

## O Desafio da Segurança de Tecnologias\*

Leonam Guimarães - Colaborador Voluntário Sênior

---

**5 de fevereiro de 2016**

Por que tragédias como Mariana, Fukushima, Chernobyl, Exxon Valdez e Bhopal ocorreram? Esses acidentes seriam evitáveis? Ou seriam a inevitável consequência da utilização generalizada de tecnologias de risco no mundo moderno? Existem duas escolas de pensamento antagonistas sobre essa questão específica da segurança. A primeira encarna a visão otimista chamada de “*teoria da alta confiabilidade*”, cujos adeptos postulam que operações extremamente seguras podem ocorrer, mesmo quando envolvem tecnologias extremamente perigosas, desde que haja um planejamento organizacional e técnicas de gestão adequadas. A segunda escola, chamada de “*teoria dos acidentes normais*”, apresenta um prognóstico muito mais pessimista: acidentes sérios envolvendo sistemas complexos de alta tecnologia são inevitáveis. Examinaremos essas duas escolas de pensamento, as mais importantes na literatura de teoria organizacional relativa à questão da segurança e confiabilidade de sistemas tecnológicos complexos.

O termo *escolas de pensamento* foi usado deliberadamente, dado que representa em muitos sentidos uma melhor descrição do que há na literatura sobre tecnologias de risco do que o termo *teorias*. Os estudos existentes estão baseados em combinações de lógica dedutiva abstrata e observação empírica indutiva, e os autores de cada escola não estão de acordo acerca de todos os detalhes relativos à segurança organizacional. Muitos termos específicos que aparecem com frequência na literatura não são sempre utilizados de maneira coerente. Além disso, é importante frisar que os prognósticos das duas escolas frequentemente se mostram imprecisos. Entretanto, os defensores de cada uma colocam o foco da atenção em um conjunto específico de fatores que, segundo eles,

contribuem ou reduzem a segurança, e cada escola desenvolve um conjunto de hipóteses gerais que é tido como válido em uma multiplicidade de organizações através do espaço e do tempo. Essas ideias podem, portanto, serem vistas como teorias decorrentes das ciências sociais e podem ser comparadas entre si.

Essas duas escolas de pensamento têm suas raízes intelectuais em diferentes tradições da literatura sobre a teoria das organizações. Elas têm compreensões básicas distintas sobre como as organizações trabalham e mantêm diferentes visões acerca da melhor maneira de analisar organizações complexas. As teorias oferecem explicações gerais opostas a respeito das causas dos acidentes ocorridos com sistemas tecnológicos perigosos e oferecem recomendações alternativas no sentido de incrementar a segurança no futuro. De forma mais ampla, elas têm visões conflitantes sobre o que poderia ser denominado *grau de perfeição* que é possível ser alcançado em organizações complexas. Finalmente, as teorias da alta confiabilidade e dos acidentes normais acarretam prognósticos muito distintos sobre as causas e a probabilidade de ocorrência de acidentes tecnológicos severos.

### **Teoria das Organizações de Alta Confiabilidade**

Os teóricos da alta confiabilidade acreditam que as tecnologias de risco podem ser controladas de modo seguro por organizações complexas se planejamento e técnicas de gestão inteligentes forem adotados<sup>[1]</sup>. Esta conclusão otimista é baseada no argumento de que organizações eficientes podem satisfazer quatro condições específicas, necessárias para criar e manter um nível de segurança adequado: (1) as elites políticas e os líderes da organização devem dar alta prioridade à segurança e confiabilidade; (2) existência de níveis significativos de redundância, permitindo que unidades de reserva ou de superposição compensem falhas; (3) reduções dos índices de erro através da descentralização da autoridade, de uma forte cultura organizacional e de operações de treinamento contínuas; e (4) aprendizagem organizacional através de um processo de tentativa e erro, complementado por ações de antecipação e simulação.

Essas condições foram observadas em várias organizações de alta confiabilidade e, se essas condições existirem em outras organizações, então a teoria teria como prognóstico que acidentes

sérios e catástrofes podem ser evitados. Embora a combinação apropriada de estratégias em um caso específico obviamente dependa da natureza do problema em particular, a estratégia anti-catástrofe esboçada acima poderia ser aplicada praticamente a qualquer tecnologia de risco. Acredita-se que essas quatro condições podem ser aplicadas em grande parte das organizações que requerem tecnologias avançadas e nas quais o custo do erro é tão grande que precisa ser absolutamente evitado.

Dessa forma, embora os teóricos da alta confiabilidade não estabeleçam que quantidades e combinações precisas desses fatores sejam necessárias para o sucesso operacional com as tecnologias de risco, seu otimismo geral é evidente. Organizações adequadamente concebidas e bem geridas têm condições de operar com segurança até mesmo as tecnologias mais arriscadas.

### **Teoria dos Acidentes Normais**

Os teóricos dos acidentes normais adotam uma visão de sistemas abertos naturais em que as organizações e os seus membros são atores que têm seus próprios interesses e estes são potencialmente conflitantes, e em que as organizações são fortemente influenciadas por forças políticas e sociais mais abrangentes no ambiente<sup>[2]</sup>. Esses veem as organizações como detentoras de preferências incoerentes, tecnologias obscuras e participação fluida. A teoria prevê que acidentes graves são inevitáveis quando as organizações que controlam tecnologias de risco dispõem tanto de alta complexidade interativa (que produz falhas peculiares e imprevistas) quanto de acoplamento com precisão (que faz com que falhas se multipliquem e fujam rapidamente do controle).

Cada um dos quatro fatores identificados previamente que contribuem para uma grande confiabilidade é considerado a partir da visão dos acidentes normais como ineficaz, difícil de ser melhorado, ou até contraproducente. Mesmo quando líderes dão muita prioridade para a segurança e a confiabilidade, o que não é sempre um fato, objetivos competitivos organizacionais e individuais reinarão: os desejos contínuos para maximizar a produção, manter a autonomia, e proteger as reputações pessoais, podem, entretanto, impedir seriamente esforços no sentido de melhorar a segurança. Acrescentar redundância não implica necessariamente maior confiabilidade, pois também aumenta a complexidade interativa,

estimula os operadores a correrem mais riscos, e torna o sistema como um todo mais obscuro. A tomada de decisão descentralizada não implica necessariamente melhor segurança, pois sistemas acoplados com precisão exigem reações rápidas e adesão rígida aos procedimentos de operação convencionais.

Uma socialização intensa e uma forte cultura organizacional provavelmente não serão muito produtivas em organizações de risco, não somente porque os líderes não podem saber como os operadores deveriam reagir em todas as contingências, mas também porque as sociedades democráticas não estão dispostas a isolar e controlar todos os aspectos das vidas dos membros dessas organizações. Treinamento e prática constantes não tratarão de cenários de acidentes que são imprevistos, extremamente perigosos, ou politicamente desagradáveis. Finalmente, inúmeros fatores vão limitar o processo de aprendizagem por tentativa e erro: incerteza em relação às causas dos acidentes, os interesses políticos e julgamentos tendenciosos dos líderes organizacionais e dos operadores de baixo escalão, compartimentalização dentro da organização e sigilo entre as organizações.

### **Avaliando as Teorias**

Que perspectiva a respeito das organizações de risco é mais precisa? Não é uma tarefa fácil avaliar essas duas teorias. As duas têm hipóteses relativamente plausíveis e as propostas e conclusões das duas teorias parecem decorrer logicamente dessas hipóteses. Além disso, os teóricos da alta confiabilidade tanto quanto aqueles dos acidentes normais oferecem inúmeros exemplos hipotéticos e empíricos para ilustrar e apoiar seus argumentos. Portanto, como se pode avaliar o poder explicativo global das duas abordagens teóricas?

A maior dificuldade deve ser reconhecida: como nenhuma das teorias oferece uma previsão assertiva a respeito da probabilidade de ocorrência de acidentes graves envolvendo tecnologias de risco, é impossível determinar o número preciso de acidentes os quais, se fossem descobertos ao longo do tempo, dariam sustentação ou fragilizariam as teorias.

Os membros da escola da alta confiabilidade comumente são suficientemente prudentes para evitar a declaração extrema de que

a perfeição organizacional é possível. Nesse sentido, argumentam que existe uma boa chance de que as catástrofes sejam evitadas, afirmam somente que existem organizações de risco que se empenham em procedimentos próximos do erro zero e postulam que essas organizações mantêm uma proporção muito baixa de erros e uma quase ausência total de falhas catastróficas.

De modo similar, os membros da escola dos acidentes normais afirma simplesmente que em algum momento os acidentes devastadores ocorrerão: Os acidentes são inevitáveis e ocorrem o tempo todo. Os mais graves são inevitáveis embora não sejam frequentes. As catástrofes são inevitáveis, ainda que raras. Essa linguagem imprecisa sugere que as duas escolas teóricas têm uma avaliação em comum a respeito da probabilidade de ocorrência de acidentes perigosos a despeito da nítida distinção no tom de suas conclusões. Os teóricos dos acidentes normais olham para o “copo da segurança” e o veem 1% vazio. Já os teóricos da alta confiabilidade veem o mesmo copo 99% cheio.

Contudo, quando alguém leva em consideração os mecanismos causais envolvidos nas teorias, isto é, os fatores específicos, delineados na tabela a seguir, que cada teoria alega que acarretarão ou evitarão os acidentes organizacionais, as contradições entre elas tornam-se mais claras. Isso sugere que um teste mais importante das teorias implica um histórico detalhado específico de estudos de casos em que aparece uma multiplicidade desses fatores, buscando saber se esses fatores têm a influência esperada na segurança e confiabilidade.

### *Teoria da Alta Confiabilidade*

Acidentes podem ser evitados através de boa concepção e gestão organizacional.

Segurança é o objetivo organizacional prioritário.

Redundância aumenta a segurança: Duplicação e sobreposição podem tornar “um sistema confiável a partir de partes não confiáveis.”  
riscos.

Tomada de decisão descentralizada é crucial para permitir reações a surpresas imediatas e flexíveis no momento.

Uma “cultura de segurança” aumentará a confiabilidade encorajando os operadores de campo a terem reações uniformes e apropriadas.

Operações, treinamento e simulações contínuas podem criar e manter operações de alta confiabilidade.

Aprendizagem por tentativa e erro de acidentes pode ser eficaz e pode ser acrescida de antecipação e simulações.

### *Teoria dos Acidentes Normais*

Acidentes são inevitáveis em sistemas complexos e acoplados com precisão.

Segurança é um dos vários vários objetivos concorrentes.

Redundância em geral causa acidentes: aumenta a complexidade interativa e a opacidade estimula a correr

Contradição organizacional: descentralização é crucial para complexidade, porém, a centralização é necessária em sistemas acoplados com precisão.

Um modelo militar de disciplina intensa, socialização, e isolamento é incompatível com valores democráticos.

Organizações não podem treinar simulando operações não imaginadas, muito perigosas, ou politicamente desagradáveis.

Negação de responsabilidade, relatórios falsos e reconstrução da história prejudica esforços de aprendizagem.

Por exemplo, que efeito o fato dos líderes darem alta prioridade à segurança teria nas crenças e no comportamento do restante das pessoas de uma organização complexa? Qual o impacto do acréscimo de equipamentos de segurança redundantes? Há de fato aprendizagem organizacional, corrigindo as causas dos problemas de segurança, após os incidentes graves? Ou relatórios enganosos, negando responsabilidades, fez com que a história fosse reconstruída?

É importante enfatizar que a simples existência de acidentes que quase acontecem é uma prova inadequada, tanto para reduzir a

credibilidade da teoria da alta confiabilidade quanto para incrementar a credibilidade da teoria dos acidentes normais. Na realidade, há uma ironia aqui: quanto mais descubro acidentes que quase ocorrem, mais se pode dizer que o sistema funcionou, na medida em que incidentes finalmente não levaram a uma catástrofe. O fato de que erros individuais ocorrerão constitui, afinal, a razão básica pela qual a redundância e outras medidas de segurança são construídas nos sistemas tecnológicos complexos.

Quais eram as causas dos incidentes e as razões pelas quais não se intensificaram? Por exemplo, a adição de mais de um equipamento de segurança conseguiria evitar um acidente grave, tal como seria sugerido pelos teóricos da alta confiabilidade? Ou a causa do problema foi a redundância, como prognosticado pela teoria dos acidentes normais? E se a redundância causou o incidente, o que fez com que não se intensificasse?

É essencial avaliar o poder explicativo das duas teorias. Isso terá grandes implicações na nossa capacidade de gerir as organizações complexas que utilizam tecnologias de risco na sociedade moderna, evitando a recorrência de acidentes catastróficos.

---

**Notas:**

[1] *High reliability organisations: A review of the literature*, Prepared by the Health and Safety Laboratory for the Health and Safety Executive 2011, London UK, 2011. **Disponível em:** <http://www.hse.gov.uk/research/rrpdf/rr899.pdf>

[2] *Normal Accidents: Living with High Risk Technologies*, Updated edition, Charles Perrow, With a new afterword and a new postscript by the author, 1999, ISBN: 9780691004129

---

\* **Avaliação de Leonam dos Santos Guimarães:** Doutor em Engenharia, Diretor de Planejamento, Gestão e Meio Ambiente da Eletrobrás Eletronuclear e membro do Grupo Permanente de Assessoria do Diretor-Geral da Agência Internacional de Energia Atômica (AIEA).

## About Leonam Guimarães - Colaborador Voluntário Sênior



É Diretor de Planejamento, Gestão e Meio Ambiente da Eletrobrás Termonuclear S.A. - Eletronuclear e membro do Grupo Permanente de Assessoria do Diretor-Geral da Agência Internacional de Energia Atômica – AIEA. Foi Professor Titular da Faculdade de Administração da FAAP, Professor Visitante da Escola Politécnica da USP, Diretor Técnico-Comercial da Amazônia Azul Tecnologias de Defesa SA – AMAZUL, Assistente da Presidência da Eletronuclear e Coordenador do Programa de Propulsão Nuclear do Centro Tecnológico da Marinha. Especialista em Segurança Nuclear e Proteção Radiológica, é Doutor em Engenharia Naval e Oceânica pela USP, Mestre em Engenharia Nuclear pela Universidade de Paris XI e autor de vários livros e artigos sobre engenharia naval e nuclear, gestão e planejamento, política nuclear e não-proliferação.

Fonte: Site Ceiri Newspaper (o artigo original está disponível em <http://www.jornal.ceiri.com.br/o-desafio-da-seguranca-de-tecnologias/>)