Um conto sobre duas seguranças

Erik Hollnagel

Professor da Universidade do Sul da Dinamarca;

Consultor-Chefe do Centro de Melhoria de Qualidade, Região do Sul da Dinamarca;

Presidente de Segurança Industrial, Mines ParisTech, França

hollnagel.erik@gmail.com

www.resilienthealthcare.net e www.functionalresonance.com

Perceba o que não pode ser visto
Miyamoto Musashi (1584 - 1645)

Tradução: Portal proqualis.net

Sumário

A existência sustentada das sociedades modernas depende do funcionamento seguro e eficiente de múltiplos sistemas, funções e serviços especializados. Como esses elementos estão intimamente ligados, não é possível gerir a segurança apenas pela reação diante de algo que dá errado. Tanto a teoria como a prática deixam claro que, quando a gestão da segurança *sucede a*os acontecimentos, em vez de *precedê-los*, ela corre o sério risco de ficar para trás e de ser reduzida a um apagar de incêndios descoordenado e fragmentado (naturalmente, o mesmo vale para a gestão da qualidade e da produtividade). Para evitar que isso aconteça, a gestão da segurança deve olhar para a frente, não só para evitar que as coisas deem errado, mas também — o que é mais importante — para garantir que deem certo.[1] A gestão proativa da segurança deve se concentrar naquilo que faz com que o desempenho cotidiano geralmente funcione de forma correta, e não nas razões para as falhas ocasionais, e deve tentar melhorar ativamente o bom funcionamento, em vez de simplesmente evitar os problemas.

Segurança como a ausência de riscos inaceitáveis

Tradicionalmente, a segurança foi definida como uma situação na qual nada dá errado. Ou, então, já que é impossível assegurar que nada dê errado, como uma situação na qual a

[1] Num mundo completamente diferente, uma equipe de futebol ou de rugby que só jogasse defensivamente para impedir o adversário de marcar teria pouca chance de vencer a partida.

ocorrência de eventos indesejáveis é reduzida a um mínimo aceitável.[2] No entanto, essa é uma definição indireta e um pouco paradoxal, uma vez que a segurança é definida pelo seu oposto, por aquilo que ocorre em sua ausência. Em consequência dessa definição, a segurança também é medida indiretamente, não por sua presença como uma qualidade em si mesma, mas pelas consequências de sua ausência.

Em relação às atividades humanas, faz perfeito sentido nos concentrarmos em situações nas quais algo dá errado, pois essas situações, por definição, são inesperadas e podem levar a danos imprevistos e indesejáveis ou à perda de vidas e de bens materiais. Um exemplo antigo é o colapso da Ponte de Rialto, em Veneza, que ficou sobrecarregada de espectadores durante o casamento do Marquês de Ferrara, em 1444 (é claro que ocorreram muitos acidentes espetaculares antes desse, mas o registro histórico é superficial e incompleto). O colapso da ponte é um exemplo característico das preocupações clássicas com segurança, que lidavam com riscos relacionados a tecnologias e estruturas passivas, como edifícios, pontes, navios etc. A essas preocupações somaram-se as necessidades criadas pela segunda revolução industrial, em torno de 1750, que foi marcada pela invenção de uma máquina a vapor viável. A rápida mecanização do trabalho que veio a seguir levou a um número crescente de acidentes até então desconhecidos, que tinham em comum colapsos, falhas ou defeitos nas tecnologias ativas. Hale & Hovden (1998) caracterizam esse período como a era da tecnologia, na qual as preocupações com a segurança procuravam proteger as máquinas, impedir explosões ou evitar o colapso de estruturas. O foco na tecnologia como a principal — ou até a única — fonte de problemas e soluções de segurança manteve-se firme até 1979, quando o acidente na usina nuclear de Three Mile Island, nos EUA, demonstrou que cuidar da tecnologia não era suficiente.[3] Esse acidente chamou a atenção para o papel dos fatores humanos — ou até *do* fator humano —, tornando necessário considerar as falhas e os erros humanos como riscos em potencial. Sete anos depois, a perda do ônibus espacial Challenger, reforçada pelo acidente em Chernobyl, exigiu mais uma reformulação das noções tradicionais de segurança, acrescentando, desta vez, a influência das falhas organizacionais e da cultura de segurança.

Ao longo dos séculos, o ponto de partida das preocupações de segurança sempre foi a ocorrência, possível ou efetiva, de algum tipo de resultado adverso, seja ele

---

[2] A palavra em inglês para segurança, *safe*, vem do francês *sauf*, que significa "exceto" e "salvo". A origem da palavra vem do latim *salvus*, que significa ileso, saudável e seguro.

[3] A essa altura, a Engenharia dos Fatores Humanos já tinha mais de 30 anos, mas, de modo geral, havia se concentrado mais na produtividade do que em questões de segurança.

classificado como um risco, um perigo, um *near miss*, um incidente ou um acidente. Historicamente, os novos tipos de acidente foram explicados pela introdução de novas causas (p.ex., fadiga de metais, "erro humano", falha organizacional), e não pelo questionamento ou modificação da noção subjacente básica de causalidade. Dessa forma, ficamos tão acostumados a explicar os acidentes em termos de relações de causa e efeito — simples ou compostas — que já nem percebemos isso. E assim nos agarramos ferozmente a essa tradição, embora seja cada vez mais difícil reconciliá-la com a realidade.

Habituação

Uma consequência indesejada, porém inevitável, do fato de associarmos a segurança àquilo que dá errado é uma progressiva falta de atenção com o que dá certo. A explicação psicológica para isso se chama habituação, um comportamento adaptativo que pode ser descrito como uma forma de aprendizado não-associativo. Por meio da habituação, aprendemos a desconsiderar o que ocorre regularmente, simplesmente porque ocorre regularmente. A definição formal de habituação é uma "resposta decrescente como resultado da estimulação repetida" (Harris, 1943, p. 385). Na psicologia acadêmica, a habituação foi estudada, e geralmente também explicada, ao nível da neuropsicologia (Thompson & Spencer, 1966).

No entanto, é perfeitamente possível falarmos de habituação ao nível do comportamento humano cotidiano — ações e respostas. Isso foi observado já em 1890, quando William James, um dos fundadores da psicologia, escreveu que "o hábito diminui a atenção consciente com a qual realizamos nossos atos" (James, 1890, 114). Na linguagem de hoje, isso significa que deixamos de prestar atenção a algo tão logo nos acostumamos a fazê-lo. Depois de algum tempo, já não notamos o que funciona bem, nem pensamos que seja necessário fazê-lo. Isso se aplica tanto às ações como aos seus resultados — e tanto ao que fazemos pessoalmente como ao que é feito pelos outros.

De uma perspectiva evolutiva, e também do ponto de vista de um equilíbrio entre a eficiência e a meticulosidade (Hollnagel, 2009), a habituação faz muito sentido. Embora tenhamos boas razões para dar atenção ao que é inesperado e incomum, pode ser uma perda de tempo e de esforço dar muita atenção ao que é comum ou semelhante. Citando James mais uma vez: "As ações habituais são conhecidas e, por não correrem o risco de se desviar de seu objetivo, não precisam de auxílio externo" (p. 149). A redução na atenção é justamente o que ocorre quando as ações produzem regularmente os resultados desejados e esperados e quando as coisas "simplesmente" funcionam. Quando tudo dá certo, não existe

diferença entre o que é esperado e o que de fato ocorre. Dessa forma, não há nada que atraia a nossa atenção ou incite uma reação de alerta. Também não temos nenhuma motivação para tentar entender por que as coisas deram certo: isso obviamente aconteceu porque o sistema — as pessoas e a tecnologia — funcionou como deveria e porque não ocorreu nenhum inconveniente. Embora o primeiro argumento — a ausência de diferença observável entre resultados — seja aceitável, o segundo tem falhas cruciais. A razão para isso ficará clara a seguir.

Observando o que dá errado, ao invés do que dá certo

Para ilustrar as consequências de observarmos o que dá errado ao invés do que dá certo, considere a Figura 1. Ela representa o caso no qual a probabilidade (estatística) de uma falha é de 1 em 10.000 — em termos técnicos, $p = 10^{-4}$. Isso significa que, para cada vez que algo der errado (a linha fina), haverá 9 vezes em que tudo dará certo e em que o resultado será aquele que desejamos (a área em cinza). A razão de 1:10.000 corresponde a um sistema ou organização cuja ênfase está no desempenho (cf., Amalberti, 2006). Essa razão seria ainda mais extrema num sistema ultrasseguro.

Por exemplo, considere a colisão de trens em Buizingen, na Bélgica, em 15 de fevereiro de 2010 (Organisme d'Enquête pour les Accidents et Incidents Ferroviaires, 2012). Dois trens, que transportavam entre 250 e 300 pessoas, chocaram-se num dia nevado, no horário de pico da manhã. Ao que parece, os trens colidiram "lateralmente" numa junção na saída da estação de Halle. Dezoito pessoas morreram e 162 ficaram feridas, e a ferrovia foi seriamente danificada. A investigação determinou que um dos trens havia cruzado um sinal vermelho sem parar (o que é chamado SPAD, ou *Signal Passed At Danger*) e que essa pode ter sido uma das causas que contribuíram para a colisão. Uma investigação mais extensa revelou que haviam ocorrido 130 eventos SPAD na Bélgica no ano de 2012, dos quais um terço foram eventos graves. Mas também foi estimado que, em cerca de 13.000.000 casos, os trens pararam no sinal vermelho, o que gera uma razão de 10^{-5}.

As estatísticas do aeroporto de Frankfurt servem como mais um exemplo. Em 2011, houve um total de 490.007 movimentos de aeronaves, mas apenas 10 violações de separação e 11 incursões em pista. Isso corresponde a razões de $2{,}04 \times 10^{-5}$ e $2{,}25 \times 10^{-5}$, respectivamente, ou cerca de 2 casos em cada 100.000.

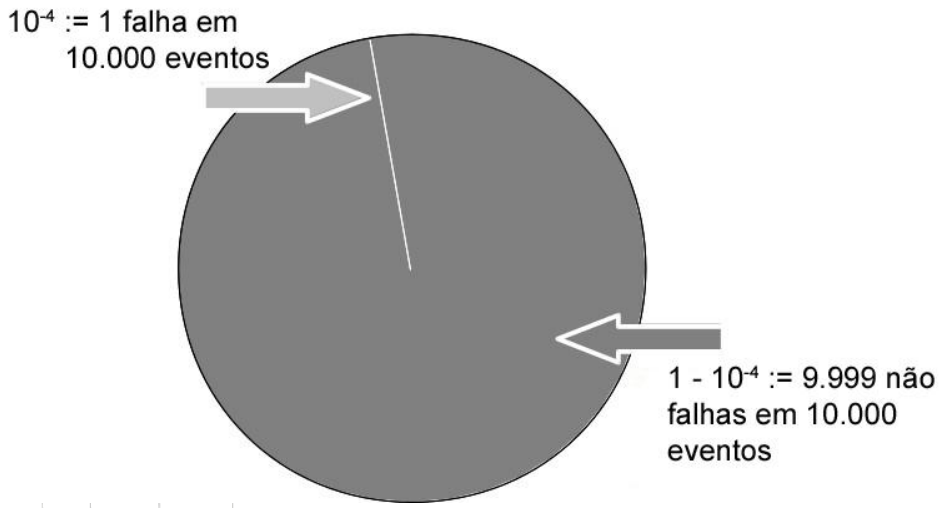

Figura 1: O desequilíbrio entre o que dá certo e o que dá errado

A tendência de concentrarmo-nos no que dá errado é reforçada de muitas maneiras. Ela é frequentemente exigida pelas autoridades; é apoiada por modelos e métodos;[4] é documentada em incontáveis bancos de dados e ilustrada em inúmeros gráficos; é descrita em literalmente milhares de artigos, livros e atas de conferências; e existe um número incalculável de especialistas, consultores e empresas que nos lembram constantemente da necessidade de evitar riscos, falhas e acidentes — e de como os seus serviços podem nos ajudar a fazê-lo. O resultado final é uma abundância de informações sobre tudo o que pode dar errado e sobre o que deve ser feito para evitá-lo. O foco nas falhas também se adéqua à nossa compreensão estereotipada sobre o que é a segurança e sobre como deve ser gerida, conforme já mencionado anteriormente. Essa receita baseia-se no princípio simples conhecido como "encontrar e corrigir": procure falhas e defeitos, tente descobrir suas causas e, então, tente eliminá-las e/ou aprimorar as barreiras.

Uma consequência infeliz e contraproducente desse modelo é que a segurança e a atividade principal (a produção) competem por recursos; assim, os investimentos em segurança são vistos como custos e, portanto, são (às vezes) difíceis de justificar ou manter.

[4] Reason (1979) defendeu que "o erro e o desempenho correto são dois lados da mesma moeda, e uma teoria adequada sobre o primeiro implicará uma melhor compreensão do segundo do que a que temos atualmente". Esse era o pensamento geral na época. Porém, hoje em dia, a conclusão seria a oposta, isto é, que precisamos entender o segundo para entender o primeiro.

Outra consequência é que o aprendizado se limita àquilo que deu errado, ou seja, ocorre com pouca frequência e só utiliza uma pequena fração dos dados disponíveis.[5]

A situação é bastante diferente quando examinamos o que dá certo, isto é, os 9.999 eventos do total de 10.000. O foco no que dá certo não recebe muito apoio. Não há pressão por parte das autoridades para examinarmos o que funciona bem e, se alguém quiser fazê-lo, terá dificuldade em encontrar auxílio; temos poucas teorias ou modelos sobre como funciona o bom desempenho humano e organizacional e poucos métodos que nos ajudem a estudá-lo; os exemplos são escassos (Reason, 2008) e é difícil encontrar dados reais; temos dificuldade em encontrar artigos, livros ou outras formas de literatura científica sobre o tema; por fim, há poucos profissionais que possam ser considerados peritos no tema ou que sequer o considerem importante. Além disso, essa perspectiva vai de encontro ao foco tradicional nas falhas, e até mesmo aqueles que a veem como um tema digno de investigação deparam-se com problemas ao entrarem nas questões práticas: não existem métodos ou ferramentas simples e temos muito poucos bons exemplos com os quais aprender.

Ainda assim, uma consequência interessante dessa perspectiva é que a segurança e a atividade principal já não competem pelos recursos; o que beneficia a primeira também beneficiará a segunda. Outra consequência é que o aprendizado pode se concentrar no que deu certo, ou seja, existem literalmente inúmeras oportunidades de aprendizado e os dados para isso estão facilmente disponíveis — uma vez que a atenção deixa de estar concentrada das falhas.

Segurança I: Evitando que as coisas deem errado

Podemos chamar de Segurança I a definição tradicional de segurança como uma situação na qual o número de resultados adversos (acidentes/incidentes/*near misses*) é o mais baixo possível. Consequentemente, o objetivo da gestão da Segurança I é atingir e manter esse estado. Por exemplo, a Agency for Healthcare Research and Quality, dos EUA, define a segurança como a "*ausência de lesões acidentais*", enquanto a Organização Internacional da Aviação Civil a define como "*o estado no qual os danos às pessoas ou aos bens materiais são reduzidos a um nível aceitável e mantidos nesse nível, ou abaixo dele, por meio de um processo continuado de identificação de perigos e gestão de riscos*"!

[5] Uma visão mais cínica diria que o aprendizado se limita àquilo que conseguimos descrever e explicar.

A "filosofia" da Segurança I está ilustrada na Figura 2. Ela promove uma visão bimodal ou binária do trabalho e das atividades, segundo a qual estes serão bem ou mal sucedidos (isto, naturalmente, está de pleno acordo com os métodos tradicionais de representar os acidentes e os riscos, que sempre se baseiam em alguma forma de árvore ramificada). Quando tudo funciona conforme o esperado (o funcionamento "normal"), os resultados serão aceitáveis; tudo funciona corretamente, isto é, o número de eventos adversos mantém-se num nível aceitável. Porém, quando algo dá errado, quando existe uma disfunção, humana ou não, o resultado será uma falha (um resultado inaceitável). A questão, portanto, é compreendermos como ocorre a transição do normal para o anormal (o mau funcionamento); por exemplo, entendermos se houve uma transição abrupta ou se ocorreu um "encaminhamento gradual em direção ao problema". Segundo a lógica da Segurança I, a segurança e a eficiência serão alcançadas quando conseguirmos bloquear essa transição.

O foco nas falhas cria a necessidade de encontrarmos suas causas. Quando uma causa é encontrada, o próximo passo lógico é eliminá-la ou desfazer possíveis relações de causa e efeito. A partir daí, o resultado deve ser medido contando-se a redução no número de eventos indesejados após a intervenção. Dessa forma, a Segurança I implica o que poderíamos chamar de "*hipótese das causas diferentes*", isto é, a ideia de que os eventos adversos e o funcionamento correto possuem diferentes causas ou "mecanismos". Se não fosse assim, a eliminação das causas e a neutralização dos "mecanismos" também reduziria a probabilidade de que os processos funcionassem corretamente; portanto, seria contraproducente.

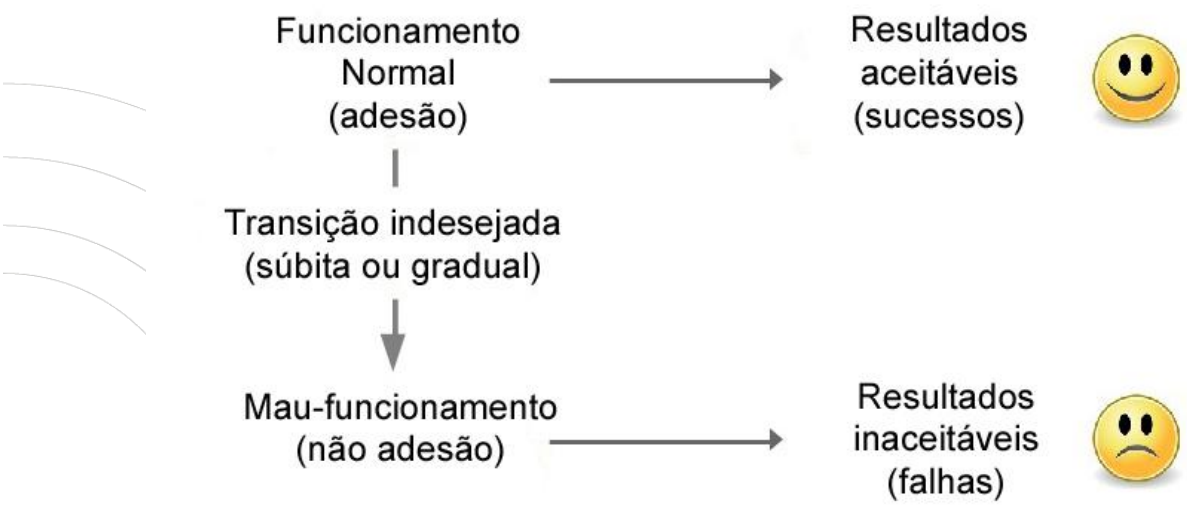

Figura 2: Como a Segurança I enxerga os sucessos e as falhas

A Segurança I adota o pressuposto tácito que os sistemas funcionam corretamente porque foram bem concebidos e são mantidos de forma escrupulosa, porque os procedimentos são completos e corretos, porque os gestores conseguem prever e antecipar até mesmo as menores contingências e porque as pessoas se comportam da forma esperada — e, sobretudo, por terem sido ensinadas ou treinadas a fazê-lo. Isso leva inevitavelmente a uma ênfase na *adesão* ao modo como o trabalho é realizado.

O contexto para a perspectiva da Segurança I encontra-se em sistemas bem compreendidos, bem testados e bem comportados. Tais sistemas tipicamente possuem equipamentos altamente confiáveis, trabalhadores e gestores atentos em seus testes, observações, procedimentos, treinamentos e operações, um pessoal bem treinado, uma administração esclarecida e bons procedimentos operacionais. Se esses pressupostos estiverem corretos, os seres humanos — enquanto "máquinas falíveis" — são claramente uma desvantagem, e a variabilidade de seu desempenho pode ser vista como uma ameaça. Segundo a lógica da Segurança I, o objetivo — o estado de segurança almejado — pode ser atingido restringindo-se todo tipo de variabilidade no desempenho. Alguns exemplos de restrições utilizadas com frequência são a seleção, o treinamento estrito, as barreiras de diversos tipos, os procedimentos, a padronização, as regras e as normas. O otimismo indevido em relação à eficácia dessa solução tem raízes históricas. Porém, embora o otimismo pudesse ser parcialmente justificado há cem anos, o mesmo não ocorre na

atualidade. A principal razão para isso é que o ambiente de trabalho se modificou drasticamente, a tal ponto que os pressupostos que tínhamos no passado recente já não são válidos.

Segurança I: Gestão reativa da segurança

A natureza da gestão da segurança depende claramente da definição de segurança. Da perspectiva da Segurança I, o objetivo da gestão de segurança é garantir que o número de resultados adversos seja mantido o mais baixo possível — ou tão baixo quanto razoável em termos práticos (p.ex., Melchers, 2001). Um bom exemplo disso é o ciclo de pesquisa da OMS ilustrado na Figura 3. A figura mostra um ciclo repetitivo de etapas que começa quando algo dá errado, resultando em dano a alguém. No cuidado de saúde, "medir o dano" significa contar quantos pacientes sofreram dano ou morreram, e por quais tipos de eventos adversos. Nas ferrovias, os acidentes podem ser definidos como "mortes, lesões incapacitantes e lesões menores sofridas por funcionários, por 200.000 horas de trabalho cumpridas pelos funcionários da companhia ferroviária" ou como "acidentes entre trens ou em passagens de nível que cumpram os critérios de notificação, por milhão de milhas percorridas". Podemos encontrar definições semelhantes em todos os domínios nos quais existe uma preocupação com a segurança.

Essa abordagem para a segurança é *reativa*, pois se baseia em responder a algo que deu errado ou que foi identificado como um risco — como algo que poderia dar errado. A resposta geralmente envolve a busca de maneiras de eliminar a causa — ou causas — detectada ou de controlar os riscos, o que pode ser feito detectando e eliminando as causas ou melhorando as opções para a detecção e a recuperação. A gestão reativa da segurança adota o *credo da causalidade*, que pode ser expresso da seguinte maneira: (1) os resultados adversos (acidentes, incidentes) ocorrem quando algo dá errado; (2) portanto, os resultados adversos têm causas, que podem ser detectadas e corrigidas.

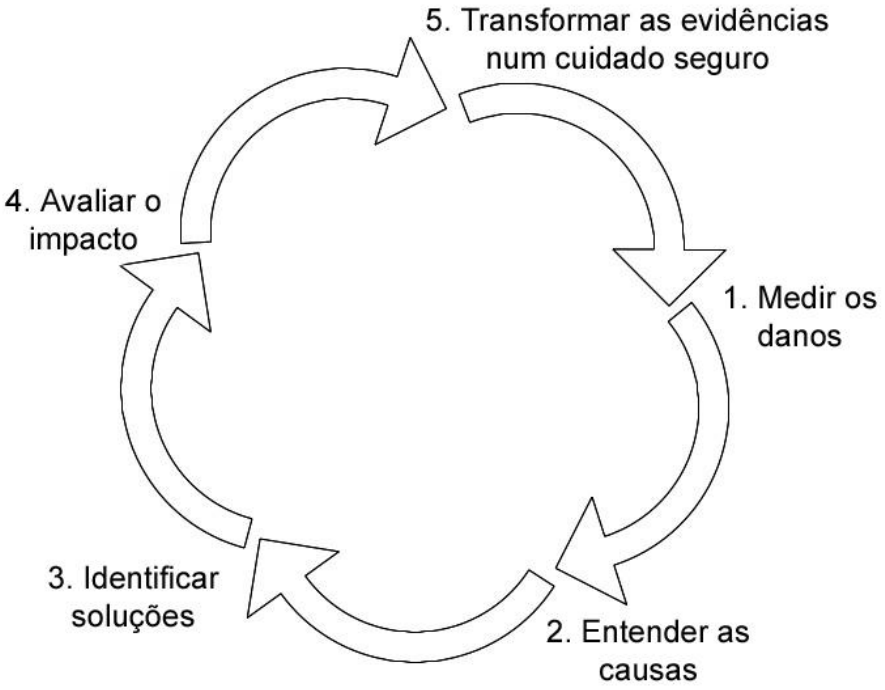

Figura 3: Ciclo de gestão reativa da segurança (OMS)

Da perspectiva da Segurança I, o objetivo da gestão de segurança é manter o número de acidentes e incidentes o mais baixo possível, reagindo diante da ocorrência de um evento inaceitável. Em princípio, essa gestão reativa da segurança pode funcionar se os eventos não ocorrerem com uma frequência tão elevada que chegue a dificultar ou impossibilitar a realização do trabalho real, isto é, das atividades principais. Porém, se a frequência de eventos adversos aumentar, a necessidade de responder exigirá, mais cedo ou mais tarde, tamanho consumo de capacidades que as reações se tornarão inadequadas e, em parte, não conseguirão acompanhar o processo. Na prática, isso significa que a organização irá perder o controle da situação e, com isso, a capacidade de gerir efetivamente a segurança (Hollnagel & Woods, 2005).

É fácil encontrar exemplos práticos dessa situação. Vários eventos climáticos — tornados ou tufões — podem facilmente exaurir a capacidade de resposta dos serviços de resgate. O mesmo vale para os incêndios florestais ou os grandes derramamentos de petróleo, que pode vazar de navios ou do fundo do oceano. Se os pacientes chegarem a um serviço de emergência a uma taxa mais alta que a taxa de tratamento e alta hospitalar, a capacidade de tratá-los logo será exaurida. Isso pode ocorrer durante situações cotidianas (Wears & Perry, et al., 2006) ou durante uma epidemia (Antonio et al., 2004). Num nível mais mundano, a maioria das indústrias (usinas elétricas, companhias aéreas etc.) tem

dificuldade em gerir o turbilhão de notificações de incidentes exigidas por lei. Mesmo que sejam analisados apenas os casos mais graves, ainda poderá não haver tempo suficiente para compreender os acontecimentos e responder a eles.

Além disso, é preciso que o processo gerido seja suficientemente conhecido e regular a ponto de permitir a preparação prévia de respostas (antecipação). A pior situação é claramente aquela em que ocorre algo completamente desconhecido, pois, nesse caso, será preciso gastar tempo e recursos para descobrir o que aconteceu e decidir o que fazer antes que a resposta seja efetivamente implementada. Para que a gestão reativa da segurança seja efetiva, a organização deve conseguir reconhecer os eventos com muita rapidez, de modo a iniciar uma resposta preparada num prazo mínimo. A desvantagem dessa abordagem é que o reconhecimento apressado e descuidado do problema pode levar a respostas inadequadas e ineficazes.

Segurança II: Garantindo que as coisas deem certo

Com o desenvolvimento contínuo dos sistemas técnicos e sociotécnicos, devido, em parte, ao nosso fascínio por tecnologias da informação cada vez mais poderosas, os sistemas e ambientes de trabalho tornaram-se cada vez mais incontroláveis (Hollnagel, 2010). Como os modelos e métodos da Segurança I presumem que os sistemas sejam controláveis, isto é, que sejam bem compreendidos e bem comportados, tais modelos e métodos são cada vez menos capazes de atingir o "estado de segurança" exigido e almejado. Como essa incapacidade não pode ser superada por uma "extensão" ainda maior das ferramentas da Segurança I, faz sentido considerarmos se o problema não poderia estar na definição de segurança. Assim, uma solução possível consiste em modificar a definição e nos concentrarmos no que dá certo, e não no que dá errado (como sugerido pela Figura 1). Isso fará com que a definição de segurança passe de "evitar que algo dê errado" para "assegurar que tudo dê certo" — ou, mais precisamente, para a capacidade de manter um bom funcionamento diante de condições variáveis, de modo que o número de resultados desejados e aceitáveis (em outras palavras, as atividades cotidianas) seja o mais alto possível.[6] A consequência dessa definição é que a base da segurança e de sua gestão passa a ser compreender por que as coisas dão certo, isto é, compreender as atividades cotidianas.

[6] Esta definição parafraseia a definição de resiliência como a "capacidade intrínseca de um sistema de ajustar seu funcionamento antes, durante ou depois de mudanças ou perturbações, de modo a sustentar as operações necessárias sob condições esperadas ou inesperadas" (Hollnagel *et al*, 2011)

A Segurança II presume explicitamente que os sistemas funcionam porque os profissionais conseguem ajustar aquilo que fazem para se adequar às condições de trabalho. As pessoas aprendem a identificar e a superar as falhas de *design* e os defeitos funcionais, pois não só conseguem reconhecer as exigências reais e ajustar seu desempenho conforme o necessário, como também interpretam e aplicam os procedimentos para que se adéquem às condições. As pessoas também conseguem detectar e corrigir os erros que ocorrem ou que estão prestes a ocorrer, intervindo antes que a situação se torne mais grave. O resultado disso é a variabilidade de desempenho, não no sentido negativo, que enxerga a variabilidade como o descumprimento de uma norma ou padrão, e sim no positivo, no qual a variabilidade representa os ajustes que servem de base para a segurança e a produtividade (Figura 4).

Em contraste com a Segurança I, a Segurança II reconhece que temos uma compreensão incompleta dos sistemas, que as descrições podem ser complicadas e que as mudanças são frequentes e irregulares, ao invés de infrequentes e regulares. Em outras palavras, a Segurança II reconhece que os sistemas são incontroláveis, e não controláveis (Hollnagel, 2010). Apesar da alta confiabilidade da tecnologia e dos equipamentos nestes sistemas, os funcionários e gestores muitas vezes trocam a meticulosidade pela eficiência. Além disso, a competência dos profissionais é variável e pode ser inconsistente ou incompatível, e os procedimentos operacionais confiáveis são escassos. Nessas condições, os seres humanos são claramente uma vantagem, e não uma desvantagem, e sua capacidade de ajustar seu trabalho segundo as condições é um trunfo, e não uma ameaça.

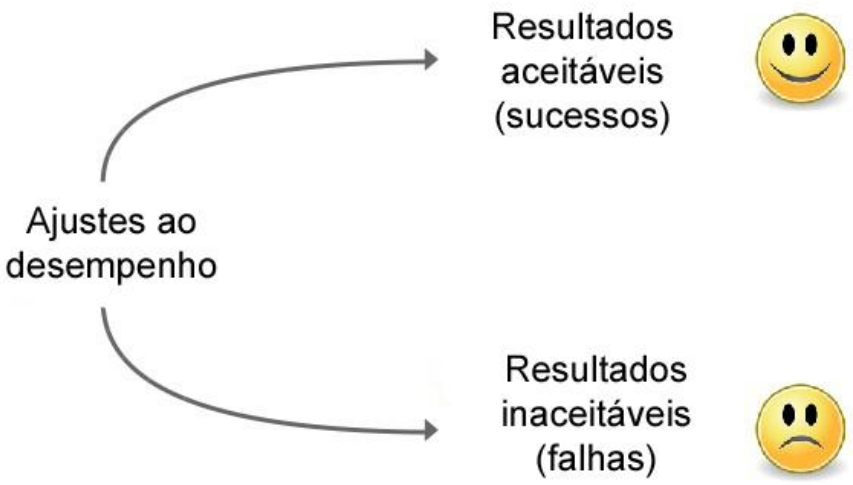

Figura 4: Como a Segurança II enxerga os sucessos e as falhas

A variabilidade de desempenho ou os ajustes ao desempenho são uma condição *sine qua non* para o funcionamento dos sistemas sociotécnicos, a menos que estes sejam extremamente simples. Dessa forma, os resultados ou falhas inaceitáveis não podem ser evitados pela eliminação ou restrição da variabilidade de desempenho, pois isso também afetaria os resultados aceitáveis e desejados. Em vez disso, é preciso fazer esforços para favorecer os improvisos e ajustes ao desempenho que são necessários, representando claramente os recursos e limitações de uma situação e fazendo com que seja mais fácil antecipar as consequências das ações. A variabilidade de desempenho deve ser gerida, refreada caso siga na direção errada e amplificada caso siga na direção certa. Para isso, é preciso, em primeiro lugar, reconhecer a variabilidade de desempenho; em segundo, monitorá-la; e, em terceiro, controlá-la. Esse é o âmbito de ação da gestão da segurança segundo a perspectiva da Segurança II.

Segurança II: Gestão proativa da segurança

A gestão da Segurança II e a engenharia da resiliência consideram que tudo ocorre essencialmente da mesma forma, independentemente do resultado. Assim, não é necessário termos um conjunto de causas e "mecanismos" para o que dá errado (acidentes e incidentes) e outro para o que dá certo (o trabalho cotidiano). O objetivo da gestão da segurança é assegurar o último; porém, ao fazê-lo, também reduziremos o primeiro. Embora tanto a Segurança I como a Segurança II levem a uma redução dos resultados indesejados, elas utilizam abordagens fundamentalmente diferentes, com importantes consequências sobre a gestão e a medição do processo — e também sobre a produtividade e a qualidade.

Da perspectiva da Segurança II, o objetivo da gestão da segurança é assegurar que o máximo possível dê certo, isto é, que o trabalho cotidiano atinja seus objetivos declarados. Isso não pode ser feito apenas pela reação, pois esta apenas corrigirá o que já aconteceu. Em vez disso, a gestão da segurança deve ser proativa, fazendo ajustes *antes* que algo aconteça e, portanto, afetando ou até evitando sua ocorrência. Uma das principais vantagens dessa estratégia é que as respostas rápidas, como um todo, exigem menos esforço, pois as consequências do evento terão menos tempo para se desenvolver e disseminar. Além disso, as respostas rápidas obviamente nos permitem poupar um tempo precioso.

Para que a gestão proativa da segurança funcione, é necessário prever, com uma certeza aceitável, o que poderia acontecer e possuir os meios adequados (pessoas e

recursos) para fazer algo a respeito. Isso, por sua vez, requer uma compreensão sobre o funcionamento do sistema, sobre o desenvolvimento e modificação de seu ambiente e sobre as maneiras pelas quais as funções podem depender uma da outra e se afetar mutuamente. Podemos adquirir essa compreensão examinando os padrões e relações entre diferentes eventos, em vez de buscar as causas de eventos específicos. Para enxergar e encontrar esses padrões, precisamos reservar algum tempo para compreender o que acontece, em vez de gastar todos os recursos no combate a incêndios.

Um exemplo trivial é o ato de "selar as escotilhas" de um navio quando uma tempestade se aproxima. Embora essa noção tenha origem na marinha, muitas pessoas que vivem em terra — ou numa plataforma de petróleo — também aprenderam a importância de se preparar para uma tempestade. No mundo financeiro, a gestão proativa da segurança é fundamental — uma instituição financeira que se limite a reagir logo irá à falência. Num domínio diferente, as precauções que se seguiram ao anúncio feito em 2009 pela Organização Mundial da Saúde sobre uma possível pandemia de gripe H1N1 são um exemplo de gestão proativa da segurança. Depois de ter sido dado o alerta, os governos europeus e de outras regiões passaram a armazenar quantidades consideráveis de medicamentos e vacinas para se assegurar de que possuíam os recursos necessários. Embora, no fim das contas, tenha ficado claro que era um alarme falso, o caso ilustra as características essenciais da gestão proativa da segurança.

Obviamente, um dos problemas da gestão proativa da segurança é a incerteza em relação ao futuro e o fato de que uma situação esperada pode não acontecer. Nesse caso, os preparativos terão sido em vão, havendo um desperdício de tempo e de recursos. Outro problema é a possibilidade de que as previsões sejam imprecisas ou incorretas, levando à realização de preparativos indevidos. Dessa forma, a gestão proativa da segurança representa um risco, em boa medida econômico. Porém, a alternativa, que é não estarmos preparados quando algo grave acontece, certamente será mais dispendiosa, tanto no curto como no longo prazo.

Conclusão

Embora as atividades cotidianas realizadas na linha de frente de uma organização nunca sejam apenas reativas, a pressão existente na maior parte das situações laborais requer que sejamos eficientes, em vez de meticulosos. Isso reduz as possibilidades de sermos proativos (Hollnagel, 2011). A gestão proativa da segurança, de fato, requer algum esforço inicial

destinado a considerar o que poderia ocorrer, a preparar respostas apropriadas, a alocar recursos e a conceber planos de contingência.

Na prática, é mais fácil sermos proativos em relação aos eventos de grande escala que aos de pequena escala, pois os primeiros tendem a se desenvolver de forma relativamente lenta — embora possam começar de forma abrupta. Os eventos de grande escala são regulares, e não irregulares, e frequentemente existem indicações claras de que uma resposta é necessária. Além disso, as respostas adequadas já são conhecidas, o que permite fazer preparativos antecipados.

É mais difícil sermos proativos diante dos numerosos eventos de pequena escala que constituem as situações de trabalho cotidianas. Nesses casos, os acontecimentos podem ser mais rápidos e inesperados, temos poucos indicadores para orientar-nos e os recursos muitas vezes são usados ao limite da escassez. Temos menos recursos a alocar e menos tempo para mobilizá-los. O ritmo de trabalho deixa poucas oportunidades para refletirmos sobre o que está ocorrendo e para atuar de forma estratégica. De fato, as pressões do trabalho e as demandas externas muitas vezes levam a soluções oportunistas que forçam o sistema a entrar num modo reativo. Para sairmos dessa situação — passando do modo reativo ao proativo — é necessário um esforço deliberado. Embora o custo dessa estratégia possa parecer inviável a curto prazo, trata-se, sem dúvida, de um investimento inteligente a longo prazo.

Apresento aqui algumas sugestões práticas sobre como iniciar esse processo:

- *Examine o que dá certo, além do que dá errado.* Aprenda com o que dá bom resultado e também com o que apresenta falhas. Não espere até que algo ruim aconteça; ao contrário, tente compreender o que realmente ocorreu nas situações em que não pareceu haver nada de extraordinário. A razão para as coisas darem certo não é simplesmente o fato de que todos seguiram os procedimentos. As coisas dão certo porque as pessoas fazem ajustes razoáveis segundo as exigências da situação. Descubra quais são esses ajustes e tente aprender com eles!
- *Quando algo deu errado, procure variações no desempenho cotidiano, e não causas específicas.* Sempre que algo é feito, é bastante provável que já tenha sido tentado antes. As pessoas logo descobrem quais ajustes em seu desempenho funcionam bem e, então, passam a confiar neles — justamente porque funcionam. Dessa forma, culpar as pessoas por fazerem o que geralmente fazem é contraproducente. Em vez disso, devemos tentar descobrir quais são os ajustes de desempenho geralmente utilizados pelos profissionais e as suas razões. As

coisas dão errado pelas mesmas razões que dão certo, mas é muito mais fácil e menos incriminatório estudar as razões para aquilo que dá certo.

- *Examine regularmente os acontecimentos e concentre-se em analisar a frequência com que ocorrem, em vez de sua gravidade.* É muito mais fácil sermos proativos diante do que ocorre com frequência do que diante de eventos raros. Uma pequena melhoria no desempenho cotidiano pode ser mais importante que uma grande melhoria no desempenho excepcional.
- *Reserve tempo para refletir, aprender e comunicar-se.* Se todo o tempo for utilizado na realização do trabalho básico, não haverá tempo para consolidar as experiências ou repor os recursos — incluindo a compreensão da situação. Dentro da cultura organizacional, a alocação de recursos — especialmente o tempo — para a reflexão, a partilha de experiências e o aprendizado deve ser vista como algo legítimo. Se não for assim, como é possível fazer qualquer tipo de melhoria?
- *Mantenha-se ciente da possibilidade de ocorrência de falhas — e seja diligente.* Tente pensar em — ou faça uma lista de — situações indesejáveis e imagine de que forma elas poderiam ocorrer. Então, pense em maneiras de evitar que aconteçam, ou de reconhecê-las e de responder a elas à medida que ocorrem. Essa é a essência da gestão proativa da segurança.

O caminho a seguir

A principal razão para justapormos a Segurança I e a Segurança II é a necessidade de chamar a atenção para as consequências de basearmos a gestão da segurança em uma ou em outra. As diferenças básicas estão resumidas na tabela abaixo.

	Segurança I	Segurança II
Definição de segurança	O número de coisas que dão errado é o mais baixo possível	O número de coisas que dão certo é o mais alto possível
Princípio de gestão da segurança	Reativo: responder a um acontecimento	Proativo: tentar antecipar os eventos e acontecimentos
Explicações para os acidentes	Os acidentes são causados por falhas e defeitos	Tudo acontece basicamente da mesma forma, independentemente do resultado
Como é enxergado o fator humano	Como um risco	Como um recurso

Nas situações cotidianas de trabalho, as pessoas costumam utilizar uma mistura de Segurança I e Segurança II. O equilíbrio preciso depende de muitos fatores, como a natureza do trabalho, a experiência dos profissionais, o clima organizacional, as pressões por parte dos administradores e clientes etc. Todos sabem que prevenir é melhor que remediar, mas as condições nem sempre conduzem a isso.

A situação é diferente quando falamos de níveis de gestão e atividades regulatórias. Neste caso, é evidente que a visão da Segurança I é preponderante, por razões já explicadas no início deste texto (o desequilíbrio pode também ser causado pelo fato de termos que escolher entre a eficiência e a meticulosidade: é muito mais simples contar os poucos eventos que dão errado do que os numerosos eventos que dão certo. Além disso, costumamos presumir — erroneamente — que é mais fácil explicar os primeiros do que os últimos).

Tendo em vista que os sistemas sociotécnicos dos quais depende a nossa existência continuam a se tornar cada vez mais complicados, parece claro que a manutenção de uma abordagem baseada na Segurança I será inadequada a longo prazo; e talvez já seja inadequada a curto prazo. Dessa forma, não deveria ser difícil tomar a decisão de adotar a abordagem da Segurança II. Ainda assim, o caminho a seguir não consiste numa substituição da Segurança I pela Segurança II, e sim numa combinação das duas formas de pensar. Ainda é verdade que a maior parte dos eventos adversos é relativamente simples — ou pode ser tratada como relativamente simples sem que isso tenha consequências graves — e que, portanto, pode ser abordada da maneira tradicional à qual estamos acostumados. No entanto, há um número crescente de casos nos quais essa abordagem não funciona. Nesses casos, é necessário adotar a perspectiva da Segurança II — o que, essencialmente, significa adotar a perspectiva da engenharia de resiliência. A Segurança II é, antes de tudo, uma maneira diferente de encararmos a segurança; portanto, é também uma maneira diferente de aplicarmos muitos dos métodos e técnicas que nos são familiares. Além disso, a Segurança II precisará de métodos próprios para examinar aquilo que dá certo, para analisar o funcionamento dos sistemas e para *gerir* a variabilidade de desempenho, em vez de apenas *restringi-la*.

Referências

Antonio, G. E., Griffith, J. F. & Ahuja, A. T. (2004). Aftermath of SARS. In A. T. Ahuja & C. G. C. Ooi (Eds.), *Imaging in SARS*. Cambridge University Press (P 159-164).

Hale, A. R. & Hovden, J. (1998). *Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment*. In A. M. Feyer & A. Williamson (Eds), Occupational Injury. Risk Prevention and Intervention. London: Taylor & Francis.

Harris, J. D. (1943). Habituatory response decrement in the intact organism. *Psychological Bulletin*. *40*, 385–422.

Hollnagel, E. (2011). *The ETTO principle. Efficiency-Thoroughness Trade-Off or why things that go right sometimes go wrong*. Farnham, UK: Ashgate.

Hollnagel, E. & Woods, D. D. (2005). *Joint cognitive systems: Foundations of cognitive systems engineering.* Boca Raton, FL: CRC Press.

Hollnagel, E. (Ed.) (2010). *Safer complex industrial environments*. Boca Raton, FL: CRC Press.

Hollnagel, E., Paries, J., Woods, D. D. & Wreathall, J. (Eds.) (2011). Resilience engineering in practice: A guidebook. Farnham, UK: Ashgate.

James, W. (1890). *The principles of psychology*. London: Macmillan and Co.

McIntyre, N. & Popper, K. (1983). The critical attitude in medicine: the need for a new ethics. British Medical Journal, 287, December 24-31, 1919-1923.

Melchers, R. E. (2001). On the ALARP approach to risk management. Reliability Engineering & System Safety, 71(2), 201–208.

Organisme d'Enquête pour les Accidents et Incidents Ferroviaires. (2012). *Rapport d'enquete de securité: La collision ferroviaire survenue le 15 fevrier 2010 a Buizingen.* Service public fédéral Mobilité et Transports: Bruxelles, Belgium.

Reason, J. (1979). Actions Not as Planned: The Price of Automatization. In G. Underwood & R. Stevens (Eds.) *Aspects of Consciousness. Vol. I, Psychological issues*. London: Academic Press.

Reason, J. T. (2008). *The human contribution*. Farnham, UK: Ashgate.

Thompson, R. F. & Spencer, W. A. (1966). Habituation: A model phenomenon for the study of neuronal substrates of behavior. *Psychological Review*, *73*(1), 16-43.

Wears, R. L. & Perry, S. J. (2006). Free fall - a case study of resilience, its degradation, and recovery, in an emergency department. Paper presented at the 2nd International Symposium on Resilience Engineering, Juan-les-Pins, France, http://www.resilienceengineering.org/REPapers/Wears_et_al.pdf