitividade.

Foi por isso que aquela história abriu este livro. Não porque seja maior que Chernobyl, Bhopal ou Brumadinho. Mas porque mostra que a mesma arquitetura pode começar numa decisão cotidiana, sem câmeras, sem sirenes e sem a certeza de que alguém um dia chamará aquilo de tragédia.

Antes da próxima quebra



Agora o leitor já conhece o mecanismo.

A peça, a chama, o microrganismo, o software, o combustível e a estrutura pertencem a histórias diferentes. A quebra anterior repete um gesto: um limite perde autoridade e a organização continua.

Às vezes, isso acontece por pressão. Em outras, por desenho inadequado, silêncio, fragmentação, confiança excessiva, fraude ou simples hábito. O resultado imediato quase sempre parece administrável.

Grandes colapsos não começam quando tudo sai do controle. Começam quando o sistema aceita que uma parte do controle pode ser suspensa.

Três perguntas antes de continuar

A complexidade dos casos não elimina três perguntas simples.

Primeira: qual risco está avançando? Não qual resultado estamos tentando proteger, mas qual condição pode produzir dano se continuar.

Segunda: que limite deveria interromper a sequência? Pode ser uma especificação, uma reserva, uma validação, um bloqueio, uma comunicação ou a decisão de não liberar.

Terceira: o que está retirando autoridade desse limite? Falta de recurso, meta, hierarquia, hábito, interesse, ausência de verificação ou uma regra que nunca representou a realidade.

Essas perguntas não substituem engenharia, investigação ou julgamento. Servem para impedir que a urgência comece pelo problema errado.

A primeira quebra quase nunca parece uma tragédia

Ela parece uma exceção. Um teste adiado. Uma reserva reduzida. Um alerta reclassificado. Uma inspeção que pode esperar. Um resultado que provavelmente está errado.

O perigo não está apenas na decisão isolada. Está no aprendizado que ela produz quando termina bem. A exceção vira precedente, o precedente vira prática e a prática reescreve o significado da regra.

Por isso, o momento mais importante não é aquele em que a consequência já exige coragem pública. É o momento discreto em que cumprir ainda custa apenas atraso, conflito ou dinheiro.

É ali que o futuro permanece barato.

Parar também é resultado

Durante muito tempo, gestão foi associada a fazer avançar: produzir, entregar, crescer, reduzir, acelerar. Os casos deste livro mostram uma competência igualmente decisiva: reconhecer quando avançar deixou de ser desempenho.

Parar uma linha, cancelar um lançamento, bloquear um lote, retirar um produto, abandonar uma rota ou admitir que a evidência não sustenta a promessa pode parecer perda. Em sistemas críticos, é a forma mais concreta de proteger pessoas, cliente e organização.

A liderança não será medida apenas pelo que conseguiu realizar. Também será medida pelas sequências que teve autoridade para interromper antes que recebessem um nome nas manchetes.

Esse é o ponto em que protocolo deixa de ser burocracia e se torna ética aplicada à decisão.

O último limite

Nenhum sistema elimina todos os erros. Pessoas se distraem, equipamentos envelhecem, modelos falham, dados chegam incompletos e situações novas escapam ao planejamento.

O objetivo do protocolo não é prometer perfeição. É criar tempo, evidência e barreiras suficientes para que uma falha não atravessasse sozinha toda a organização.

Quando a primeira proteção falhar, a segunda precisa percebê-la. Quando o alerta aparecer, alguém precisa ter autoridade para mudar o plano. Quando a evidência contrariar a expectativa, a verdade precisa sobreviver à pressão.

Esse é o compromisso real: não impedir que qualquer coisa quebre, mas impedir que a quebra anterior seja normalizada até que nada mais consiga conter a consequência.

A Q U E B R A

R X O

Agradecimentos

Este livro nasceu de décadas dentro de operações industriais, de conversas com profissionais que conhecem o peso de uma decisão e da lembrança de situações em que dizer a verdade custava mais do que permanecer em silêncio.

Agradeço às equipes de produção, qualidade, engenharia, manutenção, segurança, meio ambiente, logística e projetos com as quais trabalhei. Foram elas que me ensinaram que um processo não é controlado por um documento isolado, mas pela combinação entre conhecimento, disciplina, recursos e coragem para interromper.

Agradeço também aos profissionais que investigaram os acontecimentos públicos reconstruídos nestas páginas. Relatórios técnicos, depoimentos, decisões judiciais e registros regulatórios preservaram lições que poderiam desaparecer sob a força das imagens finais.

Por fim, agradeço a quem já sustentou uma decisão impopular porque sabia que continuar colocaria pessoas, clientes ou a própria organização em risco. Este livro é, sobretudo, uma defesa desse instante.

Notas documentais e referências

32 casos: um relato pessoal e 31 casos públicos.

As notas ND-01 a ND-31 preservam a numeração da revisão anterior. A ND-32 documenta o caso AdeS incorporado nesta edição, sem renumerar referências existentes. Todas identificam documentos, sua natureza e o recorte a que se referem. Os números de página junto aos casos remetem a esta edição; páginas e seções dentro das referências pertencem aos documentos citados.

Esta revisão acrescenta referências verificáveis aos casos públicos e explicita os limites do relato pessoal. Não presume que todas as obras aqui identificadas tenham sido consultadas na redação original. Quando a verificação foi bibliográfica ou o acesso integral ficou limitado, isso é indicado.

Relatórios de prevenção, estudos técnicos, inquéritos públicos, depoimentos, acusações, acordos e sentenças têm funções diferentes. As expressões “primeira quebra”, “veredito” e “se fosse cumprido”, usadas nos quadros do livro, pertencem à análise do autor. Não equivalem a conclusões judiciais nem demonstram que uma única medida garantiria o desfecho hipotético.

Fontes eletrônicas identificadas e verificadas no alcance indicado até 11 de outubro de 2026. Links levam ao documento ou ao repositório que o identifica. As remissões são clicáveis.

ND-01 | A Farsa

Prólogo | p. 9-11

Relato pessoal do autor, com identidades, locais e marcas omitidos e detalhes condensados. Não foi fornecido um conjunto documental público que permita verificar independentemente as alegações. As passagens sobre manipulação de evidências pertencem ao testemunho do autor; não constituem conclusão de investigação oficial.

Natureza da fonte: testemunho pessoal anonimizado. A ausência de documentação pública é explicitada, sem preencher a lacuna com referências de outros casos.

ND-02 | Ayrton Senna

Capítulo 1 | p. 17-20

A atribuição à falha da coluna de direção segue a reconstrução técnica que reproduz a trajetória judicial italiana. As hipóteses sobre a sequência da ruptura devem ser distinguidas da conclusão judicial relatada. O texto da FIA documenta a evolução da segurança após Imola, sem funcionar como laudo causal do acidente de Senna.

MURGIA, Michele. *Ayrton Senna: storia controversa di un incidente*. Rivista Italiana della Saldatura, v. 66, n. 4, p. 545-558, jul./ago. 2014. Cópia disponibilizada pelo autor. https://www.researchgate.net/publication/297275409_Ayrton_Senna_The_controversial_history_of_an_incident

FÉDÉRATION INTERNATIONALE DE L'AUTOMOBILE (FIA). *Legacy of Safety - How the FIA responded to the tragedy of Imola 1994 and launched a drive for safer racing*. 15 maio 2024.

<https://www.fia.com/news/legacy-safety-how-fia-responded-tragedy-imola-1994-and-launched-drive-safer-racing>

Localização: Murgia, p. 545-558; FIA, histórico das mudanças de segurança. A decisão italiana é referida por intermédio de Murgia; não se declara consulta direta ao inteiro teor judicial.

ND-03 | Chapecoense / LaMia 2933

Capítulo 2 | p. 21-23

O caso corresponde ao voo LaMia 2933, operado pelo AVRO 146-RJ85 de matrícula CP2933. Matrícula e número do voo não são intercambiáveis. O acidente ocorreu em 28 de novembro de 2016 no horário local; o relatório o identifica em 29 de novembro, pela referência UTC.

COLOMBIA. AERONÁUTICA CIVIL. Grupo de Investigación de Accidentes. *Informe final de accidente COL-16-37-GIA: agotamiento de combustible, AVRO 146-RJ85, matrícula CP2933, La Unión, Antioquia, 29 de noviembre de 2016*. 2018.

https://www.aerocivil.gov.co/info/aeronautica_civil/media/1740581430_COL-16-37-GIA%20Final%20Acc%20CP2933%20La%20Unión%20nº2029-nov-16%2028Espana%20B1ol%29.pdf

Documento de referência: relatório final COL-16-37-GIA. Planejamento, combustível e decisões operacionais devem ser lidos no conjunto da investigação, sem reduzir o acidente a um único ato.

ND-04 | Challenger

Capítulo 4 | p. 27-30

O relatório da Comissão Rogers documenta a falha na junta do foguete auxiliar e o processo de decisão de lançamento. A leitura sobre normalização do desvio é uma interpretação organizacional, relacionada à literatura indicada em FG-02, e não uma expressão a ser atribuída indistintamente ao relatório oficial.

UNITED STATES. Presidential Commission on the Space Shuttle Challenger Accident. *Report of the Presidential Commission on the Space Shuttle Challenger Accident*. v. I. Washington, DC, 6 jun. 1986. Acervo NASA.

<https://www.nasa.gov/history/rogersrep/genindex.htm>

Localização: v. I, capítulos IV (causa), V (decisão de lançamento), VI (antecedentes), VII (programa de segurança) e VIII (pressões sobre o sistema).

ND-05 | Chernobyl

Capítulo 5 | p. 31-34

O INSAG-7 revê explicações anteriores e trata conjuntamente de projeto, informação aos operadores, regulamentação e cultura de segurança. O acionamento do AZ-5 não deve ser narrado como reação comprovada a uma subida prévia de potência: o anexo I registra a impossibilidade de estabelecer por que o botão foi pressionado.

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA). *The Chernobyl Accident: Updating of INSAG-1*. Safety Series n. 75-INSAG-7. Viena: IAEA, 1992. ISBN 92-0-104692-8.

https://www-pub.iaea.org/MTcd/publications/PDF/Pub913e_web.pdf

Localização: seções 5 e 6; anexo I, seção I-4.6.3, p. 66 da numeração impressa, sobre o acionamento da proteção. As páginas do arquivo eletrônico incluem folhas preliminares.

ND-06 | Bhopal

Capítulo 6 | p. 37-40

A reconstrução técnica descreve a interação entre equipamentos, refrigeração e barreiras de proteção. A rota exata de ingresso da água permanece objeto de controvérsia. A análise da perda de defesas não estabelece autoria individual nem resolve, por si, hipóteses concorrentes sobre a introdução da água.

BLOCH, Kenneth; JUNG, Briana. *Understanding the impact of unreliable machinery*. Loss Prevention Bulletin, n. 240, p. 13-16, dez. 2014. Rugby: Institution of Chemical Engineers (IChemE).

https://www.icheme.org/media/1277/lpb240_digimag.pdf

Localização: p. 13-16 da revista, edição dedicada aos 30 anos de Bhopal. Trata-se de análise técnica retrospectiva, não de decisão judicial nem de um relatório oficial único e consensual.

ND-07 | Therac-25

Capítulo 7 | p. 41-43

O estudo reconstrói seis acidentes e examina software, intertravamentos, comunicação e respostas do fabricante e de autoridades. As ocorrências não tiveram uma sequência idêntica. A narrativa do capítulo concentra-se em falhas de proteção e na dificuldade de reconhecer a sobredose.

LEVESON, Nancy G.; TURNER, Clark S. *An Investigation of the Therac-25 Accidents*. Computer, v. 26, n. 7, p. 18-41, jul. 1993. Cópia acadêmica hospedada pela Columbia University.

<https://www.cs.columbia.edu/~junfeng/08fa-e6998/sched/readings/therac25.pdf>

Localização: p. 18-41, especialmente a cronologia das ocorrências e a análise das falhas. Registros regulatórios reproduzidos no artigo são aqui acessados por intermédio dos autores.

ND-08 | Angrois

Interlúdio: última barreira | p. 44

O caso exige preservar a diferença entre a distração do maquinista e a investigação das defesas do sistema. A agência ferroviária europeia criticou o alcance e a independência da investigação espanhola. A contagem de 80 mortes no capítulo corresponde à documentação técnica e parlamentar aqui indicada.

EUROPEAN RAILWAY AGENCY. *Advice ERA/ADV/2015-6*, sobre a investigação do acidente de Santiago de Compostela. Documento divulgado em 2016. Reprodução do documento da agência.

<https://ep00.epimg.net/descargables/2016/07/07/ee44185e5915a7e767d688ca645a4313.pdf>

ESPAÑA. CONGRESO DE LOS DIPUTADOS. *Diario de Sesiones: Comisiones de Investigación*. XII Legislatura, n. 90, 3 out. 2018. Comparecimento de Eduardo del Río Martínez, da Agência Ferroviária da União Europeia.

https://www.congreso.es/public_oficiales/L12/CONG/DS/CI/DSCD-12-CI-90.PDF

Localização: parecer ERA/ADV/2015-6; depoimento parlamentar iniciado na p. 2. Parecer técnico e depoimento não devem ser apresentados como sentença penal definitiva.

ND-09 | Piper Alpha

Interlúdio: última barreira | p. 44-45

O inquérito Cullen considerou mais provável uma sequência envolvendo a bomba de condensado e a válvula de segurança removida. Essa reconstrução tem natureza probabilística. A dimensão da catástrofe envolve também isolamento, resposta ao incêndio e interligações entre plataformas.

CULLEN, William Douglas, Lord. *The Public Inquiry into the Piper Alpha Disaster*. Londres: HMSO, 1990. Cm 1310, v. 1. Reprodução pelo Health and Safety Executive.

<https://www.hse.gov.uk/offshore/assets/docs/piper-alpha-public-inquiry-volume1.pdf>

CULLEN, William Douglas, Lord. *The Public Inquiry into the Piper Alpha Disaster*. Londres: HMSO, 1990. Cm 1310, v. 2.

<https://www.hse.gov.uk/offshore/assets/docs/piper-alpha-public-inquiry-volume2.pdf>

Localização: v. 1, reconstrução do desastre e sistema de permissão de trabalho; v. 2, segurança e recomendações. O capítulo apresenta a hipótese técnica mais provável, não uma sequência integralmente observada.

ND-10 | Lac-Mégantic

Interlúdio: última barreira | p. 45

O relatório diferencia a retenção por freios manuais da contribuição temporária dos freios pneumáticos. O teste feito na configuração inadequada não demonstrou que os freios manuais, isoladamente, sustentariam a composição. A investigação identifica uma combinação de falhas operacionais e organizacionais.

TRANSPORTATION SAFETY BOARD OF CANADA (TSB). *Railway Investigation Report R13D0054: runaway and main-track derailment, Montreal, Maine & Atlantic Railway, Lac-Mégantic, Quebec, 6 July 2013*. Relatório divulgado em 19 ago. 2014. <https://www.tsb.gc.ca/eng/rapports-reports/rail/2013/r13d0054/r13d0054.html>

Localização: relatório R13D0054, análise da imobilização do trem e conclusões sobre causas e fatores contribuintes. A contagem de 47 mortes é a da investigação.

ND-11 | Brumadinho

Capítulo 8 | p. 47-50

O painel técnico foi contratado por assessoria jurídica externa da Vale e examinou o mecanismo físico da ruptura. A CPI da ALMG tem finalidade parlamentar e escopo distinto. Nenhum desses documentos deve ser confundido com julgamento individual. A contagem memorial de 272 vidas inclui dois nascituros.

ROBERTSON, Peter K.; DE MELO, Lucas; WILLIAMS, David J.; WILSON, G. Ward. *Report of the Expert Panel on the Technical Causes of the Failure of Feijão Dam I*. 12 dez. 2019. Cópia no acervo DamFailures, da Association of State Dam Safety Officials. https://damfailures.org/sites/default/files/wp-pdf/IR_Feijao-Dam.pdf

MINAS GERAIS. ASSEMBLEIA LEGISLATIVA. *CPI da Barragem de Brumadinho: relatório final*. Belo Horizonte, 2019. Aprovado em 12 set. 2019. <https://mediaserver.almg.gov.br/acervo/439/372/1439372.pdf>

MINAS GERAIS. Agência Minas. *Governo de Minas inaugura monumento na Cidade Administrativa em homenagem às 272 joias de Brumadinho*. 23 out. 2024. <https://www.agenciaminas.mg.gov.br/noticia/governo-de-minas-inaugura-monumento-na-cidade-administrativa-em-homenagem-as-272-joias-de-brumadinho>

Localização: painel, resumo executivo e seção 1.1 (termos da investigação); relatório parlamentar; comunicado estadual para a convenção de contagem das vítimas.

ND-12 | Boeing 737 MAX

Capítulo 9 | p. 51-53

Os acidentes JT610 e ET302 têm relatórios próprios. A análise do MCAS, das premissas de resposta dos pilotos e da certificação não autoriza tratar as duas sequências como idênticas. O NTSB registrou divergências em relação ao relatório etíope; essa ressalva integra a documentação.

INDONESIA. KOMITE NASIONAL KESELAMATAN TRANSPORTASI (KNKT). *Final Aircraft Accident Investigation Report: PT Lion Mentari Airlines, Boeing 737-8 (MAX), PK-LQP, 29 October 2018*. KNKT.18.10.35.04. 2019.

<https://knkt.go.id/Repo/Files/Laporan/Penerbangan/2018/KNKT.18.10.33.04-Final-Report.pdf>

ETHIOPIAN AIRCRAFT ACCIDENT INVESTIGATION BUREAU (EAIB). *Aircraft Accident Investigation Report: Boeing 737 MAX 8, ET-AVJ, Ethiopian Airlines Flight 302, 10 March 2019*. Relatório final, dez. 2022. Cópia no BEA.

https://bea.aero/fileadmin/user_upload/ET_302__B737-8MAX_ACCIDENT_FINAL_REPORT.pdf

NATIONAL TRANSPORTATION SAFETY BOARD (NTSB). *Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance*. NTSB/ASR-19/01. 19 set. 2019.

<https://data.nts.gov/investigations/AccidentReports/Reports/ASR1901.pdf>

UNITED STATES. HOUSE OF REPRESENTATIVES. Committee on Transportation and Infrastructure. *The Design, Development & Certification of the Boeing 737 MAX: Final Committee Report*. set. 2020.

https://www.govinfo.gov/content/pkg/GOVPUB-Y4_T68_2-PURL-gpo144993/pdf/GOVPUB-Y4_T68_2-PURL-gpo144993.pdf

NTSB. *NTSB Releases Comments on Ethiopia's Investigation of the Boeing 737 MAX Accident*. Comunicado e comentários sobre o relatório ET302, 27 dez. 2022.

<https://www.nts.gov/news/press-releases/Pages/NR20221227.aspx>

Localização: relatórios finais de cada voo; recomendações do ASR-19/01; relatório parlamentar sobre desenvolvimento e certificação; comentários do NTSB sobre ET302. A investigação técnica tem finalidade distinta da apuração judicial.

ND-13 | Voepass, voo 2283

Capítulo 10 | p. 55-57

O documento indicado na versão recebida é o relatório final A-116/CENIPA/2024. A publicação em 23 de julho de 2026 foi confirmada no comunicado da FAB, e a ocorrência consta do repositório CENIPA. O relatório tem finalidade preventiva; a leitura sobre perda de autoridade das barreiras é interpretação editorial.

BRASIL. CENTRO DE INVESTIGAÇÃO E PREVENÇÃO DE ACIDENTES AERONÁUTICOS (CENIPA). *Relatório final A-116/CENIPA/2024*. Aeronave ATR 72-212A, matrícula PS-VPB, ocorrência de 9 ago. 2024, Vinhedo, SP. Emitido em 23 jul. 2026.

https://sistema.cenipa.fab.mil.br/cenipa/paginas/relatorios/rf/pt/RF_PS-VPB_09AGO2024_PORT.PUB..pdf

BRASIL. FORÇA AÉREA BRASILEIRA. *FAB divulga relatório final do acidente da aeronave de matrícula PS-VPB*. 23 jul. 2026.

<https://www.fab.mil.br/noticia/aviacao/20111/2026/07/fab-divulga-relatorio-final-do-acidente-da-aeronave-de-matricula-ps-vpb/>

Limite desta revisão: o acesso ao arquivo integral não ficou disponível para cotejo. Mantém-se a síntese do autor, com identificação bibliográfica conferida; não se atribuem páginas ou excertos não verificados. O cotejo integral permanece indicado para o fechamento editorial.

ND-14 | Takata

Interlúdio: desvio ao público | p. 58

O recorte é o dos infladores com nitrato de amônio estabilizado sem dessecante, cuja degradação foi associada a tempo, calor e umidade. Não se generaliza esse mecanismo a todo airbag ou a todo produto Takata. Quantidades e situação de recalls variam ao longo do tempo.

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION (NHTSA). *Takata Recall Expansion: What Consumers Need to Know*. Página institucional, sem data editorial indicada.

<https://www.nhtsa.gov/takata-air-bags/takata-recall-expansion-what-consumers-need-know>

Localização: seção Summary, sobre a expansão de maio de 2016 e a degradação do propelente. Consulta em 10 out. 2026; a página é sujeita a atualização.

ND-15 | Blue Bell Creameries

Interlúdio: desvio ao público | p. 58-59

A contagem final do CDC reúne dez pessoas doentes e três mortes no Kansas. A investigação de 2015 identificou retrospectivamente ocorrências entre 2010 e janeiro de 2015. Assim, a data do reconhecimento do surto não corresponde à data de todos os adoecimentos.

CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC). *Multistate Outbreak of Listeriosis Linked to Blue Bell Creameries Products (Final Update)*. 9 jun. 2015. Página arquivada.

https://archive.cdc.gov/www_cdc_gov/listeria/outbreaks/ice-cream-03-15/index.html

Localização: resumo final, cronologia da investigação e atualizações de recall; a página também remete às inspeções da FDA. As medidas de bloqueio e verificação propostas no livro são a leitura preventiva do autor.

ND-16 | Flint

Interlúdio: desvio ao público | p. 59

A força-tarefa estadual examinou a mudança de abastecimento, o controle de corrosão, a amostragem e a resposta institucional. Os achados sobre falhas de gestão e proteção sanitária não equivalem, por si, a decisões sobre responsabilidade penal de pessoas determinadas.

FLINT WATER ADVISORY TASK FORCE. *Final Report*. Michigan, mar. 2016. Documento datado de 21 mar. 2016 no repositório estadual.

https://www.michigan.gov/flintwater/-/media/Project/Websites/formergovernors/Folder6/FWATF_FINAL_REPORT_21March2016.pdf

Localização: Executive Summary; Findings and Recommendations; análise dos papéis das entidades governamentais. O recorte do capítulo é o período de 2014 a 2016.

ND-17 | Dieselgate

Capítulo 11 | p. 63-66

A notificação ambiental de 2015 e os desdobramentos criminais posteriores pertencem a etapas diferentes. O recorte de aproximadamente 590 mil veículos diz respeito aos Estados Unidos, e não ao universo mundial de veículos envolvidos no caso.

UNITED STATES. ENVIRONMENTAL PROTECTION AGENCY (EPA). *EPA, California Notify Volkswagen of Clean Air Act Violations*. Comunicado relativo à Notice of Violation de 18 set. 2015.

<https://www.epa.gov/archive/epa/newsreleases/epa-california-notify-volkswagen-clean-air-act-violations-carmaker-allegedly-used.html>

UNITED STATES. DEPARTMENT OF JUSTICE (DOJ). *Volkswagen AG Agrees to Plead Guilty and Pay \$4.3 Billion in Criminal and Civil Penalties; Six Volkswagen Executives and Employees are Indicted*. 11 jan. 2017.

<https://www.justice.gov/archives/opa/pr/volkswagen-ag-agrees-plead-guilty-and-pay-43-billion-criminal-and-civil-penalties-six>

Localização: descrição do dispositivo de manipulação na comunicação da EPA e exposição do esquema no comunicado do DOJ. O anúncio de acordo não deve ser confundido com a data de homologação ou de sentença.

ND-18 | Deepwater Horizon

Capítulo 12 | p. 67-69

As fontes permitem acompanhar barreira de cimento, teste de pressão negativa e defesas subsequentes. O relatório da BP é uma investigação empresarial e deve ser identificado como tal. As conclusões da comissão presidencial e do CSB têm autoria e escopo próprios.

NATIONAL COMMISSION ON THE BP DEEPWATER HORIZON OIL SPILL AND OFFSHORE DRILLING. *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling. Report to the President*. Washington, DC, jan. 2011.

<https://www.govinfo.gov/app/details/GPO-OILCOMMISSION/>

UNITED STATES. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD (CSB). *Macondo Investigation Report*. v. 1, 5 jun. 2014.

https://www.csb.gov/assets/1/7/vol_1_final.pdf

BP. *Deepwater Horizon Accident Investigation Report*. 8 set. 2010. Relatório corporativo, reprodução em documento apresentado à SEC.

<https://www.sec.gov/Archives/edgar/data/313807/000119312510216268/dex993.htm>

Localização: reconstrução do acidente e decisões sobre o poço na comissão presidencial; sequência técnica no v. 1 do CSB; análise interna da BP. A comparação entre fontes evita atribuir a uma só organização toda a reconstrução.

ND-19 | Wells Fargo

Interlúdio: aparência | p. 70

O comunicado do DOJ registra o acordo de 2020 e as admissões relacionadas às práticas comerciais entre 2002 e 2016. O instrumento inclui diferimento da persecução penal; não é uma sentença produzida por julgamento de todas as condutas individuais.

UNITED STATES. DEPARTMENT OF JUSTICE. *Wells Fargo Agrees to Pay \$3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts without Customer Authorization*. 21 fev. 2020.

<https://www.justice.gov/archives/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices>

Localização: histórico das práticas de vendas, admissões da instituição e descrição do acordo no comunicado oficial.

ND-20 | Rana Plaza

Interlúdio: aparência | p. 70-71

A OIT documenta a dimensão humana do colapso e as medidas posteriores no setor de vestuário. A pesquisa de campo da Human Rights Watch reúne depoimentos sobre condições de trabalho, pressões e segurança. Depoimentos e investigação social não substituem uma perícia estrutural nem uma sentença.

INTERNATIONAL LABOUR ORGANIZATION (ILO/OIT). *Rana Plaza: Plus jamais ça!* 23 abr. 2014. Publicação institucional sobre o primeiro aniversário do colapso.

<https://www.ilo.org/fr/resource/rana-plaza-plus-jamais-ca>

HUMAN RIGHTS WATCH. “*Whoever Raises Their Head Suffers the Most*”: *Workers’ Rights in Bangladesh’s Garment Factories*. 22 abr. 2015. Relatório de pesquisa e entrevistas.

<https://www.hrw.org/report/2015/04/22/whoever-raises-their-head-suffers-most/workers-rights-bangladesh-shs-garment>

Localização: balanço da OIT; relato do colapso e depoimentos no relatório da HRW. O capítulo usa valores aproximados para vítimas e feridos, sem apresentar uma falsa precisão uniforme entre fontes.

ND-21 | Imperial Sugar

Interlúdio: aparência | p. 71

O CSB identificou a sequência de explosão primária e explosões secundárias, associada ao confinamento e ao acúmulo de poeira combustível. A fonte de ignição foi tratada em termos de probabilidade; não se converte essa hipótese em fato diretamente observado.

UNITED STATES. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD (CSB). *Investigation Report: Sugar Dust Explosion and Fire, Imperial Sugar Company, Port Wentworth, Georgia, February 7, 2008*. n. 2008-05-I-GA, set. 2009.

<https://www.csb.gov/userfiles/file/imperial%20sugar%20report%20final%20-%20to%20post.pdf>

Localização: descrição e análise da explosão; seções 8 (Key Findings), 9 (Root and Contributing Causes) e 10 (Recommendations).

ND-22 | Grenfell Tower

Capítulo 13 | p. 73-76

A Fase 1 examina a noite do incêndio; a Fase 2 trata das causas e das falhas que levaram à tragédia. O inquérito público identifica responsabilidades institucionais e faz recomendações; suas conclusões não devem ser apresentadas como condenações criminais.

GRENFELL TOWER INQUIRY. *Phase 1 Report: Executive Summary*. Londres, 30 out. 2019. Relatório da investigação pública presidida por Sir Martin Moore-Bick.

https://assets.publishing.service.gov.uk/media/66d82294a399e0dcf5200b2f/Grenfell_Tower_Inquiry_-_Phase_1_report_Executive_Summary.pdf

GRENFELL TOWER INQUIRY. *Phase 2 Report*. Londres: HMSO, 4 set. 2024. 7 volumes. HC 19. Portal oficial com o conjunto do relatório e os volumes da Fase 1.

<https://www.gov.uk/government/publications/publication-of-the-grenfell-tower-inquiry-phase-2-report>

Localização: resumo executivo da Fase 1; Fase 2, v. 1, capítulo 2 (resumo executivo), e volumes temáticos. A explicação envolve materiais, ensaios, certificação, projeto, regulação e resposta institucional.

ND-23 | Peanut Corporation of America

Capítulo 14 | p. 77-80

As referências abaixo são comunicados oficiais sobre o veredito e as sentenças, não o conjunto integral dos autos. Eles identificam condenações por condutas relacionadas a produtos contaminados, fraude e obstrução, com imputações distintas para cada pessoa.

UNITED STATES. DEPARTMENT OF JUSTICE. *Peanut Corporation of America Former Officials and Broker Convicted on Criminal Charges Related to Salmonella-Tainted Peanut Products*. 19 set. 2014.

<https://www.justice.gov/archives/opa/pr/peanut-corporation-america-former-officials-and-broker-convicted-criminal-charges-related>

UNITED STATES. DEPARTMENT OF JUSTICE. *Former Peanut Company President Receives Largest Criminal Sentence in Food Safety Case; Two Others also Sentenced*. 21 set. 2015.

<https://www.justice.gov/archives/opa/pr/former-peanut-company-president-receives-largest-criminal-sentence-food-safety-case-two>

Localização: descrição das provas, das condenações e das penas nos dois comunicados. A leitura sobre liberação de lotes deve ser associada às condutas efetivamente descritas, sem uniformizar todos os réus.

ND-24 | OceanGate Titan

Capítulo 15 | p. 81-84

A investigação marítima de 2025 trata de projeto, operação, fiscalização e cultura organizacional. A análise preventiva e as recomendações da Marine Board of Investigation não equivalem a sentença judicial. A ideia de que a prova independente foi afastada é a síntese editorial do capítulo.

UNITED STATES COAST GUARD (USCG). Marine Board of Investigation. *Marine Board's Report into the Implosion of the Submersible TITAN (CG1788361) in the North Atlantic Ocean near the Wreck Site of the RMS TITANIC, Resulting in the Loss of Five Lives on June 18, 2023*. Relatório de 4 ago. 2025, divulgado em 5 ago. 2025.

https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/MBOIs/TITAN_7724663_MBI_R_Redacted.pdf

USCG. *Coast Guard Marine Board of Investigation releases report on Titan submersible*. 5 ago. 2025. Comunicado oficial de divulgação.

<https://content.govdelivery.com/accounts/USDHSCG/bulletins/3ec8a2d>

Documento: relatório MBI sobre a ocorrência de 18 jun. 2023. A data do relatório e a da ocorrência devem permanecer distintas; a natureza do documento é investigativa.

ND-25 | Costa Concordia

Capítulo 16 | p. 85-87

A investigação de segurança marítima distingue a navegação que levou ao contato com o fundo das dificuldades de comunicação, gestão da emergência e evacuação. A síntese não deve reduzir todas as perdas a um único momento da manobra.

ITALY. MINISTRY OF INFRASTRUCTURES AND TRANSPORTS. Marine Casualties Investigative Body. *Cruise Ship Costa Concordia: Marine casualty on January 13, 2012. Report on the safety technical investigation*. 2013. Cópia do relatório adotado no acervo do NTSB.

[https://data.ntsb.gov/Docket/Document/docBLOB?FileExtension=.PDF&FileName=Foreign+Governme
nt+-+Adopted+Report-Master.PDF&ID=40439860](https://data.ntsb.gov/Docket/Document/docBLOB?FileExtension=.PDF&FileName=Foreign+Government+-+Adopted+Report-Master.PDF&ID=40439860)

Documento de referência: relatório italiano da investigação técnica de segurança. Autoria italiana; a hospedagem pelo NTSB não transforma o documento em relatório norte-americano.

ND-26 | ValuJet 592

Capítulo 17 | p. 89-91

O NTSB examinou a preparação e o transporte de geradores químicos de oxigênio, a manutenção contratada, a supervisão e a proteção do compartimento de carga. A causalidade é distribuída entre ações e deficiências de defesa, conforme a formulação do relatório.

NATIONAL TRANSPORTATION SAFETY BOARD. *In-Flight Fire and Impact With Terrain, ValuJet Airlines Flight 592, DC-9-32, N904VJ, Everglades, Near Miami, Florida, May 11, 1996*. NTSB/AAR-97/06; PB97-910406. Adotado em 19 ago. 1997. <https://ntsb.gov/investigations/AccidentReports/Reports/AAR9706.pdf>

Localização: Executive Summary; análise dos geradores e da supervisão; seção 3 (Conclusions), especialmente Probable Cause.

ND-27 | General Motors

Capítulo 18 | p. 93-96

O comunicado oficial de 2015 descreve o defeito do interruptor de ignição, o histórico de conhecimento e a comunicação tardia do problema. O caso foi objeto de acordo de diferimento da persecução penal, acompanhado de admissões, e não de julgamento criminal de todos os envolvidos.

UNITED STATES. DEPARTMENT OF JUSTICE. U.S. Attorney's Office, Southern District of New York. *Manhattan U.S. Attorney Announces Criminal Charges Against General Motors and Deferred Prosecution Agreement with \$900 Million Forfeiture*. 17 set. 2015.

<https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-general-motors-and-deferred>

Localização: histórico de conhecimento do defeito, vínculo com o não acionamento dos airbags e seção sobre a demora na comunicação e no recall. A referência é o comunicado oficial, que descreve o acordo.

ND-28 | Samsung Galaxy Note7

Interlúdio: verdades adiadas | p. 97

Os dois avisos da CPSC documentam o recall inicial e sua ampliação para incluir aparelhos de substituição. A conclusão sobre insuficiência da validação da primeira resposta é interpretação editorial a partir dessa sequência; os avisos de recall não constituem, por si, uma perícia completa das baterias.

UNITED STATES. CONSUMER PRODUCT SAFETY COMMISSION (CPSC). *Samsung Recalls Galaxy Note7 Smartphones Due to Serious Fire and Burn Hazards*. 15 set. 2016.

<https://www.cpsc.gov/Recalls/2016/Samsung-Recalls-Galaxy-Note7-Smartphones>

CPSC. *Samsung Expands Recall of Galaxy Note7 Smartphones Based on Additional Incidents with Replacement Phones; Serious Fire and Burn Hazards*. 13 out. 2016.

<https://www.cpsc.gov/Recalls/2017/Samsung-Expands-Recall-of-Galaxy-Note7-Smartphones-Based-on-Additional-Incidents-with-Replacement-Phones>

Localização: Recall Details de cada aviso. O caminho eletrônico da segunda página contém “2017”, mas a data de publicação do recall é 13 out. 2016.

ND-29 | Equifax

Interlúdio: verdades adiadas | p. 97-98

O relatório parlamentar examina a falha de correção do Apache Struts, a atribuição de responsáveis, os controles e a detecção. A contagem aproximada de 148 milhões e a qualificação da ocorrência como evitável são apresentadas no recorte histórico desse documento.

UNITED STATES. HOUSE OF REPRESENTATIVES. Committee on Oversight and Government Reform. *The Equifax Data Breach*. Majority Staff Report, 115th Congress, dez. 2018.

<https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>

Localização: Executive Summary, p. 2; discussão da política de correção de vulnerabilidades críticas em 48 horas, p. 64-65, na numeração impressa do relatório.

ND-30 | Theranos

Interlúdio: verdades adiadas | p. 98

O protocolo nulo aparece como alegação na acusação, e não como um veredito autônomo sobre cada demonstração. Elizabeth Holmes foi condenada por quatro acusações relativas a investidores; foi absolvida das relativas a pacientes julgadas contra ela, e houve acusações sem consenso do júri. Ramesh Balwani foi condenado por doze acusações, envolvendo investidores e pacientes. Os resultados não são intercambiáveis.

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA. *United States v. Elizabeth A. Holmes et al.: Third Superseding Indictment*. Processo 5:18-cr-00258-EJD, documento 469, protocolado em 28 jul. 2020.

<https://cand.uscourts.gov/sites/default/files/wp-content/uploads/cases-of-interest/usa-v-holmes-et-al/USA-v.-Holmes-18-CR-00258-Dkt-469-Third-Sup-Indictment.pdf>

UNITED STATES. DEPARTMENT OF JUSTICE. *Theranos Founder Elizabeth Holmes Found Guilty of Investor Fraud*. 3 jan. 2022.

<https://www.justice.gov/usao-ndca/pr/theranos-founder-elizabeth-holmes-found-guilty-investor-fraud>

UNITED STATES. DEPARTMENT OF JUSTICE. *Theranos Chief Operating Officer Ramesh “Sunny” Balwani Found Guilty of Conspiracy, Wire Fraud*. 7 jul. 2022.

<https://www.justice.gov/usao-ndca/pr/theranos-chief-operating-officer-ramesh-sunny-balwani-found-guilty-conspiracy-wire>

Localização: acusação de 2020 para a descrição das demonstrações; comunicados dos dois vereditos para os resultados. A acusação é documento processual, mas suas alegações não se tornam fatos provados pela simples existência de condenações.

ND-31 | Qantas 32*Interlúdio: QF32 | p. 122-123*

A investigação identificou uma falha de fabricação em tubulação de óleo do motor e a sequência de falha não contida. O retorno seguro a Singapura sustenta a discussão sobre resposta a falhas e defesas remanescentes. Essa leitura sistêmica é distinta da identificação técnica do defeito inicial.

AUSTRALIAN TRANSPORT SAFETY BUREAU (ATSB). *In-flight uncontained engine failure, Airbus A380-842, VH-OQA, overhead Batam Island, Indonesia, on 4 November 2010*. Investigation AO-2010-089. Relatório final divulgado em 27 jun. 2013.

<https://www.atsb.gov.au/investigations/ao-2010-089>

Localização: Final report; What happened; What the ATSB found; Safety message. A data de 4 nov. 2010 é a do evento, e 27 jun. 2013 é a da publicação do relatório final.

ND-32 | AdeS*Caso AdeS | p. 81-84*

A Anvisa documentou a suspensão preventiva da linha TBA3G em 18 de março de 2013 e, em 8 de abril, informou que a inspeção sanitária delimitara a falha ao AdeS maçã de 1,5 litro, lote AGB25. A Câmara registrou 96 embalagens e recall por risco de queimaduras. A inspeção reproduzida pela imprensa descreveu a reativação do envase durante a limpeza, hidróxido de sódio a 2,5%, ausência de detecção antes do mercado e medidas corretivas. A duração aproximada de 80 segundos e a combinação entre falha humana e mecânica são declarações públicas da Unilever. A leitura sobre intertravamento e “primeira quebra” é interpretação editorial.

BRASIL. AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). Anvisa suspende alimentos de soja da marca AdeS. 18 mar. 2013.

ANVISA. Alimentos de soja da marca AdeS são liberados. 8 abr. 2013.

BRASIL. CÂMARA DOS DEPUTADOS. Saiba mais sobre a contaminação do suco AdeS. 27 mar. 2013.

www.camara.leg.br/noticias/399484-saiba-mais-sobre-a-contaminacao-do-suco-ades/

FOLHA DE S.PAULO. Vistoria confirma contaminação de lote de AdeS com soda cáustica. 22 mar. 2013.

www1.folha.uol.com.br/.../1251083-vistoria-confirma-contaminacao-de-lote-de-ades-com-soda-caustica.shtml

FOLHA DE S.PAULO. Fabricante do suco AdeS reconhece erros e pede desculpas a clientes. 23 mar. 2013.

Localização: comunicados da Anvisa de 18 mar. e 8 abr.; síntese da Câmara de 27 mar.; inspeção sanitária e declarações empresariais reproduzidas pela Folha. As fontes públicas não sustentam atribuição causal exclusiva a uma pessoa.

Referências conceituais

Leituras de apoio às definições e à interpretação organizacional. As formulações de “protocolo” e “primeira quebra” são convenções analíticas do próprio livro.

FG-01 | Defesas e abordagem sistêmica

REASON, James. *Human error: models and management*. BMJ, v. 320, n. 7237, p. 768-770, 18 mar. 2000. DOI: 10.1136/bmj.320.7237.768.

<https://pmc.ncbi.nlm.nih.gov/articles/PMC1117770/>

Leitura de apoio para distinguir a abordagem centrada na pessoa da análise das condições do sistema e de suas defesas. Não é fonte factual de todos os casos do livro.

FG-02 | Normalização do desvio

VAUGHAN, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago: University of Chicago Press, 1996. Registro bibliográfico e apresentação na AHRQ/PSNet.

<https://psnet.ahrq.gov/issue/challenger-launch-decision-risky-technology-culture-and-deviance-nasa>

Referência conceitual identificada para aprofundamento. Não se atribui a esta revisão uma leitura integral do livro nem se inventam páginas de citação.

FG-03 | Estol e ângulo de ataque

FEDERAL AVIATION ADMINISTRATION (FAA). *Airplane Flying Handbook*. FAA-H-8083-3C, 2021. Capítulo 5: Maintaining Aircraft Control: Upset Prevention and Recovery Training.

https://www.faa.gov/sites/faa.gov/files/regulations_policies/handbooks_manuals/aviation/airplane_handbook/06_afh_ch5.pdf

Localização: seção Stalls, p. 5-12. Apoio à definição de estol no glossário.

Índice de casos

32 entradas, em ordem alfabética. “Texto” abre o caso; “Nota” abre suas referências. A nota ND-01 identifica a natureza testemunhal de A Farsa.

<i>Caso e localização</i>	<i>Texto</i>	<i>Nota</i>
A Farsa Prólogo	9	135 [ND-01]
AdeS Caso AdeS	81	151 [ND-32]
Angrois Interlúdio: última barreira	44	139 [ND-08]
Ayrton Senna Capítulo 1	17	136 [ND-02]
Bhopal Capítulo 6	37	138 [ND-06]
Blue Bell Creameries Interlúdio: desvio ao público	58	143 [ND-15]
Boeing 737 MAX Capítulo 9	51	141 [ND-12]
Brumadinho Capítulo 8	47	140 [ND-11]
Challenger Capítulo 4	27	137 [ND-04]
Chapecoense Capítulo 2	21	136 [ND-03]
Chernobyl Capítulo 5	31	137 [ND-05]
Costa Concordia Capítulo 16	89	148 [ND-25]
Deepwater Horizon Capítulo 12	67	144 [ND-18]
Dieselsgate Capítulo 11	63	144 [ND-17]
Equifax Interlúdio: verdades adiadas	101	150 [ND-29]
Flint Interlúdio: desvio ao público	59	143 [ND-16]

<i>Caso e localização</i>	<i>Texto</i>	<i>Nota</i>
General Motors Capítulo 18	97	149 [ND-27]
Grenfell Tower Capítulo 13	73	146 [ND-22]
Imperial Sugar Interlúdio: aparência	71	146 [ND-21]
Lac-Mégantic Interlúdio: última barreira	45	140 [ND-10]
OceanGate Titan Capítulo 15	85	147 [ND-24]
Peanut Corporation of America Capítulo 14	77	147 [ND-23]
Piper Alpha Interlúdio: última barreira	44	139 [ND-09]
Qantas 32 Interlúdio: QF32	126	151 [ND-31]
Rana Plaza Interlúdio: aparência	70	145 [ND-20]
Samsung Galaxy Note7 Interlúdio: verdades adiadas	101	149 [ND-28]
Takata Interlúdio: desvio ao público	58	142 [ND-14]
Therac-25 Capítulo 7	41	138 [ND-07]
Theranos Interlúdio: verdades adiadas	102	150 [ND-30]
ValuJet 592 Capítulo 17	93	148 [ND-26]
Voepass, voo 2283 Capítulo 10	55	142 [ND-13]
Wells Fargo Interlúdio: aparência	70	145 [ND-19]

Glossário

Definições para leitura do livro, em ordem alfabética. As páginas indicam passagens do texto; as fontes técnicas dos casos estão nas notas ND. Não se trata de manual de operação.

Airframe De-Icing. Sistema de remoção de gelo de superfícies da estrutura da aeronave. A proteção disponível e suas limitações dependem do modelo e de sua documentação operacional. p. 55.

AZ-5. Comando de parada de emergência do reator RBMK, também identificado como EPS-5 em traduções. Seu acionamento deveria inserir as barras de controle. p. 33.

Barreira. Defesa física, técnica ou organizacional destinada a evitar a progressão de um risco ou reduzir suas consequências. A existência formal não garante sua eficácia. p. 13, 123.

Cadeia de custódia. Registros e cuidados que permitem acompanhar coleta, guarda, acesso e transferência de evidências, preservando sua integridade e identificação. p. 130.

CIP (Cleaning in Place). Sistema de limpeza de equipamentos e circuitos sem desmontagem, com circulação controlada de soluções de limpeza e enxágue. No caso AdeS, o estado de limpeza deveria impedir o envase. p. 81-84.

Coefficiente de vazio positivo. Propriedade pela qual, em determinadas condições, o aumento de vapor no refrigerante acrescenta reatividade ao reator. p. 32.

Cultura de segurança. Valores, decisões e práticas que determinam o lugar efetivo da segurança na organização, inclusive diante de metas e pressões. p. 33, 56.

Defeat device. Dispositivo ou estratégia de manipulação capaz de alterar o funcionamento do controle de emissões nas condições de teste, conforme o caso Dieseltgate. p. 63, 64.

Estol. Condição aerodinâmica em que o ângulo de ataque ultrapassa o valor crítico e o escoamento sobre a asa se separa, reduzindo a sustentação. Não é definido apenas por uma velocidade baixa. Ver FG-03. p. 55.

Falha não contida. Falha de motor na qual fragmentos escapam de sua contenção e podem atingir outras partes e sistemas da aeronave. p. 126.

Housekeeping. Rotinas de organização, limpeza e remoção de depósitos. No caso Imperial Sugar, inclui impedir o acúmulo perigoso de poeira combustível. p. 71.

Intertravamento. Proteção que impede uma ação ou sequência enquanto condições necessárias de segurança não estiverem atendidas. p. 42, 81, 84.

Liquefação estática. Perda acentuada de resistência de material suscetível sob carregamento estático, podendo provocar grande deformação e escoamento. p. 47.

Margem de segurança. Reserva entre a condição de operação e um limite relevante, considerando variação, incerteza e degradação. p. 21.

MCAS. Maneuvering Characteristics Augmentation System. Função de controle de voo do Boeing 737 MAX que atua sobre o estabilizador em determinadas condições. p. 51, 52.

MEL. Minimum Equipment List: lista de equipamentos mínimos. Define condições e limitações para operar temporariamente com determinados itens inoperantes; não é uma autorização geral para voar com qualquer falha. p. 55, 57.

MIC. Isocianato de metila, intermediário químico utilizado na fabricação de pesticidas, altamente reativo com água. p. 37, 38.

Normalização do desvio. Processo pelo qual desvios repetidos e resultados aparentemente aceitáveis tornam uma condição anormal socialmente tolerada. Ver FG-02. p. 29, 56.

O-ring. Anel de vedação. No Challenger, integrava a vedação das juntas dos segmentos dos foguetes auxiliares de combustível sólido. p. 27.

Patch. Correção de software. A aplicação precisa ser confirmada nos sistemas afetados para que o registro da ação corresponda à condição real. p. 101, 102.

Poeira combustível. Material sólido dividido em partículas capaz de queimar e, quando disperso em condições adequadas, alimentar explosões. p. 71.

Primeira quebra. Expressão analítica do autor para o momento em que um limite destinado a controlar um risco perde autoridade sobre a decisão. Não designa necessariamente uma causa única. p. 12, 105.

Protocolo. No sentido ampliado adotado pelo autor, conjunto efetivo de regras, especificações, barreiras, testes, bloqueios e critérios de decisão voltados ao controle de risco. p. 13, 115.

Rastreabilidade. Capacidade de reconstruir origem, configuração, alterações, registros e resultados de um item, processo ou verificação. p. 125.

RBMK. Família de reatores moderados a grafite e refrigerados a água. O capítulo trata da unidade 4 de Chernobyl e de suas características na época do acidente. p. 32.

Recall. Ação para recolher, reparar, substituir ou corrigir produtos em circulação diante de um problema de segurança. Seu alcance depende do produto e da medida adotada. p. 82, 98, 101.

Redundância. Disponibilidade de recursos ou defesas adicionais para cumprir uma função. Falhas de causa comum podem comprometer simultaneamente recursos aparentemente redundantes. p. 38, 127.

Retenção de produto. Bloqueio temporário do produto acabado até que critérios de liberação demonstrem condição adequada para seguir ao mercado. No caso AdeS, a retenção foi uma das barreiras reforçadas após o evento. p. 82, 84.

Teste de pressão negativa. Verificação empregada no controle de poços para avaliar a integridade de barreiras sob uma condição de pressão reduzida no interior do poço. p. 67, 68.

Validação. Demonstração, por evidências e ensaios representativos, de que uma solução é adequada ao uso e às condições pretendidos. p. 124.

Verificação. Confirmação, por evidência objetiva, de que um requisito ou critério definido foi atendido. No livro, inclui provar que a barreira funciona na condição relevante. p. 123, 124, 125.

Sobre o autor

Ricardo Xavier de Oliveira

Ricardo Xavier de Oliveira é engenheiro de alimentos, químico e pós-graduado em Engenharia de Processos Químicos pela Unicamp. Construiu uma carreira de mais de três décadas em manufatura, com atuação nas indústrias de alimentos, química, farmacêutica e de nutrição animal.

Ao longo dessa trajetória, trabalhou em produção, qualidade, engenharia, projetos e melhoria contínua, ocupando posições de direção em operações industriais. A convivência direta com fábricas, auditorias, crises, clientes e decisões sob pressão formou a perspectiva apresentada neste livro.

Seu olhar combina método, responsabilidade e experiência prática. Em vez de encerrar análises em “erro humano”, procura identificar a arquitetura que permitiu que o risco continuasse avançando e o momento em que um limite perdeu autoridade.

A Quebra é seu projeto de síntese: uma investigação sobre protocolos, verdade, liderança e o instante em que ainda existe uma decisão capaz de mudar o desfecho.

A experiência ensina que o problema mais perigoso não é aquele que a organização desconhece. É aquele que ela aprendeu a tolerar.

**UMA INVESTIGAÇÃO SOBRE LIMITES,
DECISÕES E CONSEQUÊNCIAS**

Nem todo grande colapso começa com uma explosão.

Às vezes, começa com uma inspeção adiada, um alerta relativizado, uma meta que vence um limite ou um protocolo que já não tem autoridade para parar a sequência.

Em *A Quebra*, Ricardo Xavier de Oliveira percorre acidentes, recalls, contaminações, fraudes, desastres ambientais e perdas de confiança para revelar uma lógica comum: antes da falha visível, quase sempre houve uma quebra anterior, menos dramática, menos fotografada e muito mais decisiva.

Com linguagem acessível, rigor técnico e narrativa envolvente, o autor mostra que protocolos não são burocracia. São o último limite entre a rotina e o colapso.

Este livro é um convite para olhar os grandes desastres por outro ângulo: não apenas o que quebrou no fim, mas o que deixou de funcionar antes.

Toda tragédia tem uma história anterior.

RICARDO XAVIER DE OLIVEIRA

é engenheiro e executivo com ampla experiência em manufatura, qualidade, processos e liderança industrial. Em *A Quebra*, reúne investigação, reflexão e prática para mostrar como organizações entram em colapso quando seus limites deixam de ter autoridade.



ACESSE RXO

CÓDIGO DE BARRAS: A DEFINIR