PROQUALIS

Da Segurança I à Segurança II: um relatório

Professor Erik Hollnagel
University of Southern Denmark, Institute for Regional Health Research (IRS), Dinamarca
Center for Quality, Region of Southern Denmark

Professor Robert L Wears
University of Florida Health Science Center Jacksonville, Estados Unidos

Professor Jeffrey Braithwaite
Australian Institute of Health Innovation, Macquarie University, Austrália

Ministério da Saúde
FIOCRUZ
Fundação Oswaldo Cruz

ICICT
Instituto de Comunicação e Informação Científica e Tecnológica em Saúde

Primeira publicação em 2015 pelos autores

Impresso e encadernado por:

National Library of Congress

Dados para catálogo em publicações:

Citação sugerida:

Hollnagel E., Wears R.L. e Braithwaite J. From Safety-I to Safety-II: A White Paper. The Resilient Health Care Net: Publicado simultaneamente pela University of Southern Denmark, Dinamarca, University of Florida, EUA, e Macquarie University, Austrália.

ISBN: Ainda não definido

Publicado pela University of Southern Denmark, Dinamarca, University of Florida, EUA, e Macquarie University, Austrália em 2015 com o título

From Safety-I to Safety-II: A White Paper

Este texto foi originalmente escrito em inglês. Os editores permitiram a tradução deste relatório e cedeu os direitos de publicação ao Proqualis/Instituto de Comunicação e Informação Científica e Tecnológica em Saúde/Fiocruz, único responsável pela edição em português.

Da Segurança I à Segurança II: um relatório

Coordenação Geral: Margareth Crisóstomo Portela

Revisão técnica: Victor Grabois

Revisão gramatical/Copydesk: Infotags Desenvolvimento em Informática Ltda ME

Edição Executiva: Alessandra dos Santos e Miguel Papi

Tradução: Diego Alfaro

Da Segurança I à Segurança II: um relatório

Sumário executivo

A publicação do relatório *To Err is Human* (Errar é humano) do IOM, em 2000, catalisou um interesse crescente pela melhoria de qualidade no cuidado de saúde. Ainda assim, apesar de décadas de atenção, atividade e investimento, as melhorias têm sido terrivelmente lentas. Embora as taxas de danos pareçam estáveis, o aumento na demanda por serviços de saúde e a crescente intensidade e complexidade desses serviços (as pessoas vivem cada vez mais, com comorbidades mais complexas, e esperam obter um cuidado mais avançado e de mais alto nível) implicam que o número de pacientes que sofrem danos durante o cuidado de saúde só vai aumentar, a menos que encontremos formas novas e mais eficazes de melhorar a segurança.

A maior parte das pessoas pensa na segurança como a ausência de acidentes e incidentes (ou como um nível de risco aceitável). Por essa perspectiva, que chamamos de Segurança I, a segurança é definida como um estado no qual o menor número possível de coisas dá errado. A abordagem da Segurança I presume que as coisas dão errado devido a falhas ou disfunções identificáveis em componentes específicos: tecnologia, procedimentos, trabalhadores e as organizações nas quais estão inseridos. Os seres humanos — sozinhos ou coletivamente — são, portanto, vistos como um risco ou perigo, principalmente porque são o mais variável desses componentes. O propósito da investigação de acidentes na Segurança I é identificar as causas e os fatores que contribuem para resultados negativos, e a avaliação de risco procura determinar sua probabilidade. O princípio da gestão da segurança é o de responder quando algo acontece ou quando algo é categorizado como um risco inaceitável, normalmente tentando eliminar suas causas ou melhorar as barreiras para impedi-los, ou ambos.

Essa visão da segurança popularizou-se em setores nos quais a segurança é um elemento crucial (nuclear, aviação etc.) entre as décadas de 1960 e 1980. Naquela época, a demanda por desempenho era significativamente menor que hoje e os sistemas eram mais simples e menos interdependentes.

Existia o pressuposto tácito de que os sistemas podiam ser decompostos e que os componentes de um sistema funcionavam de modo bimodal —isto é, seu funcionamento era correto ou incorreto. Esses pressupostos levaram à descrição detalhada e estável de sistemas, o que permitia buscar as causas dos defeitos e corrigi-los. Porém, tais pressupostos já não são válidos no mundo atual, nem na indústria nem no cuidado de saúde. No setor da saúde, sistemas como a terapia intensiva ou os serviços de emergência não podem ser decompostos de forma significativa e as funções não são bimodais, nem quando consideradas em detalhe, nem no sistema como um todo. Pelo contrário, o trabalho clínico cotidiano é, e deve ser, variável e flexível.

É fundamental observar que a visão da Segurança I não considera por que o desempenho humano praticamente sempre dá certo. As coisas não dão certo porque as pessoas agem como deveriam, mas porque as pessoas são capazes de ajustar, e efetivamente ajustam, aquilo que fazem, conforme as condições de trabalho. Com o desenvolvimento e o aumento da complexidade dos sistemas, esses ajustes tornam-se cada vez mais importantes para manter um desempenho aceitável. Dessa forma,o desafio para a melhoria da segurança consiste em compreender esses ajustes.Em outras palavras, compreender por que o desempenho geralmente dá certo, apesar das incertezas, ambiguidades e objetivos conflitantes que permeiam as situações de trabalho complexas. Apesar da importância óbvia de fazer com que as coisas deem certo, a gestão da segurança tradicional presta pouca atenção a isso.

A gestão da segurança deve, portanto, deixar de tentar assegurar que "o menor número possível de coisas dê errado" e passar a assegurar que "o maior número possível de coisas dê certo". Chamamos essa perspectiva de Segurança II.Ela está relacionada à capacidade de um sistema de funcionar corretamente sob condições variáveis. A abordagem da Segurança II presume que a variabilidade no desempenho cotidiano proporciona as adaptações necessárias para responder a condições variáveis, sendo, portanto, a razão pela qual as coisas dão certo. As pessoas são vistas, consequentemente, como um recurso necessário para a flexibilidade e a resiliência do sistema. Na Segurança II, o propósito da investigação passa a ser compreender por que as coisas normalmente dão certo, pois esta é a base para explicar por que as coisas às vezes dão errado. A avaliação de riscos procura compreender as condições nas quais a variabilidade no desempenho pode se tornar difícil ou impossível de monitorar e controlar. O princípio da gestão da segurança é facilitar o trabalho cotidiano, prever desenvolvimentos e eventos e manter a capacidade de adaptação para responder com eficácia às surpresas inevitáveis (Finkel, 2011).

Tendo em conta o aumento da demanda e da complexidade dos sistemas, devemos ajustar a nossa abordagem diante da segurança. Embora muitos eventos adversos ainda possam ser tratados pela abordagem da Segurança I sem consequências sérias, existe um número crescente de casos nos quais essa abordagem não funcionará, deixando-nos sem saber de que forma as ações cotidianas nos permitem atingir a segurança. Isso pode ter consequências inesperadas, pois degrada involuntariamente os recursos e os procedimentos necessários para fazer com que as coisas deem certo.

Portanto, o caminho a seguir depende da combinação das duas mentalidades. Embora possamos continuar a utilizar muitos dos métodos e técnicas existentes, a assimilação da visão da Segurança II também exigirá novas práticas, baseadas em examinar aquilo que dá certo, pôr o foco nos eventos frequentes, manter a sensibilidade para a possibilidade de falhas, encontrar um bom equilíbrio entre meticulosidade e eficiência e considerar o investimento em segurança como um investimento em produtividade. Este artigo ajuda a explicar as principais diferenças entre as duas formas de encarar a segurança e suas implicações.

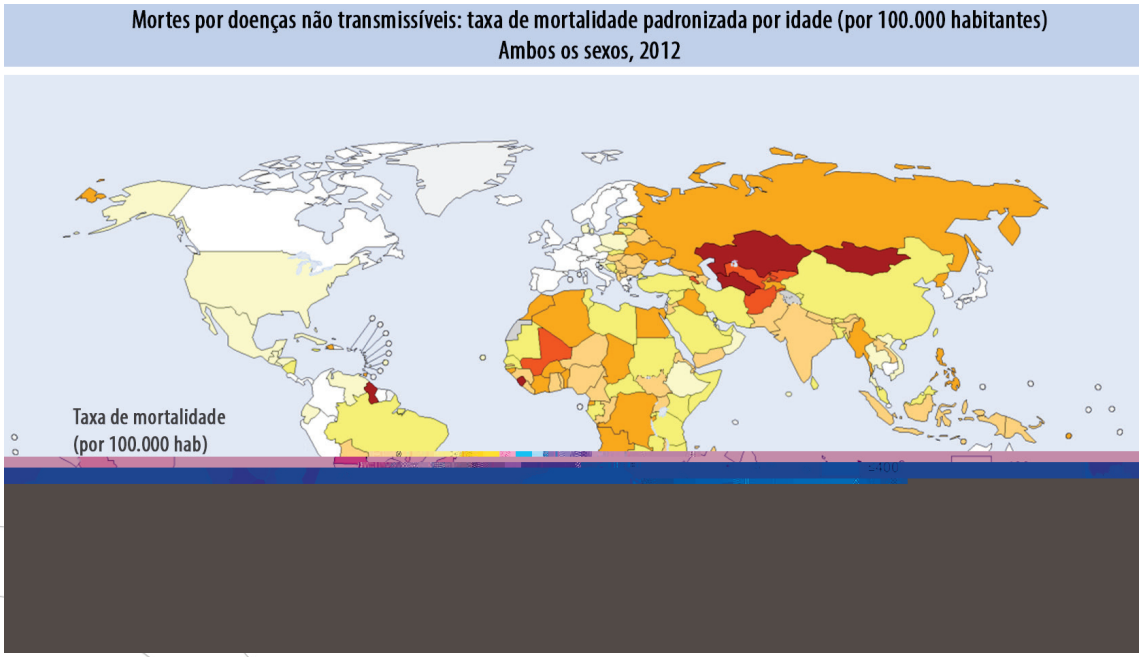
Contexto: o mundo mudou

Dizer que o mundo mudou não é só uma expressão vazia. A frase explica a intenção deste artigo e também serve para provocar a reflexão por parte do leitor.

Não há dúvidas de que o mundo em que vivemos se tornou mais complexo e interdependente e que esse desenvolvimento continua a se acelerar. Isso se aplica à forma como trabalhamos e vivemos no dia a dia. Essas mudanças talvez sejam mais evidentes na forma como nos comunicamos – a evolução dos telefones grandes e pesados para os elegantes *smartphones* e a passagem da interação pessoal frente a frente para as redes sociais e a mídia.

Nos últimos 40 anos, o cuidado de saúde passou por mudanças semelhantes. A Organização Mundial da Saúde (OMS) observa que, em todo o mundo, as doenças não transmissíveis (DNTs) tornaram-se as principais causas de mortalidade, em contraste com épocas anteriores.

As DNTs incluem doenças cardíacas, AVC, câncer, doenças respiratórias crônicas e diabetes. O mapa a seguir mostra as mortes causadas por doenças não transmissíveis em todo o mundo, por 100.000 habitantes, padronizadas por idade, entre 2000 e 2012. Essa epidemia representa uma enorme carga sobre os pacientes, suas famílias e comunidades. O número de consultas de emergência, consultas com médicos generalistas e internações gerais e em UTI para tratar essas doenças tem crescido internacionalmente, tanto em números absolutos como *per capita*. Essa tendência crescente não dá sinais de mudar em um futuro próximo. Ao mesmo tempo, surgem novas ameaças e surpresas (como Ebola, Marburg etc.) que se ramificam por todo o mundo, cada vez mais interconectado, de formas inesperadas e imprevisíveis.



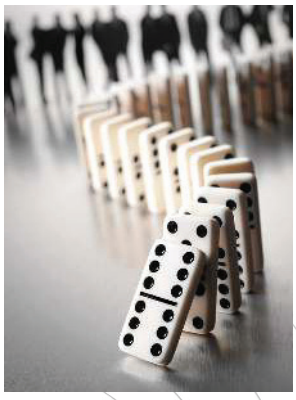
Fonte: OMS 2014, em
http://gamapserver.who.int/gho/interactive_charts/ncd/mortality/total/atlas.html

Como resposta, o uso de intervenções diagnósticas e terapêuticas de alta tecnologia (como exames de tomografia ou ressonância magnética, ultrassonografia, cirurgia minimamente invasiva, artroplastia e cirurgia cardíaca a céu aberto) deixou de ser experimental, restrito apenas a centros terciários ou quaternários para os casos mais difíceis, tornando-se um componente de rotina no arsenal dos principais hospitais de todo o mundo. O enorme número de pacientes e o ambiente sociotécnico cada vez mais complexo nos quais ocorre o cuidado de saúde constituem um desafio considerável para grupos de interesse, pacientes, profissionais de saúde, gestores, formuladores de políticas, reguladores e políticos.

O custo do cuidado de saúde associado a essa capacidade tecnológica tem crescido ainda mais rápido, a ponto de ser o maior componente individual do PIB na maioria dos países ocidentais e o que cresce mais rápido em praticamente todos os países. Por toda parte, essa taxa de crescimento tem sido considerada insustentável.

No início dessa revolução no cuidado de saúde, os eventos adversos eram considerados o preço lastimável, porém inevitável, a ser pago pelos avanços médicos. Assim, quando a segurança se tornou uma *cause célèbre* por volta do ano 2000, havia poucas abordagens estabelecidas para lidar com questões de segurança do paciente. A resposta óbvia foi adotar soluções aparentemente bem-sucedidas em outros setores. Essas soluções punham muita ênfase nas falhas em componentes, e o componente humano — o profissional de saúde — era considerado apenas mais um elemento falível. Assim, o modelo comum que embasou as primeiras iniciativas de segurança do paciente, e que se tornou a atual abordagem "ortodoxa" para a segurança do paciente, baseava-se em noções lineares de falhas em componentes individuais, do tipo "causa e efeito". Tal qual as doenças, que têm causas que podem ser diagnosticadas e

tratadas, os eventos adversos deveriam ter causas que pudessem ser identificadas e corrigidas. Modelos lineares simples, como o Modelo dos Dominós de Heinrich (1931), que está no cerne da Análise de Causa-Raiz, complementados posteriormente por modelos lineares compostos, como o Modelo do Queijo Suíço de Reason, foram logo adotados como as ferramentas básicas de segurança no cuidado de saúde. Poucos perceberam que os mesmos modelos estavam sendo cada vez mais contestados pela segurança industrial fora do cuidado de saúde, sendo considerados inadequados para os ambientes de trabalho mais novos e complexos.



Durante a segunda metade do século 20, o foco das iniciativas de segurança industrial passou dos problemas tecnológicos para os problemas em fatores humanos e, finalmente, para os problemas ligados às organizações e à cultura de segurança. Infelizmente, poucos dos modelos usados para analisar e explicar acidentes e falhas desenvolveram-se da mesma forma. Como resultado, o pensamento sobre a segurança e as práticas de segurança chegaram a um impasse, por várias razões. Esse foi o principal impulso para o desenvolvimento da engenharia da resiliência na primeira década deste século (p. ex., Hollnagel, Woods e Leveson, 2006). A engenharia da resiliência reconhece que o mundo se tornou mais complexo e que, por isso, as explicações para resultados indesejados no desempenho de um sistema não podem se limitar a uma compreensão das relações de causa e efeito descritas por modelos lineares.

Segurança I

Para a maior parte das pessoas, segurança significa a ausência de resultados indesejados, como incidentes ou acidentes. Como o termo “segurança” é usado e reconhecido por quase todos, supomos que as outras pessoas o entendem da mesma forma que nós e, portanto, raramente paramos para defini-lo com maior precisão. A finalidade deste artigo é fazer justamente isso e explorar as implicações das duas interpretações diferentes da segurança.

Em termos gerais, a segurança é definida como a qualidade necessária e suficiente de um sistema para assegurar que o número de eventos que podem causar danos a trabalhadores, ao público ou ao ambiente seja aceitavelmente baixo. A OMS, por exemplo, define segurança do paciente como “a prevenção de erros e efeitos adversos para os pacientes associados ao cuidado de saúde”.

Historicamente, o ponto de partida para as preocupações com a segurança foi a ocorrência de acidentes (resultados adversos efetivos) ou o reconhecimento de riscos (resultados adversos potenciais). Os resultados adversos (aquilo que dá errado) costumam ser explicados pela identificação de suas supostas causas, e a resposta consiste em eliminá-las ou contê-las. Da mesma forma, novos tipos de acidentes são explicados pela introdução de novos tipos de causas — que podem estar relacionadas à tecnologia (p. ex., fadiga de metais), aos fatores humanos (p. ex., carga de trabalho ou “erro humano”) ou à organização (p. ex., cultura de segurança).

Como essa abordagem tem sido eficaz na busca de soluções de curto prazo, ficamos tão acostumados a explicar acidentes em termos de relações de causa e efeito ao longo dos séculos que nem percebemos mais. E nos agarramos firmemente a essa tradição, embora seja cada vez mais difícil conciliá-la com a realidade. Infelizmente, a observação de deficiências em retrospecto não ajuda a explicar a geração ou a persistência dessas deficiências.

Para ilustrar as consequências do hábito de definir a segurança com base no que dá errado, considere a Figura 1. A linha vermelha representa o caso na qual a probabilidade (estatística) de uma falha é de 1 em 10.000. Mas isso também significa que as coisas deverão dar certo em 9.999 das 10.000 vezes — o que corresponde à área verde. No cuidado de saúde, a taxa de falhas está na ordem de alguns poucos pontos percentuais, chegando a 10 por cento em pacientes hospitalizados, dependendo do método de cálculo; mas o princípio é o mesmo: as coisas dão certo com muito mais frequência do que dão errado.

Figura 1: O desequilíbrio entre as coisas que dão certo e as que dão errado

O foco das iniciativas de Segurança I é aquilo que dá errado, e esse foco é reforçado de muitas formas. Reguladores e autoridades exigem relatórios detalhados sobre acidentes, incidentes e até mesmo sobre os chamados eventos inesperados, e agências especiais, departamentos e funcionários de organizações dedicam-se a investigar os resultados adversos. Inúmeros modelos alegam ser capazes de explicar por que as coisas dão errado, e são criados muitos métodos para encontrar o componente falho e corrigir as causas. Dados sobre eventos adversos e incidentes são coletados em grandes bancos de dados. Eventos adversos e incidentes são descritos e explicados em milhares de artigos e livros e debatidos em congressos nacionais e internacionais especializados. O resultado líquido é uma enxurrada de informações sobre as razões pelas quais as coisas dão errado e sobre o que pode ser feito para impedir que isso aconteça. A solução geral baseia-se em “encontrar e corrigir”:

procurar as falhas e defeitos, tentar encontrar suas causas e, então, eliminá-las ou introduzir barreiras, ou ambos.

A situação é bem diferente no caso dos eventos que dão certo. Apesar de sua importância crucial, eles normalmente recebem pouca atenção em atividades de gestão da segurança, como identificação de riscos, garantia de segurança e promoção da segurança. Não há exigências por parte das autoridades e dos reguladores para ver o que funciona bem e, portanto, poucas agências e departamentos dedicam-se a isso. Possíveis exceções são as auditorias e inquéritos, que podem incluir um foco nos pontos fortes, e a revisão ocasional de "boas notícias" por parte de políticos e CEOs para gerar matérias positivas na mídia. Contudo, no geral, é difícil encontrar os dados, existem poucos modelos, ainda menos métodos, e o vocabulário é escasso em comparação ao que é utilizado para aquilo que dá errado. Temos poucos livros e artigos e praticamente nenhuma reunião dedicada ao assunto. A prática de examinar aquilo que dá certo também entra em conflito com o tradicional foco nas falhas e, assim, é pouco estimulada. Isso cria um problema sério, pois não é possível assegurar que as coisas deem certo apenas impedindo que deem errado. Obviamente, também precisamos saber como as coisas dão certo.

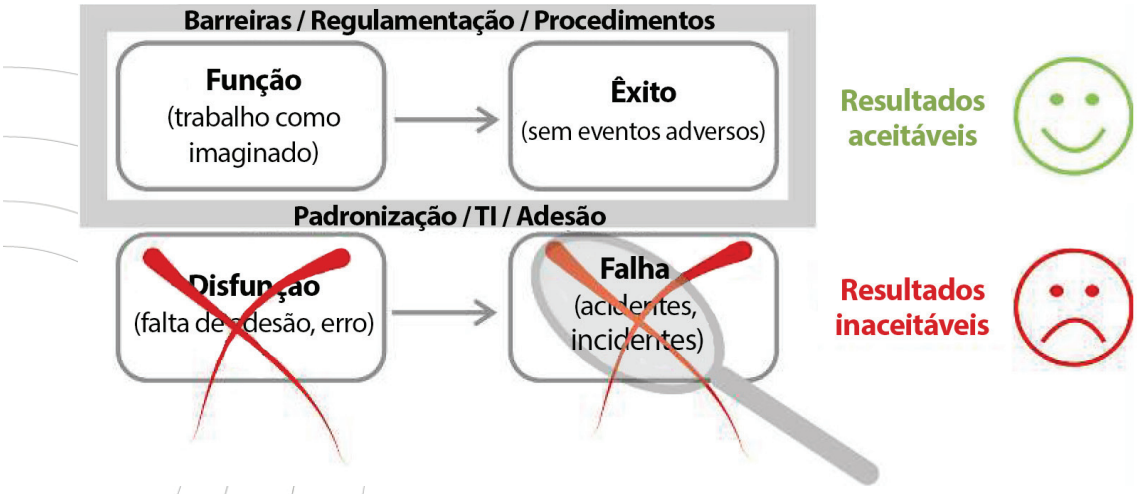
A Segurança I promove uma visão bimodal do trabalho e das atividades, na qual os resultados aceitáveis e adversos se devem a diferentes modos de funcionamento. Quando as coisas dão certo, é porque o sistema funciona como deveria e porque as pessoas trabalham como imaginado; quando dão errado, é porque algo funcionou mal ou falhou. Presume-se que os dois modos sejam distintamente diferentes, e o propósito da gestão da segurança, naturalmente, é assegurar que o sistema permaneça no primeiro modo e nunca se dirija para o segundo (Figura 2).

Figura 2: A segurança I pressupõe que as coisas que dão certo e as que dão errado ocorrem de forma diferente

Na Segurança I, o ponto de partida para a gestão da segurança é aquilo que dá errado ou que é identificado como um risco. Em ambos os casos é utilizada a abordagem "encontrar e corrigir": no primeiro caso, encontramos as causas e, então, desenvolvemos uma resposta adequada; no segundo, identificamos os perigos e procuramos eliminá-los ou contê-los. Outra solução é impedir a transição de um estado "normal" para um estado "anormal" (ou

defeito), não importando se isso se deve a uma transição repentina ou a um "desvio para a falha" gradual. Para isso, é preciso restringir o desempenho para mantê-lo no estado "normal", reforçando a adesão e eliminando a variabilidade (Figura 3). O passo final é verificar se o número de resultados adversos (infecções hospitalares, erros de medicação, falhas em dispositivos médicos etc.) diminui. Se diminuir, isso é tido como uma prova de que as iniciativas funcionaram como pretendido.

Avaliar a eficácia desse modo de segurança não é apenas sensato, mas também necessário. A seguir, vamos caracterizar a Segurança I observando suas manifestações (fenomenologia), seus mecanismos subjacentes (etiologia) e suas bases teóricas (ontologia).



Manifestações da Segurança I: examinando o que dá errado

Pela definição da Segurança I, as manifestações da segurança são os resultados adversos. Diz-se que um sistema (como uma clínica, uma farmácia, uma unidade de atendimento ou um hospital) não é seguro se os resultados adversos não forem apenas ocasionais, ou se o risco for visto como inaceitável. Da mesma forma, diz-se que um sistema é seguro se esses resultados ocorrerem raramente ou não ocorrerem, ou se o risco for visto como aceitável. Porém, esta é uma definição indireta, pois a segurança está sendo definida por seu oposto, pelo que acontece quando ela está ausente, e não quando está presente. Uma consequência curiosa é que analisamos e tentamos aprender com situações nas quais, por definição, existe uma falta de segurança.

Outra consequência curiosa é que o nível de segurança é inversamente proporcional ao número de resultados adversos. Se muitas coisas dão errado, diz-se que o nível de segurança é baixo; mas, se poucas coisas dão errado, diz-se que o nível de segurança é alto. Em outras palavras, quanto mais manifestações, menor a segurança, e vice-versa. Se o nível de segurança for perfeito, não existem resultados adversos; portanto, não há nada a medir. Isso, infelizmente, torna muito difícil, se não impossível, demonstrar que os esforços para melhorar a segurança funcionaram e, assim, é muito difícil defender a necessidade continuada de recursos.

Para ajudar a descrever as manifestações, existem várias tipologias de erros para os resultados adversos, que variam das mais simples (omissão-comissão) às mais elaboradas (várias formas de "erro cognitivo", violações ou falta de adesão). Observe que essas tipologias costumam ocultar uma confusão problemática entre erro como resultado (manifestação) e erro como causa.

Os "mecanismos" da Segurança I

Os mecanismos da Segurança I baseiam-se nos pressupostos sobre como as coisas acontecem, utilizados para explicar ou compreender as manifestações. O mecanismo genérico da Segurança I é a *crença na causalidade*, a crença predominante de que os resultados adversos (acidentes, incidentes) ocorrem porque algo deu errado, ou seja, eles têm causas que podem ser identificadas e tratadas. Embora seja obviamente razoável presumir que as consequências são precedidas por causas, é um erro supor que as causas são triviais ou que podem ser sempre identificadas.

A crença na causalidade, ao longo dos anos, tem sido expressa por muitos modelos diferentes para os acidentes. A versão mais forte da crença na causalidade é o pressuposto sobre as causas-raiz, expresso pela análise de causa-raiz. Embora esse pensamento linear simples provavelmente tenha sido adequado na primeira metade do século XX, os sistemas sociotécnicos cada vez mais complicados e intratáveis[1]que se desenvolveram na segunda metade do século, especialmente a partir da década de 1970, exigiram mecanismos mais intrincados e poderosos. O melhor deles é o Modelo do Queijo Suíço, que explica os resultados adversos como o resultado de uma combinação de falhas ativas e condições latentes. Outros exemplos são TRIPOD (Reason et al., 1989), AcciMap (Rasmussen e Svedung, 2000) e STAMP (Leveson, 2004). Ainda assim, em todos os casos, a crença na causalidade permite analisar o motivo de trás para frente, partindo das consequências para as causas subjacentes. Porém, como observou Reason (1997), "em nossas tentativas atuais, o pêndulo pode ter oscilado demais para a identificação de possíveis erros e fatores contribuintes de acidentes que estão amplamente separados, no tempo e no espaço, dos eventos em si". A crescente complexidade desses modelos levou à ideia, ligeiramente perversa, de que o "Modelo do Queijo Suíço passou da validade" (Reason, Hollnagel e Paries 2006).

As bases da Segurança I

As bases da Segurança I são os pressupostos sobre a natureza do mundo considerados necessários e suficientes para que os mecanismos funcionem. As bases da Segurança I implicam dois pressupostos importantes. O primeiro é a ideia de que os sistemas podem ser decompostos em seus componentes. O segundo é a ideia de que os sistemas e suas partes funcionam corretamente ou não — ou seja, são bimodais.

1 A definição de sistemas tratáveis [*tractable systems*] e de sistemas intratáveis [*intractable systems*] é apresentada pelos autores no glossário ao final do documento.

É possível decompor os sistemas

Sabemos que é possível construir sistemas reunindo diferentes elementos (por exemplo, instrumentos complicados como uma máquina de tomografia computadorizada ou um robô-cirurgião, ou sistemas sociotécnicos complicados como um hospital cheio de pessoas e equipamentos) e combinando e organizando cuidadosamente seus componentes. É assim que normalmente criamos sistemas.

O primeiro pressuposto é que esse processo pode ser revertido e que podemos entender os sistemas decompondo-os em partes significativas (Figura 4). Somos relativamente bem-sucedidos quando decompomos sistemas tecnológicos para encontrar as causas de acidentes — falhas em dispositivos médicos num centro cirúrgico, por exemplo. Também pressupomos que é possível decompor os sistemas "soft" (pessoas em organizações) em seus componentes (departamentos, agentes, papéis, *stakeholders*, grupos, equipes). Finalmente, pressupomos que o mesmo pode ser feito no caso das tarefas e eventos, em parte devido à sedutora simplicidade da cronologia (este evento aconteceu depois daquele; portanto, o primeiro evento "causou" o segundo). Porém, em todos os casos, estamos errados.

O funcionamento é bimodal

Também pressupomos que os "componentes" de um sistema podem estar em um dentre dois estados, funcionando corretamente ou não (disfunção) — um pressuposto que, às vezes, é incrementado com a inclusão de vários modos de operação degradados. Os componentes de um sistema geralmente são projetados ou desenvolvidos para desempenhar uma função específica; quando isso não acontece, dizemos que eles falharam, apresentaram uma disfunção ou se degradaram. Embora esse raciocínio seja válido no caso dos sistemas tecnológicos e seus componentes, não é válido para os sistemas sociotécnicos — e certamente não é válido no caso dos componentes humanos e organizacionais, a tal ponto que nem sequer faz sentido utilizá-lo.

Embora os dois pressupostos (decomponibilidade e bimodalidade) tornem mais conveniente a busca por causas e por uma resposta para "corrigi-los", eles também levam a descrições de sistemas cuja rastreabilidade e especificidade são ilusórias, e a ilusões sobre a precisão das quantificações. Portanto, são insuficientes como uma base para a gestão da segurança no mundo atual.

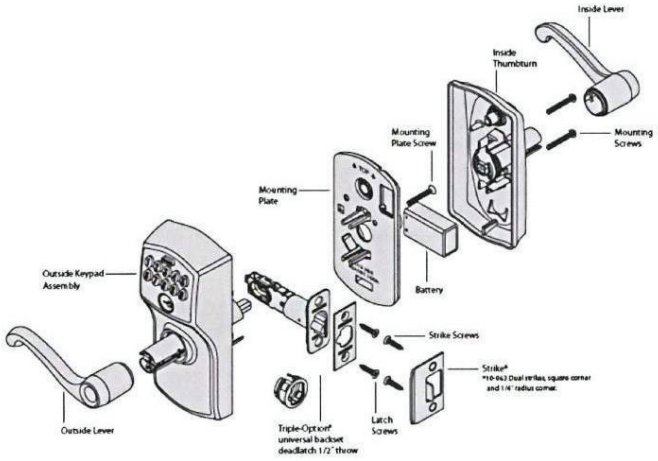


Figura 4: Um sistema decomponível

Cuidado de saúde: um mundo em mutação

As demandas sempre mutáveis no trabalho, na segurança e na produtividade

A Segurança I baseia-se numa visão de segurança desenvolvida aproximadamente entre 1965 e 1985 na área da segurança industrial e importada para a segurança do paciente anos depois. Os sistemas industriais dos anos 70 eram relativamente simples quando comparados ao mundo atual. A dependência da tecnologia da informação era limitada (principalmente devido à dimensão e à imaturidade da própria TI), o que significava que as funções de suporte eram relativamente escassas, relativamente simples e, principalmente, independentes umas das outras. O nível de integração (por exemplo, entre subsistemas e setores) era baixo e, geralmente, era possível entender e acompanhar o que acontecia. Os sistemas de suporte eram pouco conectados (independentes), em vez de fortemente conectados (interdependentes). A concepção de segurança, portanto, desenvolveu-se com base nos seguintes pressupostos:

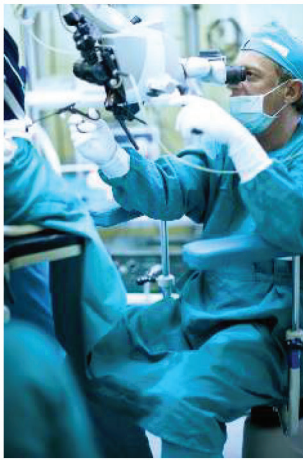
- Os sistemas e locais de trabalho são bem projetados e mantidos corretamente.
- Os procedimentos são abrangentes, completos e corretos.
- As pessoas ao final do processo (no setor da saúde, os profissionais na linha de frente do cuidado) comportam-se como esperado e conforme o treinamento recebido (trabalham como supõe-se ou imagina-se que devam trabalhar).
- Os projetistas previram todas as contingências e capacitaram o sistema com recursos de resposta apropriados. Se as coisas derem completamente errado, os sistemas podem se degradar de forma harmônica, pois os profissionais, ao final do processo, conseguem compreender e gerenciar as contingências, mesmo aquelas que os projetistas não previram.

Embora esses pressupostos nunca tenham sido completamente corretos, eram considerados razoáveis na década de 1970. Porém, não são razoáveis hoje e a segurança baseada nessas premissas é inadequada para o mundo da década atual.

O cuidado de saúde tem adotado esses pressupostos de forma pouco crítica desde a década de 1990, embora o cuidado de saúde daquela década tivesse poucas semelhanças com os ambientes industriais da década de 1970. A situação não melhorou de forma alguma se considerarmos que o cuidado de saúde em 2015 é amplamente diferente do de 1990. Apesar disso, ainda encontramos esses pressupostos na base das atuais iniciativas de segurança do paciente.

Década de 1970

Década de 1990



Hoje

Amplo desenvolvimento tecnológico

Como a maioria dos setores, o cuidado de saúde está sujeito a um *tsunami* de mudanças e melhorias diversas. Algumas mudanças vêm de tentativas bem-intencionadas de substituir os humanos "falíveis" pela tecnologia "infalível", enquanto outras são uma resposta às crescentes demandas por desempenho ou conveniência política. Na maioria dos países, os governos nacionais definiram metas de segurança ambiciosas sem considerar muito se as metas eram significativas ou até mesmo possíveis na prática. Nos Estados Unidos, por exemplo, o Presidente Clinton endossou a meta do IOM para 2000 de redução de 50% nos erros em cinco anos, dizendo que qualquer redução abaixo disso seria irresponsável. (Essas metas de segurança também levantam uma questão interessante: é possível medir um aumento na segurança contando a diminuição dos casos em que as coisas dão errado?)

Outra tendência perturbadora é o número crescente de casos nos quais os problemas são selecionados com base em apenas um critério: se podem ser "resolvidos" com uma solução tecnológica boa e simples à nossa disposição. Isso tem duas consequências principais. A primeira é que os problemas são abordados e resolvidos um a um, como se fosse possível lidar com eles isoladamente. A segunda é que a solução preferencial é tecnológica, e não sociotécnica, provavelmente porque soluções não técnicas raramente são "boas e simples".

O resultado dessa evolução é que, atualmente, poucas atividades são independentes entre si — no cuidado de saúde e em outros setores —, e essas dependências mútuas só

tendem a crescer. As funções, os propósitos e os serviços já estão fortemente conectados, e essas conexões só ficarão mais fortes. Considere, por exemplo, as principais áreas de ação da OMS para a segurança do paciente: higienização das mãos e segurança cirúrgica usando listas de verificação, além de outras que envolvem sistemas de notificação e aprendizado, implementação de "soluções", divulgação de modelos de mudança baseados em melhores práticas ("High 5s"), gestão de conhecimento, eliminação de infecções associadas a cateteres centrais e desenvolvimento e implementação de novas listas de verificação. Embora todas essas metas possam parecer plausíveis, se procurarmos atingi-las como estratégias individuais, corremos o risco de nos deparar com consequências inesperadas. Uma mudança num desses fatores afetará os outros de formas não triviais, não necessariamente salutares e, portanto, difíceis de compreender. Isso entra em conflito com os pressupostos da Segurança I, o que significa que qualquer solução baseada na mentalidade da Segurança I poderá piorar as coisas.

Em consequência do desenvolvimento tecnológico desenfreado, da fé generalizada em soluções tecnológicas boas e simples e da falta de vontade geral de sermos suficientemente meticulosos no início para sermos eficientes depois, precisamos rever nossas ideias sobre a natureza do trabalho e da segurança. Devemos aceitar que, atualmente, os sistemas são cada vez mais intratáveis. Isso significa que os princípios de funcionamento só são conhecidos em parte (ou, num número crescente de casos, são completamente desconhecidos), que as descrições são elaboradas com muitos detalhes e que é provável que os sistemas mudem antes que as descrições sejam concluídas, o que significa que as descrições estarão sempre incompletas.

Como consequência, a previsibilidade é limitada durante o *design* e a operação, e é impossível prescrever ou mesmo descrever com precisão a forma como o trabalho deve ser feito.

Os sistemas tecnológicos podem ter funcionamento autônomo, desde que seu ambiente esteja completamente especificado e que não haja variabilidade inesperada. Mas não é possível estabelecer essas condições no caso dos sistemas sociotécnicos. De fato, para que a tecnologia funcione, as pessoas (e organizações) devem trabalhar de modo a amortecer o excesso de variabilidade. As pessoas não são um problema a ser resolvido ou padronizado: elas são a solução adaptável.

As razões pelas quais as coisas funcionam – mais uma vez

Como os atuais sistemas de saúde são cada vez mais intratáveis, é impossível descrevê-los de forma completa ou especificar o que os profissionais que lidam diretamente com o paciente devem fazer até mesmo nas situações comuns. Como o desempenho não pode ser prescrito completamente, é necessário algum grau de variabilidade, flexibilidade ou adaptabilidade para que o sistema funcione. As pessoas que contribuem com esses ajustes inteligentes são, dessa forma, um recurso sem o qual o funcionamento adequado seria impossível.

Os ajustes e a variabilidade no desempenho são, portanto, normais e necessários e são a razão tanto para os resultados aceitáveis como para os inaceitáveis. Tentar atingir a segurança restringindo a variabilidade no desempenho também afetará, inevitavelmente, a capacidade de atingir os resultados desejados; logo, esta ação é contraproducente. Por exemplo, padronizar abordagens insistindo que uma diretriz clínica — com todas as suas cinquenta ou mais páginas — sobre uma queixa médica comum, como dor de cabeça ou asma, seja lida e adotada integralmente, sem questionamentos, em todas as ocasiões nas quais um paciente com essa condição clínica se apresentar ao departamento de emergência não é apenas impossível, como também quase não deixa tempo para que o cuidado em si seja prestado.

Da mesma forma, implementar mais de 2000 políticas do Ministério da Saúde (número que está tecnicamente em operação em alguns sistemas de saúde públicos) e afirmar que elas devem ser usadas continuamente para guiar o trabalho cotidiano das pessoas causaria uma pane no sistema. Assim, em vez de procurar as maneiras pelas quais podem surgir falhas e disfunções e documentar procedimentos detalhados, devemos tentar entender as características da variabilidade no desempenho diário.

Trabalho imaginado e trabalho realizado

Existe um pressuposto implícito de que o trabalho pode ser completamente analisado e prescrito e que, dessa forma, o trabalho imaginado corresponderá ao trabalho realizado. Porém, o trabalho imaginado é uma visão idealizada do ambiente formal de cada tarefa, que não considera como a execução da tarefa deve ser ajustada para corresponder às condições, sempre variáveis, do trabalho e do mundo. O trabalho imaginado descreve o que deve acontecer nas condições normais de trabalho. O trabalho realizado, por outro lado, descreve o que efetivamente acontece, a forma como o trabalho decorre ao longo do tempo em contextos complexos.

Uma razão para a popularidade do conceito do trabalho imaginado é o êxito incontestável da Teoria da Administração Científica (Taylor, 1911). Introduzida no início do século XX, a administração científica estabeleceu, já na década de 1930, estudos de tempo e movimento como uma técnica prática e demonstrou que a decomposição de tarefas e atividades poderia ser usada para melhorar a eficiência do trabalho, culminando nas linhas de produção industriais.

A administração científica usava estudos de tempo e movimento, combinados a análise e síntese racional, para determinar o melhor método para realizar qualquer tarefa específica que os trabalhadores poderiam ser induzidos a executar. Dessa forma, a administração científica proporcionou o fundamento teórico e prático para a noção de que o trabalho imaginado era uma base necessária e suficiente para o trabalho realizado (porém, a administração científica não tinha preocupações ligadas à segurança). Isso teve consequências sobre a forma de estudar os eventos adversos e de melhorar a segurança. Os eventos adversos poderiam ser compreendidos a partir da observação dos componentes, a fim de encontrar os que haviam

falhado, como na análise de causa-raiz. E a segurança poderia ser melhorada pelo planejamento cuidadoso do trabalho, em conjunto com instruções detalhadas e treinamento. Podemos encontrar essas crenças nos princípios ligados à eficácia dos procedimentos e na ênfase em assegurar a conformidade. Em resumo, a segurança pode ser atingida assegurando-se que o trabalho realizado seja idêntico ao trabalho imaginado.

Porém, nos ambientes mais intratáveis que temos hoje, o trabalho realizado difere significativamente do trabalho imaginado. Como o trabalho realizado, por definição, reflete a realidade com a qual as pessoas precisam lidar, a conclusão inevitável é que nossas noções sobre o trabalho imaginado são inadequadas, se não totalmente erradas. Isso representa um problema para os modelos e métodos que compõem o pensamento predominante da engenharia da segurança, dos fatores humanos e da ergonomia, e também desafia a autoridade gerencial tradicional. Uma implicação prática disso é que só poderemos melhorar a segurança se sairmos de nossos escritórios e salas de reuniões e entrarmos nos ambientes operacionais e clínicos junto aos profissionais dessas áreas.

Os ambientes de trabalho atuais exigem que examinemos o trabalho clínico cotidiano e o trabalho realizado, e não o trabalho imaginado; portanto, devemos procurar examinar sistemas reais, e não ideais (Wears, Hollnagel e Braithwaite, 2015). O desempenho desses sistemas é confiável porque as pessoas são flexíveis e adaptáveis, e não porque os sistemas foram concebidos e projetados à perfeição ou porque as pessoas fazem exatamente o que foi prescrito.

Dessa forma, os seres humanos deixam de representar um risco e a variabilidade no desempenho deixa de ser uma ameaça. Pelo contrário, a variabilidade no desempenho cotidiano é necessária para que o sistema funcione, sendo a razão tanto para os resultados aceitáveis como para os adversos. Como todos os resultados dependem da variabilidade no desempenho, não é possível prevenir as falhas eliminando a variabilidade. Em outras palavras, não é possível administrar a segurança impondo restrições ao trabalho normal.

A maneira como pensamos a segurança deve corresponder ao trabalho realizado, e não depender do trabalho imaginado. A Segurança I começa perguntando por que as coisas dão errado e depois tenta encontrar as supostas causas para garantir que não aconteçam novamente — ela tenta restabelecer o trabalho imaginado. A alternativa é perguntar por que as coisas dão certo (e por que nada deu errado) e depois tentar assegurar que isso aconteça novamente.

Segurança II

No curso normal do trabalho clínico, o desempenho de médicos, enfermeiros e outros profissionais de saúde é seguro porque eles conseguem ajustar seu trabalho de forma a corresponder às condições existentes. Em sistemas tratáveis e bem projetados (como na aviação, na mineração, nas fábricas e também na produção farmacêutica) a necessidade de ajustes é menor. Em muitos casos, também existe a opção de adiar ou atrasar operações quando as cir-

cunstâncias se tornam desfavoráveis, como nos casos em que os voos são cancelados devido ao clima, ou quando um problema mecânico causa o fechamento temporário de uma empresa. Às vezes, todo um sistema pode ser fechado, como aconteceu depois dos ataques de 11 de setembro de 2001 nos EUA, ou quando o vulcão Eyjafjällajökull entrou em erupção na Islândia em abril e maio de 2010.

O cuidado de saúde, por sua própria natureza, costuma ser intratável, o que significa que são necessários ajustes no desempenho para que o sistema funcione. Em muitas situações no cuidado de saúde, a precariedade das circunstâncias também não permite adiar ou atrasar o tratamento dos pacientes, mesmo se as condições de trabalho forem ruins (Wears e Perry, 2006).

Dada a incerteza, a intratabilidade e a complexidade do trabalho no cuidado de saúde, a surpresa não é que as coisas ocasionalmente deem errado, e sim que deem certo com tanta frequência. Ainda assim, como vimos, quando tentamos gerir a segurança, concentramo-nos nos poucos casos que dão errado, e não nos muitos que dão certo. Porém, a investigação dos casos raros de falhas atribuídas a “erros humanos” não explica por que o desempenho humano quase sempre dá certo nem como isso ajuda a cumprir as metas do cuidado de saúde. O foco na falta de segurança não nos mostra em que direção devemos seguir para melhorar a segurança.

A solução é surpreendentemente simples: em vez de observar os poucos casos nos quais as coisas dão errado, devemos observar os muitos casos nos quais as coisas dão certo e tentar entender como isso acontece. Devemos reconhecer que as coisas dão certo porque os profissionais de saúde conseguem ajustar seu trabalho às condições existentes, e não porque eles trabalham conforme imaginado. A engenharia da resiliência reconhece que os resultados aceitáveis e os resultados adversos têm uma base comum: os ajustes no desempenho cotidiano (Figura 5).

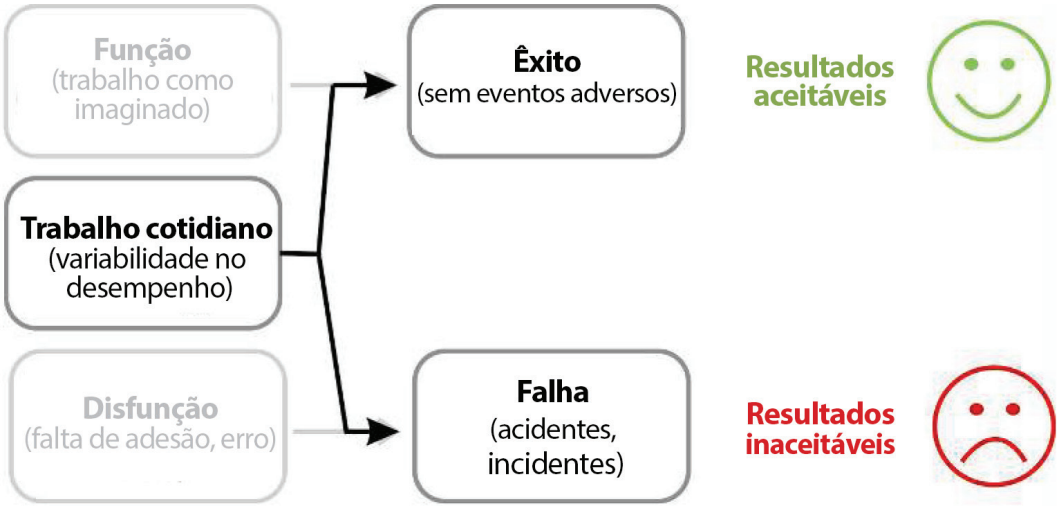


Figura 5: As coisas que dão certo e as que dão errado acontecem da mesma forma.

Como muitas das situações de trabalho atuais são intratáveis, é impossível prescrever o que deve ser feito em qualquer nível de detalhe, exceto nas situações mais triviais. A razão pela qual, apesar disso, as pessoas conseguem trabalhar com eficiência é que elas ajustam continuamente seu trabalho às condições atuais — incluindo aquilo que as outras pessoas fazem ou provavelmente farão. Com a contínua expansão horizontal e vertical dos sistemas de saúde e sua crescente intratabilidade, esses ajustes tornam-se cada vez mais importantes para que o desempenho seja eficaz e, portanto, representam tanto um desafio como uma oportunidade para a gestão da segurança.

Segundo essa visão, devemos evitar tratar as falhas como eventos únicos e individuais; em vez disso, devemos vê-las como uma expressão da variabilidade no desempenho cotidiano. Excluindo-se as atividades excepcionais, é seguro dizer que algo que dá errado dará certo muitas vezes antes — e dará certo muitas outras vezes no futuro. Compreender como ocorrem os resultados aceitáveis é a base necessária para compreender como ocorrem os resultados adversos. Em outras palavras, quando algo dá errado, o primeiro passo é compreender como (nos outros casos) costuma dar certo, em vez de procurar causas específicas que expliquem apenas a falha (Figura 6). Os resultados adversos devem-se, com mais frequência, a combinações de variabilidade conhecida no desempenho, normalmente consideradas irrelevantes para a segurança, do que a falhas e disfunções distintas.

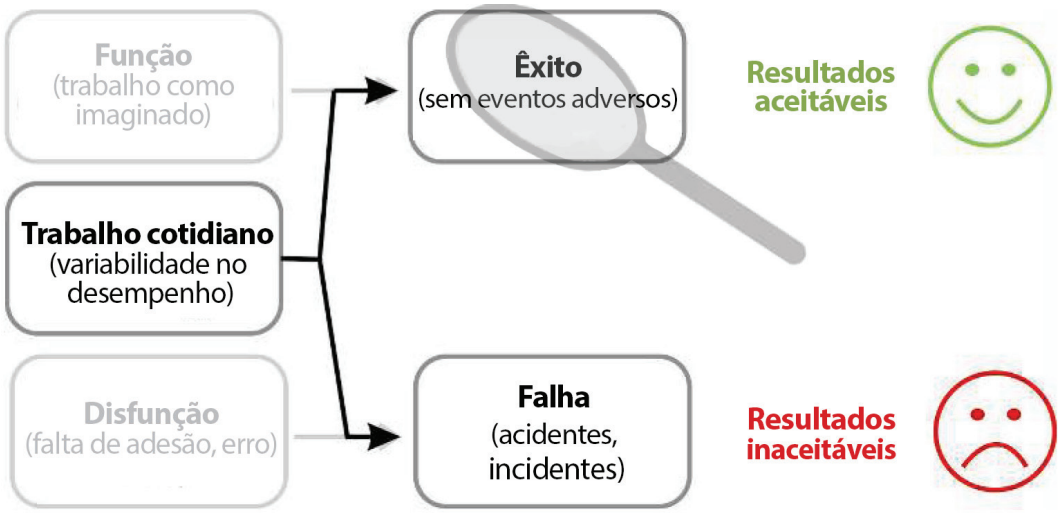


Figura 6: A base para a segurança é compreender a variabilidade no desempenho cotidiano.

As situações de trabalho são cada vez mais intratáveis, apesar de nossas melhores intenções no sentido contrário. Um dos motivos para isso é, ironicamente, nossa capacidade limitada de prever as consequências de mudanças no *design*ou de outras intervenções — tanto as consequências esperadas como os efeitos colaterais inesperados. Esse problema foi abordado há muitos anos numa discussão sobre automação, na qual Bainbridge (1983) destacou que "o projetista que tenta eliminar o operador ainda deixa o operador executar as tarefas que o projetista não conseguiu automatizar". Esse argumento aplica-se não apenas a projetos de automação, mas também a especificações de trabalho e ao *design* de locais de trabalho no cuidado de saúde em geral. Quanto mais complicada for uma situação de trabalho, maior será a incerteza em relação aos detalhes. E o trabalho clínico é incrivelmente complexo, exigindo altos níveis de avaliação pessoal e julgamento profissional para adaptar o cuidado às circunstâncias de pacientes com múltiplas morbidades.

Assim, as premissas para a gestão da segurança nos complexos ambientes de cuidado atuais podem ser resumidas da seguinte forma:

- Os sistemas e o trabalho clínico não podem ser decompostos de maneira significativa (não existem "elementos" ou "componentes" naturais).
- As funções de um sistema não são bimodais, separadas em "funcionais" ou "disfuncionais", mas o desempenho cotidiano é — e deve ser — flexível e variável.
- Os resultados surgem a partir da variabilidade no desempenho humano, que é a origem tanto dos resultados aceitáveis como dos adversos.
- Embora alguns resultados adversos possam ser atribuídos a falhas e defeitos, outros são mais bem compreendidos como o resultado de combinações na variabilidade do desempenho.

Como consequência, a definição de segurança deve ser alterada de “evitar que algo dê errado” para “assegurar que tudo dê certo”. A segurança II é a capacidade do sistema de funcionar conforme necessário em condições variáveis, de forma que o número de resultados pretendidos e aceitáveis (em outras palavras, de atividades cotidianas) seja o maior possível. A base para a segurança e para a gestão da segurança deve ser, portanto, a compreensão das razões pelas quais as coisas dão certo, isto é, a compreensão das atividades cotidianas.

A tarefa de assegurar que o máximo possível de coisas dê certo, ou seja, que o trabalho clínico cotidiano cumpra seus objetivos definidos, não pode depender das respostas diante de falhas, pois isso só vai corrigir o que já aconteceu. A gestão da segurança também deve ser proativa. As intervenções devem ser feitas antes que algo aconteça, de modo a afetar ou até mesmo impedir sua ocorrência. Uma grande vantagem dessa abordagem é que as respostas precoces, em geral, exigem um esforço menor, pois as consequências do evento terão menos tempo para desenvolver-se e difundir-se. Além disso, respostas precoces podem, obviamente, poupar um tempo precioso.

A seguir, caracterizaremos a Segurança II em mais detalhes. Analisaremos primeiro suas bases teóricas, depois seus mecanismos subjacentes e, finalmente, suas manifestações.

As bases da Segurança II: variabilidade no desempenho, em vez de bimodalidade

Ao contrário da Segurança I, a Segurança II baseia-se no princípio de que os ajustes no desempenho são corriqueiros e que o desempenho *é* sempre variável, e *deve* ser assim. Isso significa que é impossível, além de não fazer sentido, caracterizar os componentes com base em êxito ou fracasso, ou em função e disfunção. É importante que a variabilidade não seja interpretada negativamente, como um “desvio de desempenho”, uma “violação” ou uma “falta de adesão”. Pelo contrário, a capacidade de ajustar o desempenho é uma contribuição humana essencial ao trabalho, sem a qual apenas a mais trivial das atividades seria possível.

Os “mecanismos” da Segurança II: emergência, em vez de causalidade

Como os ajustes e a variabilidade no desempenho constituem a base da Segurança II, deduz-se que os mecanismos não podem depender da causalidade nem de propagações lineares de causas e efeitos. Embora ainda seja comum atribuir a maior parte dos resultados adversos a falhas ou disfunções em componentes e funções normais do sistema, existe um número crescente de casos nos quais isso não é possível. Nesses casos, diz-se que o resultado é emergente, em vez de resultante. Isso não torna impossível explicar o que aconteceu; porém, a explicação terá uma natureza diferente. O significado de emergência não é algo que acontece “magicamente”, e sim algo que acontece de uma maneira que não pode ser explicada com base nos princípios de decomposição e causalidade. Isso tende a ocorrer nos sistemas que são parcial ou inteiramente intratáveis.

Para explicar como algo aconteceu, costumamos reconstituir o evento desde o efeito até a causa, até atingirmos a causa básica — ou ficarmos sem tempo e dinheiro. Isso pode ser ilustrado por uma representação como o diagrama de espinha de peixe da Figura 7.

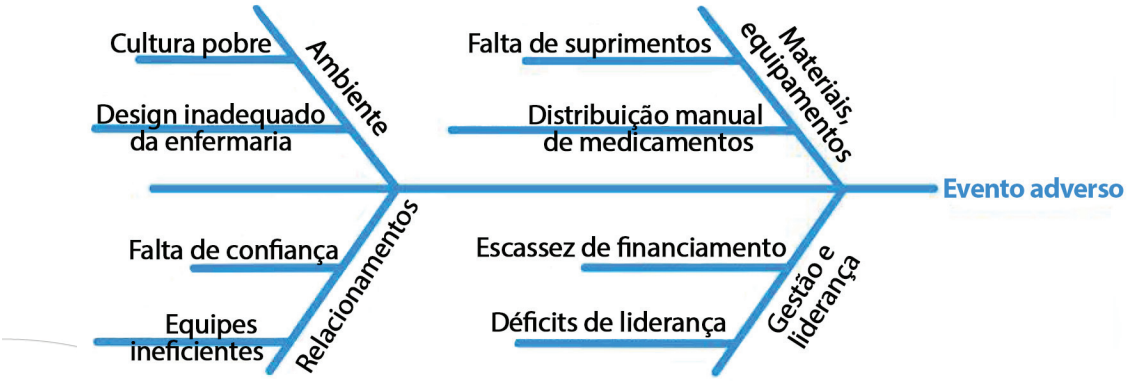


Figura 7: Diagrama de espinha de peixe usando a lógica linear para rastrear um evento adverso.

Quando algo dá errado, ocorre uma mudança observável (caso contrário, não teríamos como saber que algo aconteceu). O resultado pode ser uma cirurgia em local errado, uma infecção cirúrgica ou uma falha no diagnóstico. A Segurança I pressupõe que as causas são reais e que o propósito da investigação de acidentes e incidentes é rastrear a origem dos acontecimentos desde o resultado observável até a causa eficiente. As causas também são "reais", no sentido de que podem ser associadas a componentes ou funções que, de alguma forma, "falharam", onde a "falha" é visível após o fato ou pode ser deduzida a partir dos fatos. Da mesma forma, a avaliação de risco projeta os acontecimentos futuros, desde as causas eficientes até os possíveis resultados. Em geral, começa-se com uma base de dados sobre incidentes e avalia-se o risco de que outro evento semelhante venha a acontecer.

Nos processos emergentes, é evidente que os resultados (finais) verificados também são observáveis ou "reais", mas não podemos necessariamente dizer o mesmo em relação às suas causas. Os resultados podem, por exemplo, dever-se a condições ou fenômenos temporários que existiram apenas num determinado ponto no tempo e no espaço. O enfermeiro teve uma dor de cabeça, a filha do médico ia se casar e todos estavam comemorando, ou as políticas locais eram antagônicas naquele dia porque dois departamentos vizinhos estavam discutindo a alocação de recursos. Essas condições, por sua vez, podem ter surgido de outros fenômenos temporários (Figura 8). Assim, as "causas" são reconstruídas (ou inferidas), e não encontradas. Dessa forma, talvez seja impossível eliminá-las ou contê-las da maneira habitual, mas talvez ainda seja possível controlar as condições que determinaram sua existência se conseguirmos entender como o trabalho é feito normalmente.

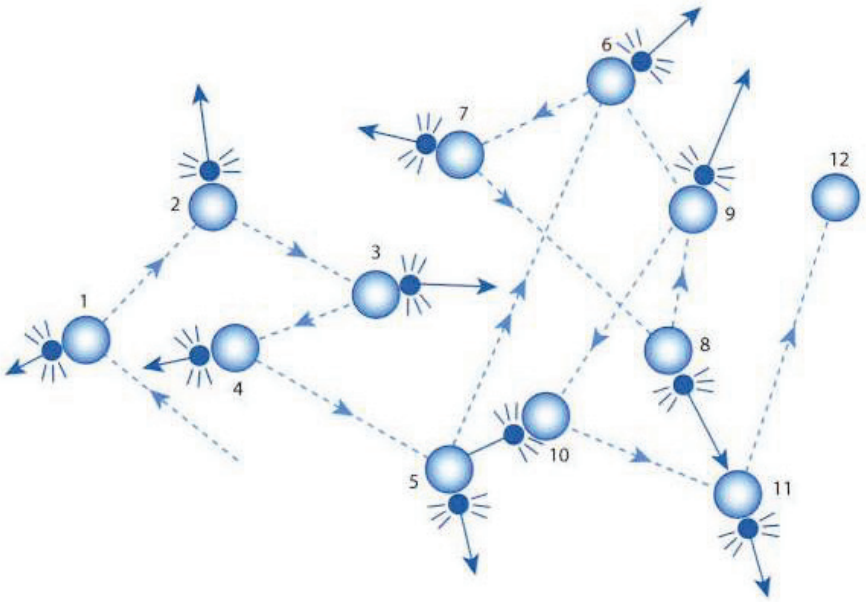


Figura 8: Fenômenos temporários e emergência.

As manifestações da Segurança II: as coisas que dão certo

Pela definição da Segurança II, as manifestações são todos os resultados possíveis, como ilustrado na Figura 9, e especialmente os resultados típicos ou de alta frequência que costumam ser ignorados pela gestão da segurança. Um sistema ainda é considerado inseguro se ocorrerem resultados adversos, mas é mais importante compreender por que o sistema é seguro quando tais resultados não ocorrem: a segurança é, consequentemente, definida pelo que acontece quando ela está presente, e não pelo que acontece quando está ausente; portanto, está diretamente relacionada aos resultados aceitáveis de alta frequência. Em outras palavras, quanto mais destas manifestações existirem, maior é o nível de segurança e vice-versa. Com isso é possível demonstrar que os esforços para melhorar a segurança funcionaram e, assim, é mais fácil defender a necessidade continuada de recursos (isso também resolve o possível conflito entre segurança e produtividade, mas essa é uma outra discussão).

Existem poucas tipologias disponíveis para descrever as manifestações da Segurança II. Embora as coisas costumem dar certo o tempo todo, não percebemos porque nos acostumamos com isso. Psicologicamente, não as valorizamos. Porém, como o desempenho cotidiano é corriqueiro, ele pode ser explicado em termos relativamente simples. Por exemplo, o desempenho cotidiano pode ser descrito como os ajustes no desempenho que servem para criar ou manter as condições de trabalho necessárias para compensar a falta de tempo, materiais, informações etc., a fim de evitar condições sabidamente prejudiciais ao trabalho. Além disso, como a variabilidade no desempenho cotidiano é corriqueira, é mais fácil monitorá-la e gerenciá-la.

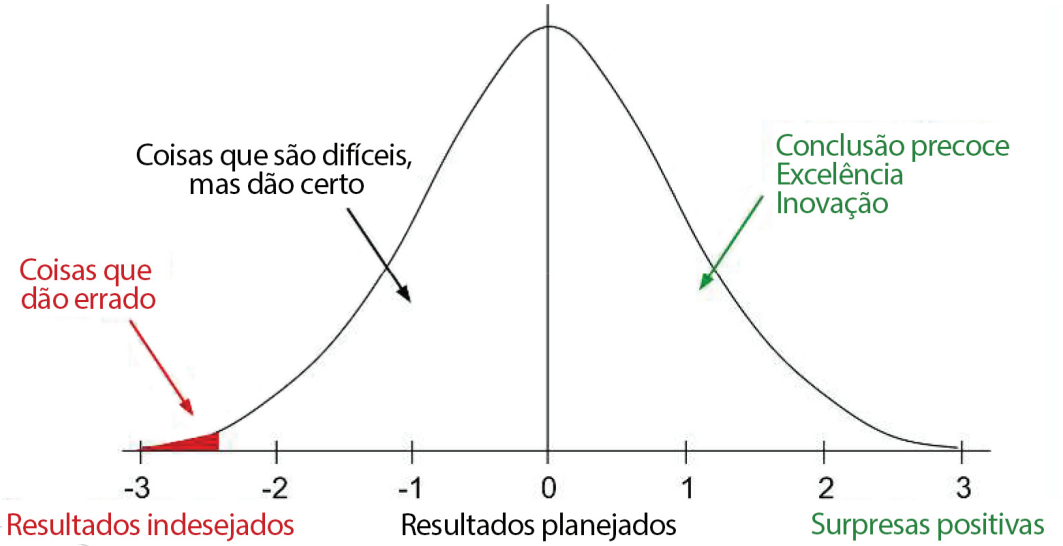


Figura 9: Probabilidade de eventos e foco na segurança.

O caminho a seguir

O principal motivo para justapor Segurança I à Segurança II é chamar atenção para as consequências de basearmos a gestão da segurança apenas em uma das duas. A tabela a seguir resume suas principais diferenças.

Tabela 1: Conceitos básicos da Segurança I e da Segurança II

	Segurança I	Segurança II
Definição de segurança	Que o menor número possível de coisas dê errado.	Que o maior número possível de coisas dê certo.
Princípio da gestão da segurança	Reativo – responder quando algo acontece ou quando é classificado como um risco inaceitável.	Proativo – tentar prever continuamente os acontecimentos e eventos.
Visão do fator humano na gestão da segurança	Os seres humanos são vistos predominantemente como um risco ou perigo. Eles são um problema a ser resolvido.	Os seres humanos são vistos como um recurso necessário para a flexibilidade e a resiliência do sistema. Eles oferecem soluções flexíveis para muitos problemas em potencial.

Investigação de acidentes	Os acidentes são causados por falhas ou disfunções. A finalidade de uma investigação é identificar as causas.	As coisas acontecem basicamente da mesma maneira, independentemente do resultado. A finalidade de uma investigação é compreender por que as coisas geralmente dão certo, o que serve como base para explicar por que ocasionalmente dão errado.
Avaliação de riscos	Os acidentes são causados por falhas ou disfunções. A finalidade de uma investigação é identificar as causas e os fatores contribuintes.	Compreender as condições nas quais a variabilidade no desempenho pode se tornar difícil ou impossível de monitorar e controlar.

O que os profissionais de saúde fazem geralmente nas situações de trabalho cotidianas é uma combinação de Segurança I e Segurança II. O equilíbrio específico depende de muitos fatores, como a natureza do trabalho, a experiência das pessoas, o clima organizacional, as pressões por parte dos administradores e pacientes, a doença do paciente e outras características. Todos sabem que a prevenção é melhor do que a cura, mas as condições nem sempre permitem que a prevenção cumpra seu papel.

A situação muda no caso dos formuladores de políticas de saúde e das atividades administrativas e regulatórias. Nestes níveis, predomina a visão da Segurança I. Um motivo para isso é que, historicamente, o principal objetivo dos formuladores de políticas, administradores e reguladores tem sido assegurar que os pacientes e o público não sofram danos. Outro motivo é que esses níveis se encontram distanciados, no tempo e no espaço, da operação efetiva dos sistemas e serviços; portanto, têm oportunidades limitadas para observar ou experimentar a forma como o trabalho é realmente feito. Um terceiro motivo é que é muito mais simples contar os poucos eventos em que ocorrem falhas do que os muitos casos nos quais tudo corre bem. Em outras palavras, trata-se de um equilíbrio entre eficiência e meticulosidade (Hollnagel, 2009) (além disso, existe o pressuposto — equivocado — de que é mais fácil explicar os primeiros que os segundos).

Embora as atividades cotidianas na linha de frente do processo raramente sejam apenas reativas, na maioria das situações de trabalho existem pressões que induzem os profissionais à eficiência, e não à meticulosidade. Com isso, torna-se menos legítimo gastar tempo e esforços para digerir e comunicar as experiências, pois isso é visto como algo não produtivo, pelo menos a curto prazo. Ainda assim, a gestão eficaz da segurança requer algum esforço inicial para pensar em como o trabalho é feito, para proporcionar os recursos necessários e para nos prepararmos para o inesperado. A pressão pela eficiência — como as típicas metas hospitalares de atender mais pacientes pelo mesmo custo, padronizando os tratamentos em “pacotes” e reduzindo o tempo médio de internação — faz com que isso seja mais difícil de atingir.

Pode ser difícil gerir a segurança proativamente no caso dos inúmeros pequenos eventos que constituem as situações cotidianas de trabalho. Nestes casos, o desenrolar dos acontecimentos pode ser rápido e inesperado, existem poucos indicadores de tendência e os recursos podem, muitas vezes, ser estendidos ao limite. O ritmo de trabalho deixa pouca oportunidade para reflexões sobre o que está acontecendo e para ações estratégicas. De fato, as pressões do trabalho e das demandas externas muitas vezes exigem soluções oportunistas que forçam o sistema a entrar num modo reativo. Para sair dessa situação, passando do modo reativo para o proativo, é necessário um esforço deliberado. Embora isso possa não parecer viável a curto prazo, é inquestionavelmente um investimento sensato a longo prazo.

A gestão proativa da segurança é mais fácil no caso dos eventos de grande escala porque o desenvolvimento destes é relativamente lento, mesmo quando eles têm um início abrupto (por exemplo, no caso de um furacão ou tempestade de grande porte que causa muitas lesões e abala infraestruturas, ou uma pandemia). Geralmente existem indicadores claros que determinam quando uma resposta é necessária. As respostas apropriadas também são conhecidas, de modo que os preparativos podem ser feitos com antecedência.

É importante enfatizar que a Segurança I e a Segurança II representam duas visões complementares da segurança, e não duas abordagens incompatíveis ou conflitantes. Portanto, muitas das práticas atuais podem continuar a ser usadas, embora possivelmente seja necessária uma ênfase diferente. A transição para a visão da Segurança II, porém, também inclui algumas práticas novas, como descrito a seguir.

Transição para a Segurança II

Procure o que dá certo

A ideia básica é: observe o que dá certo e o que dá errado e aprenda com o que funciona, mas também com o que falha. Não espere que algo ruim aconteça e tente entender o que efetivamente ocorre em situações nas quais nada extraordinário parece acontecer. As coisas não correm bem simplesmente porque as pessoas seguem os procedimentos e trabalham como imaginado. As coisas correm bem porque as pessoas fazem ajustes razoáveis de acordo com as demandas da situação. Descobrir quais são esses ajustes e tentar aprender com eles é pelo menos tão importante quanto descobrir as causas dos resultados adversos.

Quando algo dá errado, como um surto infeccioso, uma falha na comunicação, um erro médico ou um problema como paciente errado/procedimento errado, é improvável que esse seja um evento isolado. Pelo contrário, trata-se de algo que deu certo muitas vezes antes e que vai dar certo muitas vezes depois. É necessário compreender por que essas atividades cotidianas dão certo — o segredo do sucesso — para compreender por que elas podem falhar. Na perspectiva da Segurança II, as coisas não falham devido a algum tipo de erro ou disfunção, e sim devido a combinações inesperadas na variabilidade do desempenho cotidiano.

A diferença entre a visão da Segurança I e da Segurança II está ilustrada na Figura 10.O enfoque da Segurança I são os eventos nas caudas da distribuição normal, e especialmente os eventos na cauda esquerda, que representam os acidentes. Esses eventos são fáceis de observar porque são raros e porque os resultados são diferentes do habitual. Porém, são difíceis de explicar, embora seja muito tentador procurar as causas básicas e utilizar modelos lineares. Como esses eventos são raros e difíceis de compreender, também são difíceis de alterar e de gerenciar.

Figura 10: Relação entre a probabilidade de evento e a facilidade de percebê-lo.

A Segurança II concentra-se nos eventos situados no centro da distribuição. Eles são "difíceis" de ver, mas só porque geralmente os ignoramos em nossas atividades diárias. A "lógica" parece ser: se algo funciona, por que perderíamos nosso tempo com isso? Mas a verdade é que as coisas normalmente não funcionam da forma como presumimos e que o trabalho realizado pode ser consideravelmente diferente do trabalho imaginado. Os eventos no centro do gráfico podem ser compreendidos e explicados em termos dos ajustes mútuos no desempenho que proporcionam a base para o trabalho cotidiano. Por estes eventos serem frequentes, ocorrerem em pequena escala e serem de fácil compreensão, são fáceis de monitorar e gerenciar. As intervenções sobre tais eventos têm um escopo concentrado e limitado (porque o assunto não é complicado).Por isso, também é mais fácil, embora não necessariamente óbvio, prever quais poderão ser seus efeitos principais e colaterais.

Evidentemente, existe um benefício evolutivo em não prestarmos atenção (ou muita atenção) no que é normal, desde que não nos prejudique e desde que o ambiente permaneça estável. Porém, em nossa sociedade, o ambiente já não é mais estável; portanto, esse benefício é ilusório.

O ambiente de trabalho (e, portanto, o trabalho em si) é cada vez mais imprevisível. Isso significa que as rotinas que funcionam bem hoje podem não funcionar bem amanhã; por isso,

é importante prestarmos atenção em como elas funcionam. Esse é o tipo de meticulosidade que nos permite ser eficientes e rápidos no momento de realizar mudanças.

Foco em eventos frequentes

Uma segunda mensagem é: procure o que acontece regularmente e concentre-se nos eventos com base em sua frequência, e não em sua gravidade. Um grande número de pequenas melhorias no desempenho cotidiano pode contar mais do que uma grande melhoria no desempenho excepcional.

Tempo e recursos costumam limitar a investigação de incidentes. A tendência, então, é observar incidentes com consequências graves e deixar o resto para outra hora — que nunca chega. O pressuposto implícito é que o potencial de aprendizagem é proporcional à gravidade do incidente ou acidente.

Isso é obviamente um engano. Embora seja correto dizer que se economiza mais dinheiro evitando um acidente de grande escala do que um de pequena escala, isso não significa que o potencial de aprendizagem também seja maior. Além disso, o custo acumulado de incidentes de pequena escala, porém frequentes, pode facilmente ser maior. Como os eventos pequenos e frequentes são mais fáceis de compreender e de gerenciar (como dito anteriormente), faz mais sentido observá-los do que os raros eventos com resultados graves.

Permanecer sensíveis à possibilidade de falhas

Uma terceira mensagem: embora a Segurança II se concentre nas coisas que dão certo, ainda devemos lembrar que as coisas também podem dar errado e "continuar sensíveis à possibilidade de falhas". Mas as "falhas possíveis" não representam só as coisas que podem funcionar mal como na visão da Segurança I; representam também os resultados desejados que talvez não sejam atingidos, ou seja, a nossa incapacidade de assegurar que as coisas deem certo.

Para assegurar que as coisas deem certo é necessária uma preocupação constante em relação ao que está dando certo, não só para garantir que as coisas continuem assim, mas também para neutralizar a tendência de cairmos num viés de confirmação ou de nos concentrarmos nos resultados ou perspectivas mais otimistas.

Para nos mantermos sensíveis à possibilidade de falhas, é necessário criar e manter uma visão geral e abrangente do trabalho, tanto a curto como a longo prazo. Assim podemos prever e, portanto, prevenir o acúmulo de pequenos problemas ou falhas, realizando pequenos ajustes para mitigar combinações potencialmente prejudiciais de variabilidade no desempenho. Muitos resultados adversos provêm da agregação oportunista de atalhos em combinação com deficiências na supervisão de processos ou na identificação de perigos. Essa sensibilidade em relação àquilo que acontece, às maneiras pelas quais as coisas dão certo e às maneiras pelas quais podem falhar é, portanto, importante para a prática da Segurança II.

Devemos ser meticulosos e também eficientes

A quarta mensagem é: não favoreça a eficiência em detrimento da meticulosidade — ou, pelo menos, não em demasia. Quando utilizamos a maior parte ou todo o tempo tentando fazer com que as contas fechem, sobra pouco ou nenhum tempo para consolidar experiências ou entender o trabalho realizado. A cultura organizacional deve legitimar a alocação de recursos, especialmente o tempo, para a reflexão, a troca de experiências e o aprendizado. Caso contrário, como é possível que as coisas melhorem?

Não é possível atingir a eficiência no presente sem a meticulosidade no passado. Da mesma forma, não é possível atingir a eficiência no futuro sem a meticulosidade no presente, ou seja, sem planejamento e preparação. Embora a meticulosidade possa ser vista como uma perda de produtividade (eficiência) no presente, trata-se de uma condição necessária para a eficiência no futuro. Portanto, para sobrevivermos a longo prazo, é essencial atingirmos algum tipo de equilíbrio.

Investimento em segurança, os ganhos gerados pela segurança

A quinta e última mensagem é: fazer as coisas darem certo é um investimento em segurança e produtividade. Gastar mais tempo para aprender, pensar e nos comunicar costuma ser visto como um custo. Na verdade, a própria segurança é vista como um custo. Isso reflete a visão da Segurança I, na qual um investimento em segurança é um investimento para impedir que algo aconteça. Conhecemos os custos, como quando contratamos um seguro. Mas não sabemos do que é que somos poupados, pois isso é incerto e tem um tamanho desconhecido. Na área de riscos, costuma-se dizer que "se você acha que a segurança é cara, experimente um acidente". Se calcularmos o custo de um acidente de grande porte, como o de Betsy Lehman, a paciente com câncer que recebeu quatro vezes a dose prescrita, já elevada, do quimioterápico ciclofosfamida ao longo de quatro dias (Altman 1995), ou o de Willie King, o diabético de 51 anos que teve a perna errada amputada (Clary 1995), concluímos que quase todo investimento em segurança tem um bom custo-benefício. No entanto, como não podemos provar que as precauções de segurança efetivamente são ou foram o motivo pelo qual um acidente não ocorreu e como não sabemos quando existe a probabilidade de que aconteça um acidente, o cálculo tem um viés a favor de reduzir o investimento (isso é algo que normalmente se observa em épocas mais difíceis).

Na Segurança I, os investimentos em segurança são vistos como custos, isto é, não são produtivos. Assim, se fazemos um investimento e não ocorrem acidentes, o investimento é visto como um custo desnecessário. Se ocorrem acidentes, ele é visto como um investimento justificado. Se não fazemos investimentos e não ocorrem acidentes, isso é visto como uma economia justificada. Porém, se ocorrem acidentes, isso é visto como falta de sorte ou como um erro de julgamento.

Na Segurança II, um investimento em segurança é visto como um investimento em produtividade, porque a definição — e o propósito — da Segurança II é fazer com que o maior

número possível de coisas dê certo. Assim, se fazemos um investimento e não ocorrem acidentes, o desempenho cotidiano ainda será melhorado. Se ocorrem acidentes, o investimento novamente é visto como justificado. Se não fazemos investimentos e não ocorrem acidentes, o desempenho pode continuar aceitável, mas não melhorará. Porém, se ocorrem acidentes, isso é visto como erro de julgamento.

Conclusão

Como os sistemas sociotécnicos dos quais depende o cuidado de saúde continuam a ficar cada vez mais complicados, parece claro que manter a abordagem da Segurança I será inadequado a longo prazo e também a curto prazo. Adotar a abordagem da Segurança II, portanto, não deveria ser uma decisão difícil.

Ainda assim, o caminho a seguir não depende da substituição da Segurança I pela Segurança II, e sim de uma combinação dessas duas mentalidades (Figura 11). A maior parte dos eventos adversos ainda é relativamente simples — ou pode ser tratada como relativamente simples sem consequências graves; portanto, podemos lidar com eles da maneira habitual. Existe um número crescente de casos, porém, nos quais essa abordagem não irá funcionar. Nesses casos, é necessário adotar a perspectiva da Segurança II, que essencialmente significa promover um cuidado de saúde resiliente (Hollnagel, Braithwaite e Wears, 2013).

A Segurança II é, antes de mais nada, uma maneira diferente de encarar a segurança e, por isso, também é uma forma diferente de aplicar muitos métodos e técnicas conhecidos. Todavia, ela também vai exigir métodos próprios para que possamos observar as coisas que dão certo, analisar como elas funcionam e gerenciar a variabilidade no desempenho, em vez de nos limitarmos a restringi-la (Wears, Hollnagel e Braithwaite, 2015).

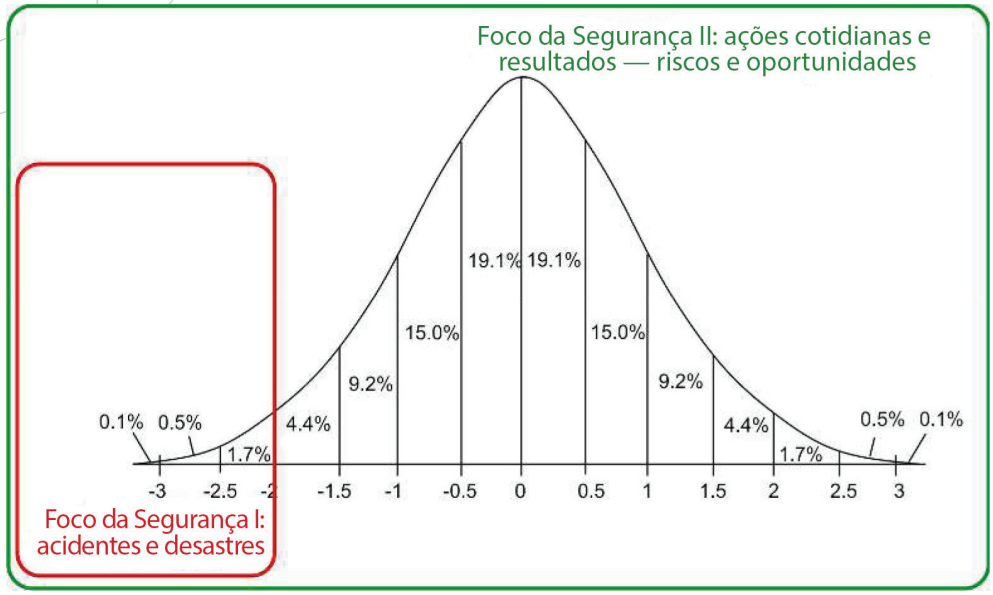


Figura 11: Foco da Segurança I e da Segurança II

Epílogo

Para apresentar uma compreensão diferente do mundo atual e dos sistemas nos quais trabalhamos e dos quais dependemos, pode ser necessário algo como uma mudança de paradigma. A comunidade da segurança tem chegado a um consenso sobre como as coisas funcionam e como garantir a segurança, mas o aumento de nossos conhecimentos estabilizou-se e o grave problema dos eventos adversos continua a existir. Precisamos encarar o fato de que o mundo não pode ser explicado por modelos de causa e efeito. Incidentes e acidentes não acontecem apenas de maneira linear — eles também incluem fenômenos emergentes decorrentes da complexidade do sistema de saúde em geral. Perguntar "por que" não é suficiente para explicar o sistema em uso e não leva a melhorias na segurança.

Como consequência da mudança de paradigma, os especialistas e gestores da segurança precisam sair de sua "zona de conforto" e explorar novas oportunidades. Nesse novo mundo, os gestores e profissionais de saúde estão procurando modelos e métodos que possam utilizar. Alguns métodos já estão disponíveis e têm sido aplicados em diferentes situações. Por exemplo, o Método de Análise de Ressonância Funcional (FRAM; Hollnagel, 2012) procura identificar e descrever as funções essenciais de um sistema, caracterizar a possível variabilidade nas funções, definir a ressonância funcional com base nas dependências e conexões entre funções e identificar formas de monitorar o desenvolvimento da ressonância para mitigar o tipo de variabilidade que pode levar a resultados indesejados ou ampliar o tipo de variabilidade que pode levar a resultados desejados (http://www.functionalresonance.com/).

O novo paradigma também significa que as prioridades da gestão da segurança devem mudar. Em vez de fazer investigações após a ocorrência de um evento ou de se esforçar para reduzir a ocorrência de resultados adversos, a gestão da segurança deve alocar recursos para observar os eventos que dão certo e aprender com eles. Em vez de aprender com eventos segundo sua gravidade, devemos tentar aprender com os eventos segundo sua frequência. Em vez de analisar em profundidade eventos graves e únicos, devemos explorar extensamente a regularidade dos muitos eventos frequentes para entender os padrões de desempenho do sistema. Um bom ponto de partida seria reduzir nossa dependência nos "erros humanos" como uma causa quase universal de incidentes e, em vez disso, compreender a necessidade de variabilidade no desempenho.

Referências

Altman, L. (1995). “Big doses of chemotherapy drug killed patient, hurt 2d”. The New York Times, 24 de março.

Bainbridge, L. (1983). Ironies of automation. Automatica, 19(6), 775-779.

Clary, M. (1995). “String of Errors Put Florida Hospital on the Critical List”. Los AngelesTimes, 14 de abril. Acessado em 11 de dezembro de 2014: http://articles.latimes.com/1995-04-14/news/mn-54645_1_american-hospital.

EUROCONTROL (2009). A white paper on resilience engineering for ATM. Bruxelas: EUROCONTROL.

Finkel, M. (2011). On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield. Stanford, CA: Stanford University Press.

Heinrich, H. W. (1931). Industrial accident prevention: A scientific approach. Nova York: McGraw-Hill.

Hollnagel, E. (2009). The ETTO principle: Efficiency-thoroughness trade-off. Why things that go right sometimes go wrong. Farnham, Reino Unido: Ashgate.

Hollnagel, E. (2012). FRAM: The Functional Resonance Analysis Method. Farnham, Reino Unido: Ashgate.

Hollnagel, E., Braithwaite, J. e Wears, R. L. (2013) Resilient health care. Farnham, Reino Unido: Ashgate.

Hollnagel, E., Woods, D. D. e Leveson, N. G. (2006). Resilience engineering: Concepts and precepts. Aldershot, Reino Unido: Ashgate.

Leveson, N. G. (2004). A new accident model for engineering safer systems. Safety Science, 42(4), 237-270.

Rasmussen, J. e Svedung, I. (2000). Proactive risk management in a dynamic society. Karlstad, Suécia: Swedish Rescue Services Agency.

Reason, J., Shotton, R., Wagenaar, W. A., Hudson, P. T. W. e Groeneweg, J. (1989). Tripod: A principled basis for safer operations. Haia: Shell Internationale Petroleum Maatschappij.

Reason, J. T. (1997). Managing the risks of organizational accidents. Aldershot, Reino Unido: Ashgate Publishing Limited.

Reason, J., Hollnagel, E., e Paries, J. (2006). Revisiting the Swiss Cheese Model of Accidents. EUROCONTROL. Brétigny-sur-Orge, França. Recuperado em 6 de outubro de 2008, de 6/EEC_note_2006_13.pdf.

Shorrock, S. e Licu, T. (2013). Target culture: lessons in unintended consequences. HindSight 17. Bruxelas: EUROCONTROL.

Taylor, F. W. (1911). The principles of scientific management. Nova York: Harper.

Wears, R. L. e S. J. Perry (2006). Free fall - a case study of resilience, its degradation, and recovery, in an emergency department. 2nd International Symposium on Resilience Engineering, Juan-les-Pins, França, Mines Paris Les Presses.

Wears, R. L., Hollnagel, E. e Braithwaite, J. (2015) The resilience of everyday clinical work. Farnham, Reino Unido: Ashgate.

OMS (2014). NCD* death rate, age standardized (per 100 0000 population), 200-2012. Acessado em 11 de dezembro de 2014. http://gamapserver.who.int/gho/interactive_charts/ncd/mortality/total/atlas.html.

Glossário

Ajustes (aproximados): Quando as condições de trabalho não estão bem especificadas ou quando o tempo ou os recursos são limitados, é necessário ajustar o desempenho para que seja coerente com as condições. Esse é um dos principais motivos da variabilidade no desempenho. Porém, as mesmas condições que tornam necessários os ajustes de desempenho também apontam que os ajustes serão aproximados, e não perfeitos. No entanto, as aproximações são, na maioria das situações, boas o suficiente para assegurar o desempenho pretendido.

Análise de causa-raiz (ACR): No pensamento da Segurança I, violações de segurança, erros e eventos adversos manifestam-se regularmente. Os modelos lineares sugerem que é possível evitar sua recorrência se chegarmos à fonte fundamental de um problema e a corrigirmos. Daí surge a análise de causa-raiz. Seus críticos dizem que, na melhor das hipóteses, isso é apenas um trabalho reativo e que poucas fontes fundamentais de problemas podem ser tratadas com soluções simplistas.

Bimodalidade: Os sistemas e componentes tecnológicos funcionam de maneira bimodal. Em termos mais rigorosos, isso significa que, para qualquer elemento de um sistema (desde um componente até o sistema como um todo), esse elemento vai funcionar ou não. No segundo caso, diz-se que o elemento falhou. O princípio bimodal, no entanto, não se aplica a seres humanos e organizações. Pessoas e organizações são multimodais, isto é, seu desempenho é variável — às vezes melhor e às vezes pior, mas nunca completamente disfuncional. Quando um "componente" humano deixa de funcionar, não pode ser substituído da mesma forma que um componente tecnológico.

Crença na causalidade: Existe um pressuposto amplamente aceito de que os eventos adversos ocorrem porque algo deu errado. Quando a causa é encontrada, a situação pode ser resolvida. Por essa lógica, todos os acidentes e erros podem ser evitados: é a crença na causalidade. No entanto, de acordo com princípios do cuidado de saúde resiliente, os êxitos e falhas decorrem das mesmas atividades normais.

Decomposição: Quando um problema, processo ou sistema pode ser dividido em partes a fim de conceptualizá-lo ou compreendê-lo, ele é decomponível.

Engenharia da resiliência: Disciplina científica que se concentra no desenvolvimento das práticas e princípios necessários para permitir que o desempenho dos sistemas seja resiliente.

Equilíbrio entre eficiência e meticulosidade: O equilíbrio entre eficiência e meticulosidade (ETTO, do inglês "*efficiency-thoroughness trade-off*") descreve o fato de que as pessoas (e organizações), como parte de suas atividades, devem buscar praticamente sempre um equilíbrio entre os recursos (tempo e esforço) que gastam para preparar uma atividade e os recursos (tempo, esforço e materiais) que gastam em realizá-la.

Eventos adversos: Os efeitos indesejáveis dos danos causados por uma prescrição, tratamento ou intervenção de saúde costumam ser chamados de eventos adversos. Outros termos relacionados:

incidentes, erros, efeitos colaterais indesejáveis ou danos iatrogênicos. De acordo com a Segurança I, uma certa proporção dos eventos adversos é considerada evitável.

Flexibilidade de um sistema: Um sistema flexível é aquele que consegue se adaptar em resposta a mudanças internas ou externas. Para que o desempenho de um sistema se sustente ao longo do tempo, é fundamental que ele seja responsivo e adaptável.

Modelo dos dominós: A teoria dos dominós original de Heinrich, publicada no início da história da segurança, em 1931, descreve a cadeia cumulativa ou a sequência de eventos que são acionados por um estímulo inicial, relacionando-se metaforicamente a uma fila de dominós sendo derrubados.

Modelo do Queijo Suíço: Todos os sistemas sociotécnicos incluem barreiras e defesas para evitar que aconteçam acidentes e que estes prejudiquem os resultados. O modelo do queijo suíço para as causas de acidentes sugere que essas diversas barreiras se assemelham a várias camadas de queijo suíço empilhadas uma após a outra. Embora as camadas mitiguem o risco de ocorrência de acidentes, elas às vezes podem ter “furos”, não funcionando como pretendido. Quando esses furos estão alinhados, todas as defesas são vencidas, aumentando em muito a probabilidade de acidentes.

Processos emergentes: Num número crescente de casos, é difícil ou impossível explicar o que acontece como resultado de processos ou acontecimentos conhecidos. Nesses casos, diz-seque os resultados são emergentes, e não resultantes. Os resultados emergentes não são aditivos nem previsíveis a partir dos conhecimentos que temos sobre seus componentes, nem podem ser decompostos nesses componentes.

Resiliência: Diz-se que o desempenho de um sistema é resiliente quando ele é capaz de ajustar seu funcionamento antes, durante ou depois da ocorrência de eventos (mudanças, distúrbios e oportunidades) e, portanto, sustenta as operações necessárias tanto nas condições esperadas como nas inesperadas.

Segurança I: Neste caso, a segurança é descrita como a condição na qual o número de resultados adversos (por exemplo, acidentes, incidentes e *near misses*) é o mais baixo possível. Para atingir a Segurança I, precisamos assegurar que as coisas não deem errado, seja pela eliminação das causas das disfunções e dos riscos, seja pela contenção de seus efeitos.

Segurança II: Neste caso, a segurança é descrita como a condição na qual o número de resultados aceitáveis é o mais alto possível. Trata-se da capacidade de um sistema de funcionar adequadamente sob condições variadas. Para atingir a Segurança II, precisamos assegurar que as coisas deem certo, e não impedir que deem errado.

Sistemas intratáveis: Um sistema é chamado de intratável se for difícil ou impossível acompanhar e compreender seu funcionamento. Normalmente, isso significa que o desempenho é irregular, que as descrições são complicadas em termos de partes e relações e que é difícil compreender os detalhes do funcionamento do sistema. Sistemas intratáveis também são mal

especificados, ou seja, é impossível dar uma descrição completa da forma como o trabalho deveria ser realizado num conjunto suficientemente grande de situações.

Sistemas sociotécnicos: Originalmente cunhada por Trist, Bamforth e Emery a partir de seu trabalho em minas de carvão inglesas, a teoria dos sistemas sociotécnicos concentra-se nas relações entre os trabalhadores e a tecnologia. Mais recentemente, a ênfase tem sido observar as complexas infraestruturas das sociedades e das organizações e o comportamento humano. Segundo essa perspectiva, a sociedade em si, juntamente com suas organizações e instituições, constitui uma série de sistemas sociotécnicos complexos.

Sistemas tratáveis: Um sistema é considerado tratável se for possível acompanhar e compreender seu funcionamento. Normalmente, isso significa que o desempenho é bastante regular, que as descrições são relativamente simples em termos de partes e relações e que é fácil compreender os detalhes do funcionamento do sistema.

Teoria da administração científica: Frederick W. Taylor foi um dos primeiros teóricos da administração. Ele estudou o trabalho e as tarefas que o compunham, procurando simplificá-lo e otimizar sua eficiência. Também conhecida como Taylorismo, a administração científica realiza estudos de tempo e movimento para ajudar a determinar a maneira mais eficiente de realizar tarefas. Os gerentes devem planejar e treinar e os trabalhadores devem acatar instruções, trabalhar duro e ter um desempenho eficiente. Esse esquema nega autonomia ao trabalhador e não está adequado aos ambientes de trabalho modernos, incluindo o cuidado de saúde.

Trabalho realizado: O que efetivamente acontece. Os prestadores do cuidado ou de serviços — médicos, enfermeiros e outros profissionais de saúde — realizam o trabalho clínico na linha de frente. Eles compreendem os detalhes finos de como o trabalho clínico é realizado, mas nem sempre têm responsabilidade pelas normas, políticas e procedimentos que governam seu trabalho.

Trabalho imaginado: O que projetistas, administradores, reguladores e autoridades acreditam que acontece ou deveria acontecer. Eles estão longe da linha de frente do cuidado e recebem informações de segunda ou terceira mão sobre como o trabalho é realizado. Além disso, sempre existe um atraso entre o trabalho clínico cotidiano e as informações que os administradores e formuladores de políticas recebem a seu respeito. A base para desenvolver normas, políticas e procedimentos, portanto, será sempre incompleta e, com frequência, incorreta.

Variabilidade no desempenho: A abordagem atual para a segurança (Segurança II) baseia-se no princípio de equivalência entre “êxitos” e “falhas” e no princípio de ajustes aproximados. Dessa forma, o desempenho na prática é sempre variável. A variabilidade no desempenho pode se propagar de uma função para outra e, assim, causar efeitos não lineares ou emergentes.

Sobre os autores

Professor Erik Hollnagel

O Dr. Erik Hollnagel, M.SC., PhD é Professor do *Institute of Regional Health Research* da *University of Southern Denmark* (Dinamarca), consultor-chefe do *Centre for Quality, Region of Southern Denmark*, Professor convidado do *Centre for Healthcare Resilience and Implementation Science* da *Macquarie University* (Austrália) e Professor Emérito do *Department of Computer Science* da *University of Linköping* (Suécia). Ao longo de sua carreira, ele trabalhou em universidades, centros de pesquisa e indústrias de vários países, lidando com problemas de muitos domínios, incluindo geração de energia nuclear, indústria aeroespacial e aviação, engenharia de software, tráfego terrestre e cuidado de saúde.

Entre seus interesses profissionais estão a segurança industrial, a engenharia da resiliência, a segurança do paciente, a investigação de acidentes e a modelagem de sistemas sociotécnicos de grande escala. Ele é autor ou editor de 22 livros, incluindo cinco livros sobre engenharia da resiliência, e publicou um grande número de artigos e capítulos de livros. Seus trabalhos mais recentes, publicados pela Ashgate, são “Safety-I and Safety-II: The past and future of safety management”, “Resilient Health Care”, “FRAM – the Functional Resonance Analysis Method” e “Resilience engineering in practice: A guidebook”. O Professor Hollnagel também coordena a rede *Resilient Health Care* (www.resilienthealthcare.net) e a FRAMily

(www.functionalresonance.com).

Professor Robert Wears

O Dr. Bob Wears, M.D., PhD, M.S. é médico emergencista, Professor de medicina de emergência da *University of Florida* e Professor convidado da *Clinical Safety Research Unit* do *Imperial College London*. Sua formação inclui um mestrado em Ciência da Computação, um ano sabático de pesquisa com foco em psicologia e fatores humanos na segurança no *Imperial College*, seguido por doutorado em Segurança Industrial na *Mines ParisTech* (*Ecole Nationale Supérieure des Mines de Paris*). Ele atua no conselho de diretores da *Emergency Medicine Patient Safety Foundation* e em vários conselhos editoriais, incluindo *Annals of Emergency Medicine, Human Factors and Ergonomics, Journal of Patient Safety* e *International Journal of Risk and Safety in Medicine*.

O Professor Wears coeditou dois livros, *Patient Safety in Emergency Medicine* (Segurança do Paciente em Medicina de Emergência) e *Resilient Health Care* (Cuidado de Saúde Resiliente).

Seus interesses de pesquisa incluem estudos técnicos do trabalho, engenharia da resiliência e segurança do paciente como movimento social. Seus artigos de pesquisa e comentários foram publicados no JAMA, *Annals of Emergency Medicine, Safety Science, BMJ Quality & Safety, Cognition Technology & Work, Applied Ergonomics* e *Reliability Engineering & Safety Science*.

Professor Jeffrey Braithwaite

Dr. Jeffrey Braithwaite, BA, MIR (Hons), MBA, DipLR, PhD, FAIM, FCHSM, FFPHRCP (Reino Unido) é diretor fundador do *Australian Institute of Health Innovation*, diretor do *Centre for Healthcare Resilience and Implementation Science* e Professor de Pesquisa em Sistemas de Saúde da *Faculty of Medicine and Health Sciences* da *Macquarie University*, na Austrália. Sua pesquisa examina a natureza mutável dos sistemas de saúde, particularmente a segurança do paciente, normas e certificação, liderança e gestão, a estrutura e a cultura de organizações e suas características de rede, atraindo um financiamento de mais de 60 milhões de dólares australianos. Atua como Professor convidado na *University of Birmingham*, no Reino Unido, na *Newcastle University*, no Reino Unido, na *University of Southern Denmark*, na Dinamarca, na *University of New South Wales*, na Austrália, e no *Canon Institute of Global Studies*, em Tóquio, Japão.

O Professor Braithwaite tem muitas publicações (mais de 300, no total) e se apresentou em congressos nacionais e internacionais em mais de 600 ocasiões, atuando em mais de 60 como palestrante principal. Sua pesquisa aparece em periódicos como *British Medical Journal, The Lancet, Social Science & Medicine, BMJ Quality and Safety, International Journal of Quality in Health Care, Journal of Managerial Psychology, Journal of the American Medical Informatics Association* e muitos outros periódicos de prestígio. O Professor Braithwaite recebeu inúmeros prêmios nacionais e internacionais por seus ensinamentos e sua pesquisa.

Agradecimentos

Gostaríamos de homenagear nossos estimados colegas da *Resilient Health Care Network*, que são uma fonte constante de ideias e inspiração. Agradecimentos sinceros à Dra. Brette Blakely, Jackie Mullins e Sue Christian-Hayes, que pesquisaram documentos, forneceram fotos e revisaram e formataram este artigo. Os erros restantes são de nossa inteira responsabilidade. Nossa gratidão também à iniciativa de Tony Licu de encomendar o Artigo do Eurocontrol sobre Segurança I e Segurança II (Hollnagel, E., Leonhardt, J., Licu, T. e Shorrock, S. (2013). *From Safety-I to Safety-II: A White Paper.* Bruxelas, Bélgica: Eurocontrol.), que foi a inspiração para este documento.