COMPÊNDIO DE FATORES HUMANOS PARA INDÚSTRIA DE ÓLEO E GÁS

VOLUME 1

Fundamentos, Perspectivas e Modelo para Aplicação Setorial

Catalogação na publicação
Bibliotecário catalogador - Mariana Acorse - CRB76775

A138

Compêndio de Fatores Humanos para Indústria de Óleo e Gás : Volume 1 — Fundamentos, Perspectivas e Modelo para Aplicação Setorial / coordenação de Rafael Ceni de Almeida, Marcelo Cury e Lima e Priscilla Salles de Moraes ; Associação Brasileira das Empresas de Bens e Serviços de Petróleo (ABESPetro). — Rio de Janeiro : ABESPetro, 2026.

396 p.; 17 X 24 cm il. Color
ISBN : 978-65-02-52120-5

1. Indústria de petróleo e gás. 2. Engenharia de fatores humanos. 3. Segurança de processo. I. Almeida, Rafael Ceni de, coord. II. Lima, Marcelo Cury e, coord. III. Moraes, Priscilla Salles de, coord. IV. Título..

CDD 620.82
CDU 331.101.1

COMPÊNDIO DE FATORES HUMANOS PARA INDÚSTRIA DE ÓLEO E GÁS

VOLUME 1

Fundamentos, Perspectivas e Modelo para Aplicação Setorial

Integração Teórica em Fatores Humanos
GT Fatores Humanos



Conselho editorial e colaboradores

Patrocínio Institucional

Publicação:
ABESPetro — Associação Brasileira das Empresas de Bens e Serviços de Petróleo
Presidente Executivo: Telmo Ghiorzi
Comitê Técnico: Comitê de SMS da ABESPetro
Grupo de Trabalho: Fatores Humanos
Coordenação Geral do GT: Marcelo Cury e Lima | Priscilla Salles de Moraes

COORDENAÇÃO EDITORIAL
VOLUME 1
Rafael Ceni de Almeida
Marcelo Cury e Lima
Priscilla Salles de Moraes

REVISÃO TÉCNICO-CIENTÍFICA
Prof. Dr. Eder Henriqson
(PUCRS / Lund University)
Partes I, II e IV
Prof. Dr. Josué E. Maia França (Petrobras University / KTH - Instituto Real de Tecnologia da Suécia)
Partes III e IV

Autores e Revisores por pares por seção

Parte / Seção	Autor(es)	Revisão por Pares
PARTE I — Fundamentos e Evolução Histórica	Rafael Ceni de Almeida e Eder Henriqson	Eder Henriqson
PARTE II — Perspectivas Teóricas Fundamentais	*(Ver seções abaixo)*	Eder Henriqson
2.1 Teoria dos Acidentes Normais (NAT)	Paula Freitas e Kaio Pimentel	Rafael Ceni de Almeida
2.2 Teoria da Alta Confiabilidade (HRO)	Priscilla Salles de Moraes e Rafael Ceni de Almeida	Eder Henriqson

Parte / Seção	Autor(es)	Revisão por Pares
2.3 Perspectiva Rasmusseniana	Hannah Martins e Fabiano Lima	Rafael Ceni de Almeida
2.4 Engenharia de Resiliência (RE)	Louize Dan, Guilherme Areias e Thais Santos	Rafael Ceni de Almeida
2.5 Dependência de Trajetória (Path Dependency)	Cristina Ribeiro e Marcelo Cury	Rafael Ceni de Almeida
PARTE III — Ecossistema de FH e Abordagens Complementares	*(Ver seções abaixo)*	Josué E. Maia França
3.1 Ecossistema de Fatores Humanos	Josué E. Maia França	Josué E. Maia França
3.2 Aprendizagem com Eventos e Investigação de Acidentes	Rafael Ceni de Almeida	Caroline Capaverde
3.3 Cultura Justa e Accountability	Rafael Ceni de Almeida e Priscilla Salles de Moraes	Beatriz Gershenson
3.4 Análise de Confiabilidade Humana (HRA) e Tarefas Críticas	André Gandini e Rafael Ceni de Almeida	Josué E. Maia França
3.5 Engenharia de Fatores Humanos (HFE)	André Gandini e Rafael Ceni de Almeida	Josué E. Maia França
3.6 Segurança de Processo	André Gandini e Rafael Ceni de Almeida	Gilsa Monteiro e Josué E. Maia França
PARTE IV — Framework Integrador para Aplicação Setorial	Rafael Ceni de Almeida, José Carlos Bruno, Eder Henriqson, Josué E. Maia França.	Eder Henriqson e Josué E. Maia França

Validação Setorial

A validação prática do conteúdo deste volume é realizada por meio de consulta às empresas associadas da ABESPetro e a especialistas seniores indicados pelo Comitê de SMS, em complemento à revisão técnico-científica acadêmica. Esta etapa assegura a aderência da obra às realidades operacionais do setor brasileiro de óleo, gás e energia.

Equipe de produção editorial

Projeto gráfico: EnterDesign
Editoração e diagramação: Juliana Estevo
Revisão linguística e copidesque: Rafael Ceni de Almeida e Marcelo Cury
Normalização bibliográfica: Rafael Ceni de Alemida
Ilustração e produção de figuras técnicas: Rafael Ceni de Almeida

Agradecimentos Institucionais

O GT Fatores Humanos agradece às instituições parceiras que ancoraram o referencial teórico, metodológico e regulatório deste volume:
PUCRS — Pontifícia Universidade Católica do Rio Grande do Sul
Petrobras University e ITA — Instituto Tecnológico de Aeronáutica
ANP — Agência Nacional do Petróleo, Gás Natural e Biocombustíveis
IADC Brasil e IOGP — International Association of Oil & Gas Producers

Sobre a natureza desta publicação

Esta publicação tem caráter técnico-científico e orientativo. O Compêndio não estabelece requisitos, critérios de conformidade, níveis mínimos de desempenho ou linhas de base de auditoria: as práticas, métodos e ferramentas aqui descritos constituem repertório disponível ao julgamento técnico das organizações, a ser aplicado de forma proporcional ao risco, à complexidade e ao contexto de cada operação. Os requisitos aplicáveis às instalações do setor são os estabelecidos pela regulamentação vigente. Havendo divergência entre o texto aqui apresentado e o texto regulatório, prevalece o regulatório.

Sumário

Conselho editorial e colaboradores *5*
Quem Somos *10*
Empresas Associadas *12*
Prefácio *14*
Prefácio do Presidente-Executivo da ABESPetro *17*

Parte I

Fundamentos e evolução histórica de Fatores Humanos *21*
1.1 Conceitos Fundamentais de Fatores Humanos *22*
1.2 Evolução Histórica de Fatores Humanos e da Ciência da Segurança *33*
1.3 Os Limites da Segurança Tradicional e a Escala de Amalberti *54*
1.4 Fatores Humanos como Jornada de Aprendizagem Organizacional *58*

Parte II

Perspectivas teóricas fundamentais: Estado da Arte *69*
2.1 Teoria dos Acidentes Normais (NAT) *72*
2.2 Teoria da Alta Confiabilidade e as Organizações de Alta Confiabilidade (HRT/HRO) *95*
2.3 Perspectiva Rasmusseniana: Objetivos Conflitantes e Migração aos Limites *117*
2.4 Engenharia de Resiliência (RE) *136*
2.5 Perspectivas de Dependência de Trajetória *174*

Parte III

Ecossistema de fatores humanos e abordagens complementares *197*
3.1 Ecossistema de Fatores Humanos *200*
3.2 Aprendizagem com Eventos e Investigação de Acidentes *203*
3.3 Cultura Justa e Accountability *234*
3.4 Análise de Confiabilidade Humana (HRA) e Tarefas Críticas *256*
3.5 Engenharia de Fatores Humanos (HFE) *265*
3.6 Segurança de Processo *271*

Parte IV

Modelo integrador para aplicação setorial *301*
4.1 Da Teoria à Transformação Organizacional: Fatores Humanos como Jornada de Aprendizagem *302*
4.2 Os Cinco Movimentos da Jornada de Fatores Humanos *307*
4.3 Dinâmicas da Mudança: Obstáculos, Resistências e Armadilhas da Transformação *320*
4.4 Ênfase na Prevenção de Eventos com Potencial de Gravidade: Segurança de Processo e Segurança Pessoal *323*
4.5 Matriz de Aplicação por Perspectiva Teórica *333*
4.6 A Expansão do Olhar: Do Micro ao Macro *335*
4.7 Integração do Ecossistema Setorial: Contratantes, Contratadas e Regulador *336*
4.8 Articulação com a NT 10/2023 da ANP *339*
4.9 A Jornada como Compromisso Contínuo *340*

Glossário Técnico Unificado *344*

Quem Somos

Sobre a ABESPetro

A Associação Brasileira das Empresas de Bens e Serviços de Petróleo (ABESPetro) é uma instituição civil sem fins lucrativos, cujo objetivo é promover o desenvolvimento econômico sustentável das empresas que fornecem bens e serviços para a atividade de exploração e produção de petróleo. Foi fundada em 2004 e representa o primeiro elo desta cadeia produtiva. A entidade busca promover crescimento, eficiência e competitividade ao ambiente de negócios em que suas associadas estão inseridas. As empresas associadas à ABESPetro ativam outros elos da indústria de petróleo e exercem efeito multiplicador sobre empregos, renda e arrecadação. A ABESPetro tem hoje mais de 60 empresas em seu quadro de associadas. Elas atuam nos segmentos de reservatórios e poços, instalações submarinas de coleta e escoamento de fluidos, sondas de perfuração e unidades estacionárias de produção de petróleo, logística e apoio a operações.

Para mais informações, acesse www.abespetro.org.br.

Estrutura e Governança da ABESPetro

Diretoria Executiva
Telmo Ghiorzi | Presidente-Executivo (coordenador do trabalho)
Hérica Kruger | Gerente de Administração e Conformidade
Elisa Andrade | Coordenadora de Políticas Públicas
Mariana Finello | Analista de Políticas Públicas
Tatiana Borges | Analista de Comunicação
Silvana Leal | Analista de Administração e Finanças
Celso Gomes | Estagiário

Conselho de Administração | Gestão 2026-2028
Rodrigo Ribeiro | Constellation | Presidente
Lauro Puppim | Saipem | Vice-presidente
Hugo Neto | Halliburton
Ivan Cruz | Subsea7
Jonas Lobo | SBM Offshore
Luana Duffé | TechnipFMC
Luiz Capellotto | Baker Hughes
Simão Silva | Oceaneering

Comitês Temáticos | Coordenadores | Gestão 2026-2028
Aduaneiro | Bianca Lima (SLB) e Michele Rolim (Maersk)
Jurídico | Miriam Yanikian (Constellation) e Rayanne Marinheiro (Baker Hughes)
Pessoas | Silvia Bastos (Constellation) e Mirian Cardoso (Ocyan)
Política Industrial | Thereza Moreira (Saipem) e Guilherme Matos (Oceaneering)
SMS | Emanuel Veiga (Baker Hughes) e José Saturnino (NOV)
Tributário | Aline Bergfeld (Maersk) e Carlos Trugilho (Baker Hughes)

Comitê de Ética e Integridade
Dayane Souza (Mota-Engil)
Gilberto Couto (Foresea)
Hugo Valente (NOV)
Natália Fonseca (Oceanpact)
Sancler Cardoso (Constellation)

Empresas Associadas




VALARIS
Ventura Offshore
Weatherford
wood.
YINSON Production
Camorim
CHC Brasil
cladtek
Constellation.
COSL
EXPRO
Foresea
Forship
FUGRO
GranServices
Intermoor Moorings and Anchors
manserv
100 Years MCDERMOTT
MDL INGENIOUS INSTINCT
MFX MFX do Brasil
NOV
OCEANEERING
OceanPact
ocyan
OIL STATES
Seagems
SBM OFFSHORE
Schneider Electric
Seadrill
SIEMENS
TechnipFMC
GRUPO TECHOCEAN
Transocean
TSA HOLDING
UTEC Geo-services

Prefácio

Este volume inaugura a coleção "**Compêndio de Fatores Humanos para Indústria de Óleo e Gás**", iniciativa do Grupo de Trabalho de Fatores Humanos da ABESPetro. A obra responde à demanda das empresas associadas que, desde 2024, elegeram Fatores Humanos como tema prioritário do Comitê de SMS – um reconhecimento da crescente relevância deste campo para a segurança e o desempenho operacional do setor.

A indústria de óleo, gás e energia enfrenta desafios sem precedentes: integração de tecnologias digitais, automação avançada, interfaces humano-máquina cada vez mais sofisticadas e pressões operacionais que tensionam continuamente os objetivos de eficiência e segurança. Neste contexto, a compreensão dos fatores que influenciam o desempenho humano deixa de ser uma especialidade técnica e torna-se uma competência organizacional estratégica.

Embora tenha a indústria de petróleo e gás como referência, este compêndio não se restringe a ela. Seus fundamentos foram construídos, em grande parte, a partir da aviação, do setor nuclear, da indústria química e de outros sistemas sociotécnicos complexos. Por isso, aplica-se igualmente a outros segmentos da indústria de energia e a toda organização que opera atividades de alto risco.

Este primeiro volume, intitulado "**Fundamentos, Perspectivas e Modelo para Aplicação Setorial**", foi concebido com três propósitos centrais:

- promover o nivelamento conceitual, com uma linguagem comum sobre fundamentos, terminologia e abordagens do campo;
- oferecer um repertório teórico de perspectivas que, articuladas, permitem análises mais completas dos sistemas sociotécnicos, em vez de uma doutrina única;
- preservar o rigor das formulações originais de cada escola, sem simplificações que descaracterizem suas contribuições.

O compêndio não pretende dizer às organizações o que fazer. Seu objetivo é

oferecer bases para que cada uma desenvolva uma análise própria e traduza conceitos em práticas adequadas ao seu contexto. Tem **caráter técnico-científico e orientativo**: não estabelece requisitos, critérios de conformidade nem linhas de base de auditoria, e suas práticas devem ser aplicadas de forma proporcional ao risco e à complexidade de cada operação. Havendo divergência com a regulamentação vigente, prevalece o texto regulamentar.

A obra é organizada em quatro partes:

- Parte I: fundamentos e evolução histórica do campo;
- Parte II: perspectivas teóricas específicas do estado da arte;
- Parte III: Ecossistema de Fatores Humanos e abordagens complementares;
- Parte IV: framework integrador para o contexto brasileiro, articulado à NT 10/2023 da ANP.

Busca-se uma linguagem acessível, sem perder precisão, tanto para especialistas quanto para quem está iniciando sua jornada no tema.

Agradecemos ao Conselho de Administração e à Diretoria Executiva da ABESPetro pelo apoio institucional que tornou possível esta obra, bem como ao Comitê de SMS, às empresas associadas, aos colaboradores, revisores e instituições parceiras, em especial aos especialistas acadêmicos que asseguram a fidelidade às fontes originais. Esperamos que este compêndio contribua para elevar o padrão técnico do setor e fortalecer uma cultura voltada à aprendizagem, à confiabilidade e à resiliência.

Coordenação do Grupo de Trabalho de
Fatores Humanos da ABESPetro,
Outubro de 2026


BRAVA STAR
BRAVA STAR

Prefácio do Presidente-Executivo da ABESPetro

A indústria de petróleo e gás caracteriza-se pela intensidade tecnológica, pela complexidade de suas operações e pela necessidade de conciliar segurança, confiabilidade, eficiência e competitividade. Entretanto, a disponibilidade de tecnologias avançadas não assegura, por si só, sua utilização eficaz. Entre o domínio de um equipamento e a capacidade de operá-lo com segurança existe um conjunto de conhecimentos, competências e práticas que precisa ser desenvolvido e aperfeiçoado.

É essa perspectiva que torna relevante a publicação deste Compêndio de Fatores Humanos para Indústria de Óleo e Gás, elaborado no âmbito do Grupo de Trabalho de Fatores Humanos, vinculado ao Comitê de Segurança, Meio Ambiente e Saúde (SMS) da ABESPetro.

Desde o início do projeto, tenho enfatizado uma palavra que traduz seu significado: coragem.

Coragem dos coordenadores, dos integrantes do Grupo de Trabalho, dos autores, revisores e demais colaboradores que aceitaram o desafio de construir uma obra coletiva, de natureza técnico-científica, sobre um campo de conhecimento complexo e marcado por diferentes perspectivas. Coragem de iniciar uma empreitada sem garantias de êxito, enfrentar as incertezas inerentes à produção do conhecimento e transformar uma ambição compartilhada nesta publicação.

Mas há outra dimensão dessa coragem: a disposição de questionar conceitos e práticas consolidados, inclusive aqueles que orientaram, por décadas, a gestão da segurança na indústria.

A obra contribui para essa reflexão ao demonstrar que o desempenho operacional não depende apenas dos equipamentos, dos procedimentos ou das competências

individuais. Resulta das interações entre pessoas, tecnologias, processos, estruturas organizacionais e condições de trabalho.

Essa abordagem representa uma evolução em relação às concepções tradicionais de segurança, centradas na identificação de erros individuais e no cumprimento de regras. Sem desconsiderar a responsabilidade de cada profissional ou a importância da disciplina operacional, o compêndio evidencia que compreender acidentes, incidentes e operações bem-sucedidas exige examinar o sistema sociotécnico em que ocorrem.

Há, nesse ponto, uma convergência com as abordagens contemporâneas da inovação e do desenvolvimento de capacidades tecnológicas. A inovação não resulta de uma sequência linear entre pesquisa científica, desenvolvimento tecnológico e aplicação produtiva. Constitui um processo interativo e cumulativo, no qual o conhecimento também emerge da experiência, da solução de problemas e das relações entre diferentes agentes.

Da mesma forma, segurança e confiabilidade não decorrem apenas da aplicação de normas e tecnologias. Dependem da capacidade das organizações de aprender, identificar vulnerabilidades, interpretar situações imprevistas e transformar conhecimentos em competências duradouras.

Essa compreensão possui implicações para toda a cadeia produtiva. As operações de petróleo e gás envolvem redes interdependentes de operadoras, prestadoras de serviços, fabricantes de equipamentos e fornecedores de tecnologias. O desempenho de cada organização é influenciado pelas decisões e práticas das demais. Segurança e confiabilidade são, portanto, também resultados das interações ao longo dessa cadeia.

Esse entendimento converge com uma das principais pautas da ABESPetro: fortalecer as capacidades tecnológicas, produtivas e organizacionais das empresas que integram a indústria brasileira de petróleo e gás, promovendo cooperação, aprendizagem e desenvolvimento entre seus diferentes elos.

Para tanto, não basta incorporar tecnologias ou estabelecer exigências contratuais e regulatórias. É necessário criar condições para que o conhecimento seja adquirido, compartilhado e transformado em capacidades efetivas. Modelos de

contratação, incentivos econômicos, estruturas de governança e relações entre empresas podem favorecer ou dificultar esse processo.

O compêndio oferece uma contribuição ao reunir diferentes perspectivas teóricas e propor um modelo integrador para aplicação setorial. Ao reconhecer que não existem soluções universais, valoriza a aprendizagem organizacional, a Cultura Justa, a resiliência e a compreensão do trabalho como realizado, e não apenas como prescrito.

Essa orientação ganha importância diante da digitalização, da automação, da inteligência artificial e das transformações da indústria de energia. A sofisticação tecnológica amplia a necessidade de desenvolver competências para interpretar informações, tomar decisões e responder a situações que não podem ser previstas em sua totalidade.

Para a ABESPetro, esta publicação demonstra também o valor da cooperação entre empresas, profissionais e instituições acadêmicas na produção e disseminação do conhecimento. Registro meu reconhecimento a todos que contribuíram para sua realização e, em especial, à coragem daqueles que assumiram o desafio de concebê-la e conduzi-la.

Espero que a obra estimule o debate, a investigação e, sobretudo, a transformação do conhecimento em práticas capazes de elevar os padrões de segurança e confiabilidade de nossa indústria.

Uma indústria tecnologicamente avançada não é apenas aquela que dispõe de equipamentos sofisticados, mas aquela que acumula as capacidades necessárias para utilizá-los, aperfeiçoá-los e adaptá-los a novos desafios.

E, para avançar nessa direção, conhecimento e competência são indispensáveis. Mas é preciso, também, coragem para questionar o estabelecido, enfrentar incertezas e construir novos caminhos.

Telmo Ghiorzi
Presidente-Executivo da ABESPetro
Associação Brasileira das Empresas de Bens e Serviços de Petróleo
Rio de Janeiro, novembro de 2026





Parte I

Fundamentos e evolução histórica de Fatores Humanos

Autores: Rafael Ceni de Almeida e Eder Henriqson

1.1 Conceitos Fundamentais de Fatores Humanos

1.1.1 O Que Vem a Ser Fatores Humanos?

De forma simples e direta, **Fatores Humanos é o campo que estuda a influência mútua entre os seres humanos e o sistema de trabalho do qual fazem parte** – como esse sistema condiciona o desempenho das pessoas e como as pessoas fazem o sistema funcionar. O que fazemos, por que fazemos e como fazemos dependem, portanto, das condições organizacionais, tecnológicas, ambientais e individuais, dentre outras, sob as quais o trabalho é efetivamente realizado. O conhecimento produzido pelo campo orienta a intervenção sobre essas condições, sobretudo por meio do projeto do trabalho, para favorecer, ao mesmo tempo, o desempenho do sistema e o bem-estar de quem nele atua.

No plano internacional, a Associação Internacional de Ergonomia (IEA) utiliza os termos Ergonomia e Fatores Humanos de forma intercambiável (por exemplo, Fatores Humanos/Ergonomia – FHE ou EFH), e define Fatores Humanos (ou Ergonomia) como:

> *"A disciplina científica que trata da compreensão das interações entre os seres humanos e outros elementos de um sistema, e a profissão que aplica teoria, princípios, dados e métodos ao projeto a fim de otimizar o bem-estar humano e o desempenho global do sistema" — International Ergonomics Association (IEA), 2000.*

No plano regulatório brasileiro, a NT nº 10/2023 da ANP, com base no CCPS – Center for Chemical Process Safety (2019) e no HSE – Health and Safety Executive (1999), define fatores humanos como:

> *"Todos os fatores organizacionais, ambientais, tecnológicos e individuais que influenciam o comportamento no trabalho de uma forma que pode afetar a saúde e a segurança" — ANP, 2023, item 1.2.*

Nota terminológica: As duas definições acima são complementares. A da IEA descreve o campo de conhecimento; a da NT n.º 10/2023, os fatores que influenciam o comportamento no trabalho e que a gestão e a regulação acompanham. A própria NT reconhece essa dupla acepção: no mesmo item 1.2, registra que associações como a ABERGO e a CIEHF tratam Fatores Humanos como sinônimo de Ergonomia e, no item 1.3, delimita como escopo regulado a adequação dos projetos das instalações e das tarefas às capacidades físicas e cognitivas dos trabalhadores – o núcleo de projeto que caracteriza o campo. Para distinguir os dois usos, este compêndio escreve Fatores Humanos com iniciais maiúsculas, sem artigo e com verbo no singular – quando se refere ao campo ("Fatores Humanos é...", "de Fatores Humanos"), e os fatores humanos com artigo, em minúsculas e no plural – quando se refere aos fatores ("os fatores humanos são..."). É a mesma regra que vale para nomes próprios no plural: sem artigo, o verbo fica no singular ("Minas Gerais é"); com artigo, vai para o plural ("os Estados Unidos são"). Shorrock (2019b) adota solução semelhante em inglês, usando maiúsculas quando fala da disciplina e minúsculas quando fala da expressão tal como é usada no dia a dia. Os sentidos que a expressão costuma assumir no uso corrente são apresentados na Reflexão Conceitual, adiante.

Para além das definições normativas, uma formulação útil para situar o foco contemporâneo do campo é proposta por Henriqson:

> *"Fatores Humanos é o campo de conhecimento científico interdisciplinar que estuda a relação interativa entre os seres humanos e os sistemas de trabalho nos quais estão inseridos – suas tecnologias, processos e rotinas operacionais. Seu propósito é compreender, de um lado, como esses sistemas dependem da contribuição humana para operar e, de outro, como condicionam o desempenho das pessoas que neles atuam" — Henriqson, 2026.*

Essa formulação destaca um deslocamento conceitual importante: o objeto de Fatores Humanos não é o ser humano isolado, nem o sistema técnico em si, mas **a relação interativa entre eles**. Sistemas sociotécnicos contemporâneos só funcionam porque pessoas reconciliam continuamente as imperfeições do projeto do trabalho e dos sistemas que o sustentam com as exigências do contexto; ao mesmo tempo, esses sistemas – suas tecnologias, procedimentos, pressões e estruturas – moldam o que é possível, o que é difícil e o que é inseguro fazer.

Reflexão Conceitual

De forma aparentemente contraintuitiva, porém conceitualmente importante, numa visão contemporânea ou sistêmica, **Fatores Humanos não é o plural de "fator humano"**. No uso corrente, a expressão assume três sentidos distintos do campo (Shorrock, 2017a, 2017b, 2017c): o *fator humano*, a pessoa vista como fonte de falha em um sistema supostamente bem projetado; *os fatores do ser humano*, capacidades e limitações como atenção, memória e fadiga; e os fatores que afetam *o ser humano*, como equipamentos, procedimentos e cultura. Os dois últimos reúnem conhecimento valioso e orientam boa parte da prática e da regulação; o primeiro tende a reduzir a explicação a quem errou. **O campo de Fatores Humanos vai além dos três ao se ocupar da interação entre esses elementos no sistema sociotécnico** (Shorrock, 2017d). Tampouco se trata, primordialmente, de analisar ou corrigir comportamentos individuais. Por isso, "fator humano" não é causa de acidente nem conclusão de investigação: é o ponto em que a análise de Fatores Humanos começa (Shorrock, 2019b).

Uma síntese conceitualmente útil vem de Bridger (2021):

> *"Fatores Humanos não é sobre pessoas. É sobre as condições de trabalho em uma organização e como elas afetam as pessoas"*
> — R. S. Bridger, 2021.

A formulação é deliberadamente provocativa: não nega o protagonismo do ser humano, mas redireciona o foco analítico – o objeto de intervenção em Fatores Humanos não é o indivíduo isolado, mas o sistema sociotécnico do qual ele é parte indissociável. Assim, em vez de perguntar "quem errou?", a abordagem de Fatores Humanos convida a refletir:

"Que condições de trabalho tornaram esse resultado possível?"

"O que fazia sentido para as pessoas envolvidas, naquele momento, considerando as condições em que atuavam?"



Essa mudança de olhar é central para práticas modernas de segurança, de aprendizado organizacional e de construção de sistemas mais confiáveis e resilientes.

Redirecionar o foco às condições de trabalho, contudo, não dissolve a responsabilidade individual: pessoas em todos os níveis fazem escolhas, e o pensamento sistêmico não deve servir para diluí-las "no sistema" (Shorrock, 2017d; ver nota sobre *accountability*, seção 1.1.5).

Dessa compreensão decorre a definição que orienta este volume:



Definição adotada neste compêndio

Fatores Humanos é um campo científico interdisciplinar que, a partir de uma perspectiva sistêmica, estuda a relação interativa entre as pessoas e os sistemas de trabalho, considerando suas dimensões organizacionais, tecnológicas, ambientais e individuais, entre outras, e reconhecendo que os resultados do trabalho emergem dessa interação. Seu propósito é compreender essas relações e intervir sobre as condições que as moldam, visando otimizar, de forma integrada, a segurança, o bem-estar humano e o desempenho dos sistemas sociotécnicos complexos.

Nota: *A adoção desta formulação não invalida as definições anteriores – cada uma ilumina uma faceta legítima de um campo amplo e interdisciplinar. Trata-se de uma referência de trabalho, adotada para dar unidade a este compêndio – não de uma definição única ou definitiva de Fatores Humanos.*

1.1.2 As Quatro Dimensões de Fatores Humanos

Os fatores que influenciam o desempenho humano podem ser agrupados em quatro grandes dimensões interdependentes. A influência não é unidirecional: as pessoas também moldam esses fatores – a escala de turnos condiciona o comportamento, mas os trabalhadores também modificam, por exemplo, por meio de trocas de turno (Shorrock, 2017c). As dimensões são:

- **Dimensão Organizacional:** Inclui a estrutura hierárquica, políticas, cultura, sistemas de gestão, pressões de produção, alocação de recursos, comunicação interna e processos decisórios. A organização cria o contexto no qual o trabalho acontece.
- **Dimensão Individual:** Engloba as capacidades e limitações cognitivas, habilidades físicas, experiência, treinamento, fadiga, estresse, motivação e estado emocional dos trabalhadores. Reconhece-se que o ser humano, por sua natureza flexível e variável, é o elo mais importante na cadeia de operações.
- **Dimensão Tecnológica:** Refere-se ao design de equipamentos, interfaces humano-máquina, automação, sistemas de alarme, controles, displays e ferramentas de trabalho. O foco está em adaptar a tecnologia às capacidades humanas, não o contrário.
- **Dimensão Ambiental:** Compreende as condições físicas do local de trabalho: iluminação, ruído, temperatura, vibração, espaço físico, acesso a equipamentos e layout das instalações. Inclui também aspectos sociais do ambiente, como dinâmicas de equipe e cultura local.

1.1.3 Fatores Humanos como Campo Interdisciplinar

Fatores Humanos é um **campo da ciência interdisciplinar** que integra conhecimentos de múltiplas áreas para compreender e otimizar o desempenho dos sistemas sociotécnicos – reconhecendo que as pessoas não estão à parte desses sistemas, mas são componentes essenciais e indissociáveis deles. Esta característica interdisciplinar é fundamental para abordar a complexidade dos ambientes de trabalho modernos, especialmente em indústrias de alto risco, como as do setor de petróleo e gás.

Uma forma útil de visualizar o escopo de Fatores Humanos é considerar sua relação com domínios da ciência e da engenharia. A Figura 1.1.1 ilustra esta estrutura, onde os itens são posicionados próximos a outros com os quais se relacionam.



Figura 1.1.1: Domínios de Fatores Humanos. Adaptado de Lee et al. (2017).

No centro do círculo está o domínio nuclear de Fatores Humanos, e imediatamente ao seu redor encontram-se os diversos subdomínios de estudo: Psicologia da Engenharia, Ergonomia, Engenharia Cognitiva, Macroergonomia, Interação Humano-Computador e Integração Humano-Sistemas. Além dos subdomínios centrais, Fatores Humanos dialoga intensamente com diversas outras disciplinas, que contribuem para sua base científica e suas aplicações práticas, como Psicologia Experimental, Design Industrial, Ciência Cognitiva, Psicologia Organizacional, entre outras (Lee et al., 2017).

A natureza interdisciplinar de Fatores Humanos impõe um desafio crítico às organizações: a superação de abordagens fragmentadas e departamentalizadas. Tradicionalmente, aspectos como segurança, qualidade, treinamento, engenharia e operações são tratados em "silos" funcionais, cada qual com seus próprios indicadores,

prioridades e linguagem. Esta fragmentação não apenas dificulta a compreensão sistêmica dos fenômenos que afetam o desempenho humano, como pode gerar conflitos de prioridades e lacunas de responsabilidade.

Uma aplicação efetiva de Fatores Humanos demanda, portanto, uma visão holística e integrada – tanto internamente (entre departamentos e níveis hierárquicos de uma organização) quanto externamente (entre os diversos elos da cadeia de valor do setor, incluindo operadoras, empresas de serviços, fabricantes de equipamentos e órgãos reguladores). É nesta integração horizontal e vertical que reside a possibilidade de intervenções verdadeiramente eficazes e de uma cultura que transcenda as fronteiras organizacionais tradicionais.

1.1.4 A Visão Tradicional e a Nova Visão

A compreensão contemporânea de Fatores Humanos envolve o reconhecimento de duas visões distintas sobre segurança e erro humano:

- **Visão Tradicional (Old View):** Fundamenta-se em conceitos que remontam aos estudos de Heinrich (1931). O erro humano é visto como causa primária dos acidentes, e as pessoas são tratadas como problemas a serem controlados. Esta visão baseia-se na premissa de que as organizações seriam intrinsecamente seguras se não fossem pelas "falhas humanas" e conduziu a máximas sem base científica sólida, como "segurança é uma escolha do indivíduo" e/ou "todos os acidentes são evitáveis" (Bruno, 2022).
- **Nova Visão (New View):** Originou-se da escola de Engenharia de Sistemas Cognitivos (CSE), desenvolvida por Rasmussen, Hollnagel e Woods desde os anos 1970, cujas elaborações são detalhadas, respectivamente, nas Seções 2.3 (Perspectiva Rasmusseniana) e 2.4 (Engenharia de Resiliência). O termo foi cunhado por Dekker no início dos anos 2000 para distinguir entre abordagens "convencionais" e "novas" para compreensão do erro humano, que deixa de ser causa primária para ser compreendido como sintoma de condições sistêmicas mais profundas. Conforme Le Coze (2022), esta perspectiva reconhece que são as pessoas – gestores e trabalhadores – que criam segurança dinamicamente,

reconciliando demandas conflitantes e mantendo unidos sistemas inerentemente imperfeitos.

A Tabela 1.1.1 a seguir sintetiza as principais diferenças entre estas duas visões:

Visão Tradicional (*Old View*)	**Nova Visão (*New View*)**
O erro humano é a causa dos acidentes	O erro humano é sintoma de problemas sistêmicos
Sistemas seriam seguros sem pessoas erráticas	Pessoas criam segurança em sistemas imperfeitos
Foco em encontrar e punir culpados	Foco em aprender e melhorar o sistema
Conformidade 100% com procedimentos garante segurança	Variabilidade é necessária para adaptar-se a um mundo complexo
Pessoas são um problema a controlar	Pessoas são recursos a valorizar
Erro humano é ponto de parada da investigação	Erro humano é ponto de partida para aprendizado

Tabela 1.1.1: Comparação entre a Visão Tradicional e a Nova Visão. Adaptado de Dekker (2019) e Le Coze (2022).

É importante ressaltar que a Nova Visão não surgiu para substituir os sistemas de gestão de segurança estabelecidos, mas para ampliá-los e qualificá-los, incorporando perspectivas capazes de reconhecer a complexidade, a variabilidade e a natureza sociotécnica dos sistemas contemporâneos. Sua aplicação prática pode manifestar-se de diversas formas, tais como: análise de riscos, investigação de eventos com foco em aprendizado, análises e aprendizagens a partir do Trabalho como Realizado (WAD) e observações/visitas de campo orientadas à compreensão do contexto operacional. Mais do que acrescentar novas ferramentas, trata-se de transformar o olhar que orienta as práticas de segurança. Conforme será aprofundado na Parte III deste compêndio, a gestão efetiva de segurança beneficia-se da articulação entre diferentes abordagens, combinando perspectivas normativas, analíticas e adaptativas e buscando sinergias em vez de fomentar divisões e segregações entre escolas e perspectivas (Le Coze, 2024).

1.1.5 O Papel do Ser Humano em Sistemas Complexos

Para compreender o papel do ser humano em diferentes contextos operacionais, é importante distinguir entre três tipos de sistemas, conforme o framework Cynefin (Snowden & Boone, 2007):

- **Sistemas Simples** são caracterizados por relações claras de causa e efeito, visíveis a todos. As melhores práticas podem ser facilmente identificadas e replicadas. O trabalho pode ser padronizado e a resposta adequada é: perceber, categorizar e responder. Exemplo: seguir uma receita culinária ou um checklist de inspeção visual.
- **Sistemas Complicados** envolvem relações de causa e efeito que existem, mas não são imediatamente óbvias – requerem análise especializada para serem compreendidas. Existem múltiplas soluções corretas, e boas práticas (não "melhores práticas") podem ser desenvolvidas. A resposta adequada é: perceber, analisar e responder. Exemplo: o projeto de um motor de aeronave ou a engenharia de um sistema de controle de poço.
- **Sistemas Complexos** são aqueles em que as relações de causa e efeito só podem ser percebidas em retrospectiva – não são previsíveis antecipadamente. Esses sistemas são caracterizados por múltiplos agentes interagindo de formas não-lineares, onde pequenas mudanças podem produzir efeitos desproporcionais. Padrões emergem da interação entre os elementos, e a resposta adequada é: sondar, perceber e responder. Exemplo: o mercado financeiro, o clima organizacional ou uma operação de perfuração em águas profundas.

A Indústria de Energia como Sistema Sociotécnico Complexo

A indústria de energia opera predominantemente em sistemas sociotécnicos complexos – ambientes onde elementos técnicos (equipamentos, processos, tecnologia) e sociais (pessoas, equipes, cultura, organização) interagem de maneira dinâmica e interdependente (Rasmussen, 1997). Conforme Perrow (1984), esses sistemas frequentemente apresentam duas características críticas: complexidade interativa (interações inesperadas entre componentes) e acoplamento forte (pouca folga entre processos, permitindo que falhas se propaguem rapidamente)

– formulação cuja apresentação completa é feita na Seção 2.1 (Teoria dos Acidentes Normais).



Nesses ambientes, a variabilidade não é um defeito a ser eliminado, mas uma característica inerente que precisa ser compreendida e gerenciada: as condições mudam constantemente, procedimentos não conseguem antecipar todas as situações, e a incerteza residual é inevitável (Hollnagel, 2012) – premissa elaborada na Seção 2.4 como pressuposto central da Engenharia de Resiliência. O ser humano, por sua natureza flexível, adaptativa e variável, constitui, portanto, o elemento mais importante na cadeia de operações. Diferentemente de máquinas, as pessoas conseguem improvisar, interpretar contextos ambíguos e adaptar sua interação com o sistema às situações não previstas.

Estas características humanas são fundamentais para reconciliar as lacunas entre o trabalho como imaginado (WAI – Work-as-Imagined) e o trabalho como efetivamente realizado (WAD – Work-as-Done) – distinção cujo detalhamento conceitual é apresentado na Seção 2.4 –, que resulta da complexidade, incerteza e variabilidade inerentes às operações (Hollnagel, 2014). Compreender essa lacuna – em vez de simplesmente tentar eliminá-la – permite às organizações identificar onde as adaptações cotidianas contribuem para o sucesso operacional e onde podem introduzir riscos não reconhecidos. A mesma capacidade adaptativa que permite aos trabalhadores manter o sistema funcionando sob condições adversas pode, em determinados contextos, aproximar as operações de limites de segurança sem que isso seja percebido (Dekker, 2019).

Conforme Dekker (2019), sistemas complexos operando sob pressão competitiva sempre precisam atender múltiplos objetivos conflitantes simultaneamente, com recursos limitados. São as pessoas que reconciliam essas demandas e mantêm unidos sistemas inerentemente imperfeitos. Não importa quão robustos sejam os sistemas técnicos – são gestores e trabalhadores que gerenciam as incertezas do trabalho, garantindo segurança e eficiência operacional.

Condições para o Desempenho Humano Eficaz

Uma condição fundamental para o desempenho humano eficaz é a existência de um ambiente de **confiança, colaboração e *accountability*** – condições habilitadoras que a Seção 3.2.10 consolida como segurança psicológica (ancorada na confiança) e Cultura Justa –, no qual os trabalhadores se sintam seguros para reportar problemas e assumir responsabilidade por suas ações, sem medo de punição (Edmondson, 2019). Esse tipo de ambiente favorece a participação ativa, promovendo o aprendizado organizacional, a melhoria contínua e a inovação – elementos essenciais para a resiliência do sistema de trabalho como um todo.

Nota sobre *accountability*: o termo é mantido em inglês por não haver tradução direta adequada em português. Deriva de account (relatar, descrever) e refere-se à **capacidade de prestar contas sobre as próprias ações e suas consequências** – distinguindo-se de "responsabilidade" (a obrigação de executar uma tarefa) e de "responsabilização" em sentido punitivo. Uma cultura de accountability saudável combina autonomia com compromisso: as pessoas têm liberdade para decidir no contexto do seu trabalho e, quando os resultados não saem como esperado, orientam-se ao aprendizado coletivo e à melhoria dos sistemas – não apenas à explicação retrospectiva do ocorrido. Ver Seção 3.3.



1.2 Evolução Histórica de Fatores Humanos e da Ciência da Segurança

1.2.1 Introdução à Evolução Histórica

A compreensão da evolução histórica de Fatores Humanos e da Ciência da Segurança constitui elemento fundamental para a contextualização das abordagens contemporâneas. Embora fortemente inter-relacionados, ambos os campos possuem origens parcialmente independentes: Fatores Humanos – campo científico interdisciplinar de escopo mais amplo (ver 1.1.3) – emergiu da ergonomia aplicada a partir da década de 1940 (ver 1.2.2), enquanto a Ciência da Segurança consolidou-se a partir dos estudos de segurança industrial desenvolvidos no início do século XX (ver 1.2.3).

Como argumenta Dekker (2019), a Ciência da Segurança constitui-se ao longo de um século de tentativas de compreender acidentes e desastres – trajetória que confere o subtítulo de sua obra de referência, *A Century of Understanding Accidents and Disasters*. Esse percurso reflete uma transição de modelos lineares e centrados no indivíduo para perspectivas crescentemente sistêmicas e organizacionais, decorrente tanto de avanços teóricos quanto das lições extraídas de grandes acidentes industriais e das profundas transformações na forma de compreender o papel do ser humano em sistemas complexos.

O percurso histórico pode ser organizado em torno de tradições de pesquisa ou perspectivas teóricas que se sucederam e coexistem. Le Coze (2019) identifica sete tradições centrais estruturadas durante a chamada "idade de ouro" (*golden age*) da pesquisa em segurança, nas décadas de 1980 e 1990; Rosness et al. (2010) propõem seis perspectivas para a análise de acidentes organizacionais. Embora estas perspectivas tenham emergido em sequência cronológica, é importante reconhecer que não se substituíram completamente, coexistindo nas organizações industriais contemporâneas em diferentes graus.

1.2.2 O Nascimento de Fatores Humanos (1940s)

O nascimento formal do campo de Fatores Humanos pode ser localizado durante a Segunda Guerra Mundial, com o trabalho pioneiro de **Alphonse Chapanis, Paul Fitts e Richard Jones**. Este momento histórico representa uma mudança paradigmática fundamental: a transição da culpabilização do operador para o reconhecimento de que padrões de erro estão sistematicamente conectados ao design dos equipamentos e ao contexto de trabalho.

Em 1943, Lt. Alphonse Chapanis, então o único psicólogo em Wright Field, Ohio, – foi designado para investigar por que pilotos e copilotos de **P-47, B-17 e B-25** frequentemente retraíam o trem de pouso em vez dos flaps após o pouso (Roscoe, 1997, *apud* Dekker, 2019, p. 142). O diagnóstico foi surpreendentemente simples: nesses aviões, os controles de trem de pouso e flaps eram interruptores ou alavancas idênticos ou quase idênticos, posicionados lado a lado, podendo ser facilmente confundidos. No C-47, em que os controles tinham formas e modos de acionamento diferentes e não eram adjacentes, esse tipo de erro praticamente não ocorria.

Como solução imediata em tempo de guerra, Chapanis introduziu o que ficaria conhecido como ***shape coding***: fixou uma pequena roda de borracha na extremidade do controle do trem de pouso e uma forma de cunha no controle dos flaps em diversos tipos de aeronaves, permitindo distinção tátil pelo piloto. Os acidentes praticamente desapareceram. Após a guerra, esses controles tátilmente discriminá-veis foram padronizados mundialmente (Dekker, 2019, pp. 142–143).

Em 1947, Paul Fitts e Richard Jones publicaram um estudo sistemático de 460 relatos de erros em controles de aeronaves, concluindo que:

> *"deve ser possível eliminar uma grande proporção dos chamados acidentes por 'erro do piloto' projetando equipamentos de acordo com os requisitos humanos" (Fitts & Jones, 1947, p. 332)*

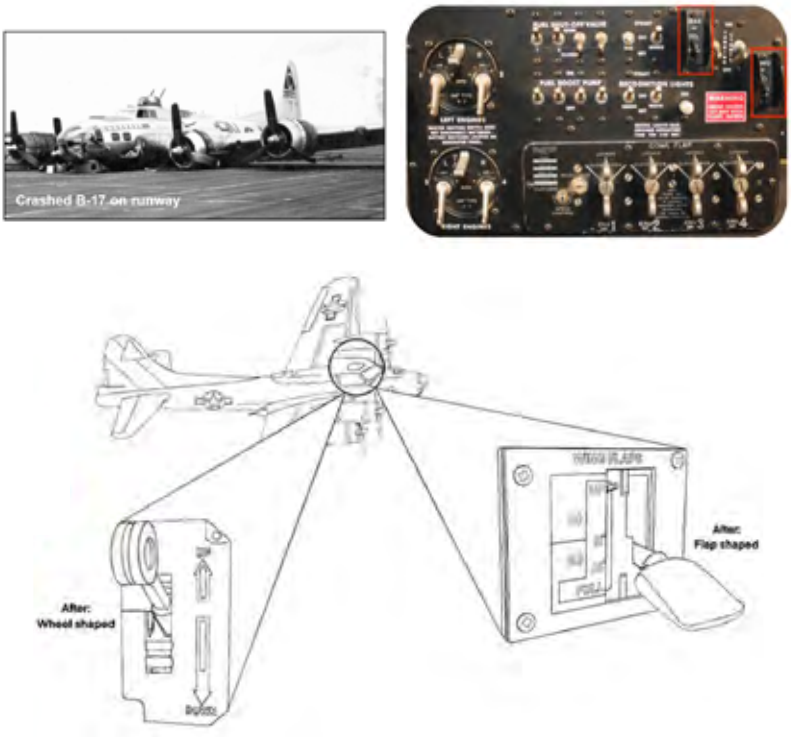


Figura 1.2.1: O nascimento de Fatores Humanos: Chapanis e o conceito de *shape coding* nos controles de aeronaves (1943). **Fontes das Imagens:** https://www.machinedesign.com/community/article/21143885/human-factors-engineers-unsung-partners-in-design e https://uxmag.com/articles/pilot-error-chapanis-and-the-shape-of-things-to-come

Esta consolidação intelectual marcou o nascimento de um novo campo voltado a adaptar a tecnologia ao ser humano, e não o contrário. A categoria "erro de piloto" passa, pela primeira vez, a ser colocada entre aspas – sinalizando a suspeita dos pesquisadores quanto ao termo: o erro deixa de ser tratado como **causa** do problema e passa a ser entendido como seu **sintoma**, sistematicamente conectado a características das ferramentas, tarefas e ambientes de trabalho (Dekker, 2019, p. 143).

Esta mudança de paradigma – de culpar o operador para questionar o design do sistema – representa a semente intelectual que florescerá décadas depois nas perspectivas organizacionais e sistêmicas, conforme será observado nas próximas seções.

1.2.3 Da Era Industrial à Segurança Tradicional (1900-1970)

O início do século XX marcou a emergência sistemática das preocupações com segurança no ambiente industrial. A Revolução Industrial havia transformado radicalmente as condições de trabalho, expondo trabalhadores a riscos sem precedentes; a produção de leis, o desenvolvimento de padrões técnicos, as inspeções de fábricas e os arranjos burocráticos de segurança já compunham um conjunto crescente de métodos, princípios, ferramentas e práticas associados ao controle de operações perigosas (Le Coze, 2019).

Herbert William Heinrich (1886–1962), então *Assistant Superintendent of the Engineering and Inspection Division* da Travelers Insurance Company, publicou em 1931 a obra *Industrial Accident Prevention: A Scientific Approach*, baseada em uma análise de cerca de 75.000 reclamações de seguro industrial (Dekker, 2019, p. 88). A obra estabeleceu conceitos que dominariam o pensamento sobre segurança por décadas, incluindo a "**pirâmide de acidentes**" (ratio fixo entre acidentes graves, menores e quase-acidentes) e a "**Teoria do Dominó**".

O modelo do dominó (Figura 1.2.2) propunha que os acidentes resultam de uma sequência linear de cinco fatores: ambiente social/ancestralidade → falha da pessoa → ato/condição insegura → acidente → lesão. A contribuição de Heinrich foi restabelecer a tese, perdida durante o auge da teoria de "propensão a acidentes", de que muitos acidentes e lesões são preveníveis por meio da interrupção da cadeia causal (Dekker, 2019). Contudo, três das principais teses de Heinrich foram posteriormente refutadas: (i) a tese da causação linear e única; (ii) a tese do *ratio* fixo entre eventos; e (iii) a afirmação de que 88% dos acidentes industriais decorrem de "atos inseguros" do trabalhador (Dekker, 2019, p. 87). Esta última tese estabeleceu o paradigma de "culpa da vítima" (*blame the victim*) que persiste em muitas organizações.



A década de 1970 foi marcada por acidentes que desafiaram as premissas da segurança convencional: Flixborough (1974), Seveso (1976) e Three Mile Island (1979). Estes eventos demonstraram que acidentes em sistemas complexos não podiam ser explicados simplesmente como "erro humano".



Figura 1.2.2: Modelo dominó de causalidade de acidentes. Fonte: Adaptado de Heinrich (1931).

Concepções de Risco e Causalidade: A Perspectiva de Energia e Barreira

A segurança tradicional estabeleceu os fundamentos de uma das formas mais influentes de pensar a prevenção de acidentes, denominada por Rosness et al. (2010, Cap. 4) **perspectiva de energia e barreira**:

Concepção 1 — Risco como energia a ser contida:

Heinrich (1931), Gibson (1961) e Haddon (1970, 1980) desenvolveram a noção de que acidentes representam a liberação descontrolada de energia quando sistemas de contenção (barreiras) falham. Esta visão concebe o risco como energia física nociva que deve ser controlada por meio de barreiras físicas e procedimentais; a segurança é alcançada interpondo barreiras entre fontes de energia e alvos vulneráveis, e o risco pode ser calculado matematicamente em função de probabilidade e consequências. Esta concepção fundamenta até hoje muitas práticas de segurança industrial, incluindo a análise de barreiras e os modelos de defesa em profundidade.

1.2.4 A Tradição Organizacional: Incubação, Fatores Latentes e Acidentes Sistêmicos (1970–1990)

As décadas de 1970 e 1980 foram marcadas por acidentes industriais catastróficos que desafiaram as premissas da segurança tradicional: **Three Mile Island (1979)**, **Bhopal (1984)**, **Challenger (1986)**, **Chernobyl (1986)** e **Piper Alpha (1988)**. Estes eventos evidenciaram que acidentes em sistemas complexos transcendem os "atos inseguros" individuais, revelando padrões sistêmicos envolvendo múltiplos níveis organizacionais, decisões gerenciais e deficiências de design (Dekker, 2019).

Neste período, o foco do pensamento sobre segurança expandiu-se do indivíduo para as organizações. Esta expansão deu origem a tradições de pesquisa fundadoras que ainda estruturam o campo.

Turner e a Teoria dos Desastres Antropogênicos: A Incubação do Acidente

Barry Turner (1978), em sua obra seminal *Man-Made Disasters*, propôs que acidentes não são eventos súbitos, mas o desfecho de um **período de incubação,** frequentemente de anos, durante o qual sinais de perigo se acumulam e são ignorados, mal interpretados ou descartados pelo sistema organizacional. Turner identificou nesse processo um padrão recorrente: a presença de "premissas centrais" (*core assumptions*) que tornam o sistema cego a eventos que as contradizem. A obra, posteriormente expandida com Nick Pidgeon (Turner & Pidgeon, 1997), funda o que Le Coze (2019) identifica como uma das tradições centrais da Ciência da Segurança: **Incubação, Cultura de Segurança e Aprendizagem**.

Rosness et al. (2010, Cap. 7) dedicam à teoria de Turner uma das seis perspectivas de sua tipologia, sob o título de **"perspectiva do processamento de informação"**, segundo a qual o acidente é compreendido como uma falha no fluxo, na interpretação e na disseminação de informações dentro da organização. Conceitos como o de *requisite imagination* (Westrum, 1993; ver Rosness et al., 2010, Cap. 7), a capacidade organizacional de antecipar eventos para os quais ainda não existe precedente, derivam diretamente desta tradição e nutrem, posteriormente, o debate sobre cultura de segurança.

Reason e o Modelo de Defesas em Camadas (posteriormente "Queijo Suíço")

James Reason, psicólogo cognitivo britânico, publicou em 1990 a obra *Human Error*, na qual desenvolveu um modelo de causação de acidentes que retomava e expandia a distinção, originalmente sugerida por Rasmussen (1980), entre **erros ativos** e **erros latentes** (também denominados "patógenos residentes"). O modelo original de 1990 representava uma sequência de cinco "planos" – decisores de alto nível, gerência de linha, pré-condições, atividades produtivas e defesas – em que erros latentes nas camadas superiores criariam, ao longo do tempo, condições propícias a falhas no nível operacional (Dekker, 2019, pp. 308–313).

A iconografia hoje popularizada como **"queijo suíço"** – múltiplas camadas de defesa com furos que ocasionalmente se alinham, permitindo que uma trajetória de acidente atravesse o sistema – emerge em incarnações posteriores do modelo, sendo consolidada em Reason (1997) e refinada em Reason, Hollnagel & Pariès (2006). Como observa Dekker (2019, p. 312), na versão original de 1990 "*o termo 'queijo suíço' ainda não havia sido cunhado para este modelo*".

A contribuição fundamental de Reason foi redirecionar a atenção para além do operador da linha de frente, reconhecendo que "atos inseguros" são frequentemente herdados de "condições latentes" criadas por decisões organizacionais anteriores. Como o próprio Reason articulou:

> *"Em vez de serem os principais instigadores de um acidente, os operadores tendem a ser os herdeiros de defeitos do sistema criados por design ruim, instalação incorreta, manutenção falha e decisões gerenciais inadequadas. Sua parte é, geralmente, a de adicionar o toque final a uma poção letal cujos ingredientes já estão há muito sendo cozidos" (Reason, 1990, p. 173, citado em Dekker, 2019, p. 312)*

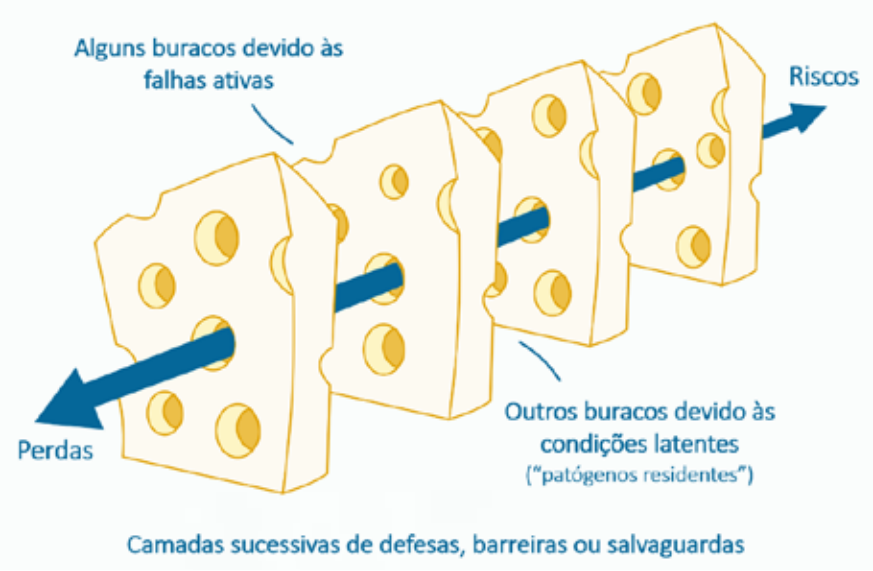


Figura 1.2.3: Modelo de defesas em camadas – posteriormente conhecido como Modelo do Queijo Suíço – de James Reason. **Fonte:** Adaptado de Reason (1990, 1997).

Concepções de Risco e Causalidade: A Virada Organizacional

Este período marca o surgimento de novas formas de conceber o risco, que expandem a compreensão para além das barreiras físicas:

Concepção 2 — Risco como propriedade estrutural da complexidade:

Em 1984, o sociólogo Charles Perrow publicou Normal Accidents, argumentando que em sistemas com certas características estruturais – alta complexidade *interativa e acoplamento apertado – acidentes não são anomalias evitáveis, mas consequências esperadas da própria arquitetura do sistema. O risco é, portanto, uma propriedade estrutural do sistema, não apenas falha humana ou técnica. Esta tese provocativa desafiou a premissa de que acidentes sempre podem ser prevenidos por meio de melhor gestão ou mais controles. A perspectiva completa de Perrow é apresentada na Seção 2.1 deste compêndio.*

Concepção 3 — Sistemas complexos podem ser altamente confiáveis:

Na mesma década em que Perrow publicava suas previsões pessimistas, pesquisadores da Universidade da Califórnia em Berkeley iniciavam um programa de pesquisa que revelaria um paradoxo empírico: algumas organizações que operam tecnologias intrinsecamente perigosas – porta-aviões, controle de tráfego aéreo, usinas nucleares – conseguiam manter registros de segurança extraordinários durante longos períodos. Esta descoberta abriu uma nova linha de investigação sobre as características organizacionais que tornam isto possível, detalhada na Seção 2.2.

Sofisticação da Concepção 1 — Defesas em profundidade:

O modelo de Reason (1990) representa uma sofisticação do modelo de barreiras. Embora preserve premissas fundamentais como a linearidade e as defesas em camadas, Reason introduz a distinção crucial entre "condições latentes" e "erros ativos", direcionando a atenção para além do operador da linha de frente (sharp end) e para o nível organizacional (blunt end).

1.2.5 A Virada Sistêmica e Perspectivas Contemporâneas (anos 1980 ao presente)

A periodização da virada sistêmica não é trivial. Conforme observa Le Coze (2019), as décadas de 1980 e 1990 constituíram uma **"idade de ouro"** (*golden age*) da pesquisa em segurança, durante a qual se consolidaram as principais tradições teóricas que estruturam o campo até hoje. Obras seminais como Turner (1978), Perrow (1984), Rasmussen (1986), Reason (1990), Vaughan (1996), Rasmussen (1997) e Weick & Sutcliffe (2001) demarcam essa consolidação. Pesquisadores como **Jens Rasmussen, James Reason, Nancy Leveson, Erik Hollnagel, David Woods, Karl Weick e Kathleen Sutcliffe** desenvolveram, ao longo desse período, abordagens que reconheciam a natureza complexa, adaptativa e emergente dos sistemas sociotécnicos.

Rasmussen (1986, 1997), engenheiro eletricista e pesquisador em Fatores Humanos e engenharia cognitiva do Risø National Laboratory, propôs modelos que reconhe-

ciam a natureza dinâmica das organizações sob pressões competitivas. Sua análise multinível – do operador individual aos reguladores governamentais – ofereceu um enquadramento para compreender como decisões em diferentes níveis organizacionais interagem para produzir condições de risco. A perspectiva Rasmusseniana é apresentada na Seção 2.3.

O período também foi marcado pelo debate acadêmico entre a **Teoria dos Acidentes Normais (NAT)** de Perrow e a **Teoria da Alta Confiabilidade (HRT)** do grupo de Berkeley. Enquanto Perrow argumentava que acidentes em sistemas complexos são inevitáveis, os pesquisadores de HRT demonstravam que certas organizações conseguiam operar com níveis extraordinários de segurança. Conforme Rijpma (1997, 2003), as relações entre as duas perspectivas são mais produtivas do que estritamente antagônicas – as duas teorias iluminam aspectos diferentes do mesmo fenômeno, e suas tensões são exploradas em profundidade na Seção 2.2.7.

No início do século XXI, a **Engenharia de Resiliência (RE)**, formalizada em Hollnagel, Woods e Leveson (2006), propôs uma reconceituação fundamental do próprio conceito de segurança. Em vez de focar exclusivamente na prevenção de falhas, esta perspectiva direciona a atenção para as capacidades adaptativas que permitem às organizações ter sucesso sob condições variadas e frequentemente inesperadas. A Seção 2.4 apresenta os fundamentos e desenvolvimentos desta abordagem.



Concepções de Risco e Causalidade: A Virada Sistêmica

As concepções contemporâneas completam a evolução do pensamento sobre segurança:

Concepção 4 — Risco como aceitação gradual:

A socióloga Diane Vaughan, em sua análise do desastre do Challenger publicada em 1996 (*The Challenger Launch Decision*), revelou como vulnerabilidades organizacionais podem se acumular gradualmente através de pequenas decisões que parecem racionais no momento em que são tomadas. Este fenômeno, denominado normalização do desvio, demonstrou que o risco possui uma dimensão temporal frequentemente negligenciada: não surge instantaneamente, mas se constrói de forma incremental.

A literatura especializada classifica o trabalho de Vaughan em diferentes tradições. Le Coze (2019) a situa no campo das **perspectivas socio-construtivistas** (junto a Westrum, Gephart, Pinch e Wynne), por sua atenção à construção social do significado e à cultura organizacional como mediadora da percepção do risco. Rosness et al. (2010, Cap. 8) a integram à perspectiva da **decisão sob objetivos conflitantes e deriva** (junto a Rasmussen, 1997, e Snook, 2000), por seu foco no processo gradual de migração das atividades em direção aos limites do desempenho aceitável. Neste compêndio, adota-se uma terceira leitura, articulando o trabalho de Vaughan à tradição da **Dependência de Trajetória** (*Path Dependency*), seguindo as interpretações propostas por Snook (2000) e Bills (2023). Esta escolha editorial busca enfatizar o caráter histórico-acumulativo dos processos analisados por Vaughan; sua fundamentação é detalhada na Seção 2.5.

Concepção 5 — Risco como problema de controle dinâmico:

Rasmussen (1997) propôs que organizações não permanecem estáticas em relação aos limites de segurança, mas migram dinamicamente em resposta a pressões de eficiência e carga de trabalho. Esta concepção reconhece que a variabilidade no desempenho não é aberração a ser eliminada, mas característica

fundamental de sistemas adaptativos que precisa ser compreendida e gerenciada. O modelo de migração aos limites é detalhado na Seção 2.3.

Nota importante: *As concepções aqui apresentadas representam marcos na evolução histórica do pensamento sobre risco e segurança. A Parte II deste compêndio detalha as perspectivas teóricas estruturadas que fundamentam a análise contemporânea de segurança em sistemas sociotécnicos – cada qual com seus pressupostos, conceitos fundamentais, forças e limitações.*

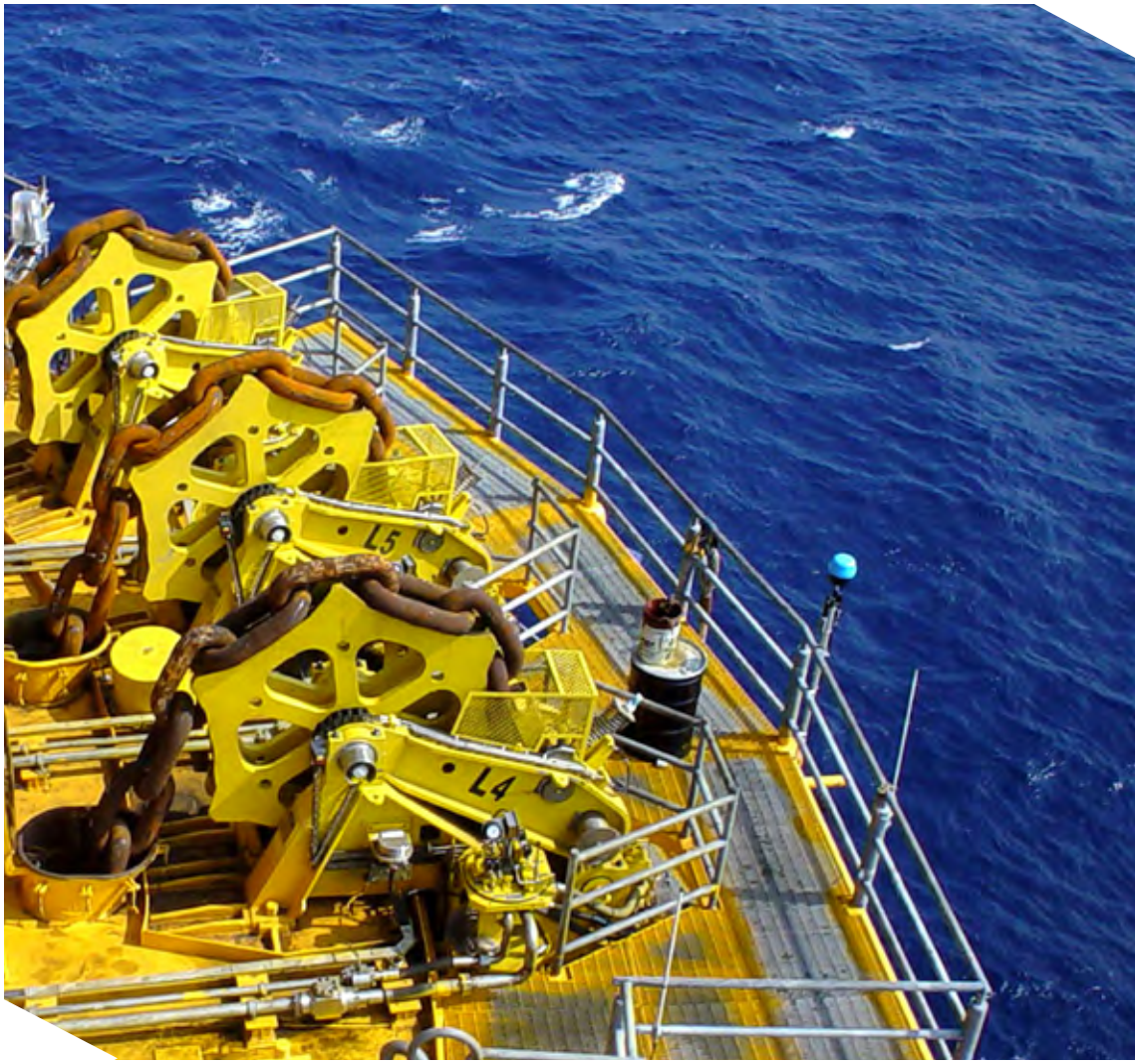
A Nova Segurança: a raiz comum dos movimentos contemporâneos

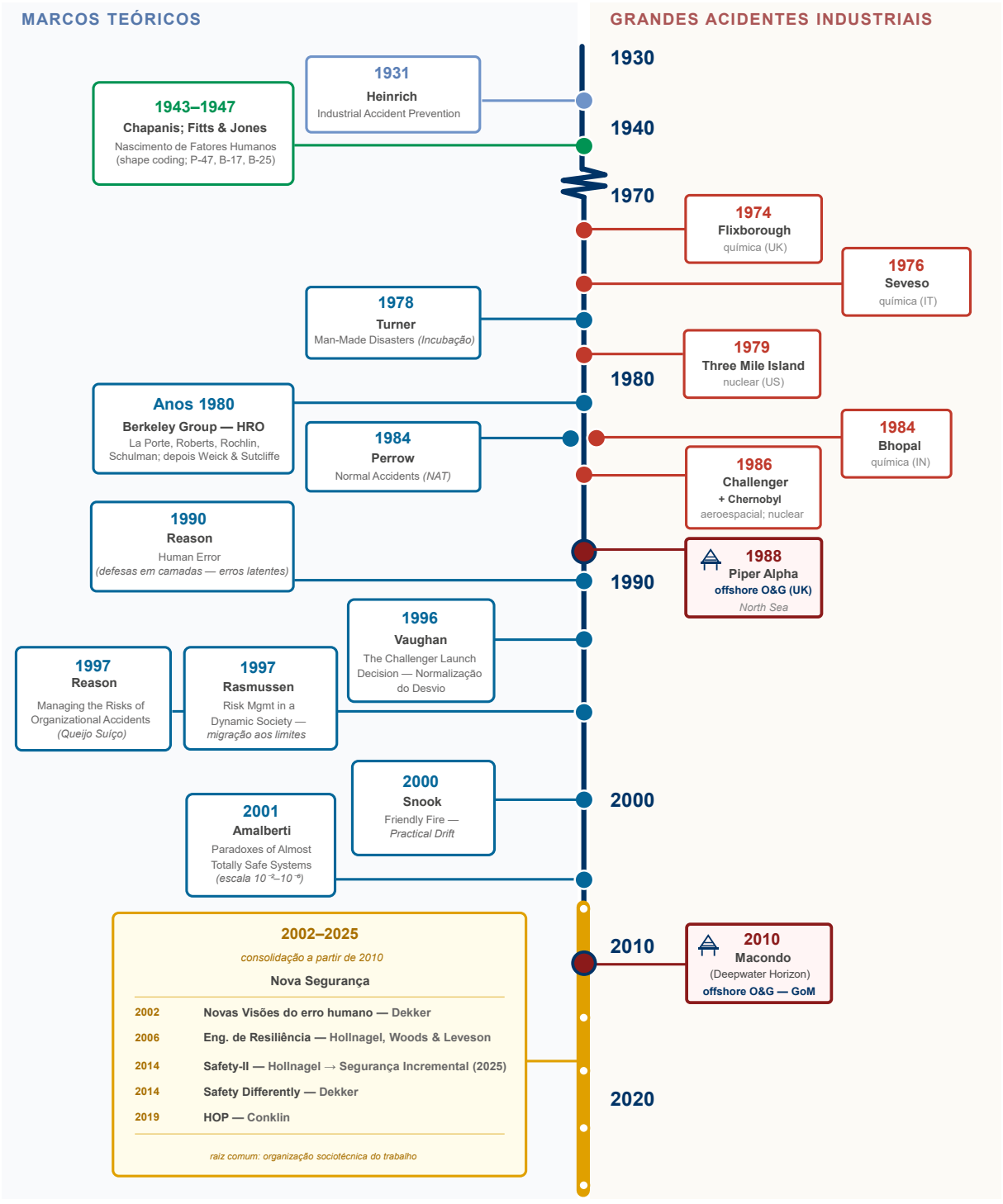
A partir dos anos 2000, e com maior nitidez após 2010, consolida-se um conjunto de movimentos que pode ser reunido sob a designação de **Nova Segurança**: as Novas Visões do erro humano (Dekker, 2002); a Engenharia de Resiliência (Hollnagel, Woods & Leveson, 2006), cuja comunidade fundadora reuniu, entre outros, Woods, Hollnagel, Leveson e, em sua primeira década, Dekker; o *Safety Differently* (Dekker, 2014); o *Safety-II* (Hollnagel, 2014) e sua reformulação recente como Segurança Incremental (Hollnagel, 2025, 2026); e o HOP (Conklin, 2019). Cada movimento tem vocabulário, autores de referência e públicos próprios, mas todos compartilham uma raiz comum: a retomada dos princípios da **organização sociotécnica do trabalho** como lógica para pensar a segurança. O que há de novo é menos o conteúdo do que o enquadramento para compreender como os arranjos sociotécnicos (tarefas, tecnologias, equipes, estruturas, metas e recursos) influenciam o desempenho de pessoas, equipes e organizações e, a partir daí, tornar os sistemas mais seguros. Neste compêndio, "Nova Visão" (Seção 1.1.4) designa a reconceituação do erro humano proposta por Dekker; "Nova Segurança" designa o conjunto mais amplo de movimentos que compartilham essa raiz.

Reconhecer essa raiz comum tem duas implicações práticas. A primeira é tratar esses movimentos como complementares, e não como escolas concorrentes, em coerência com a busca de sinergias adotada neste compêndio (Le Coze, 2024; ver Seção 3.1). A segunda é manter uma leitura crítica da proliferação de rótulos: parte da confusão conceitual em torno das "novas visões" associa-se à expansão

de um mercado de produtos e serviços de segurança (Le Coze, 2022), que tende a converter princípios em programas e marcas e, paradoxalmente, a alimentar a burocracia de segurança que esses mesmos movimentos criticam (Rae, Weber & Dekker, 2018). Para a indústria, importa menos a marca do que os princípios sociotécnicos que ela carrega.

A **Figura 1.2.4** sintetiza os marcos discutidos ao longo desta seção, demonstrando a interrelação histórica entre a maturação teórica do campo e os grandes acidentes industriais que sucessivamente lhe deram contornos.





LEGENDA

- **Segurança Tradicional** — modelos lineares de causação (Heinrich)
- **Fatores Humanos – o nascimento** — ergonomia, psicologia de engenharia e design centrado no humano
- **Ciência da Segurança** — perspectivas organizacionais e sistêmicas
- **Nova Segurança (2002–2025)** — Novas Visões, Resiliência, Safety-II, Seg. Incremental, Safety Differently, HOP
- **Grandes acidentes** — eventos catalisadores de mudança paradigmática
- **Acidentes em Óleo & Gás** — setor de referência deste compêndio

(na página anterior) Figura 1.2.4 – Evolução de Fatores Humanos e da Ciência da Segurança: Marcos teóricos, grandes acidentes industriais e paradigmas contemporâneos (1931–2025). **Fonte:** Autor a partir de Dekker (2019), Le Coze (2019) e Rosness et al. (2010 – SINTEF A17034). O agrupamento "Nova Segurança" é síntese dos autores (ver Seção 1.2.5).

Nota. A figura organiza, em linha do tempo, os principais marcos da trajetória de Fatores Humanos e da Ciência da Segurança ao longo do século XX e início do XXI. Os marcos estão classificados em ***seis categorias****, identificadas por cor e contorno:* ***(i) Segurança Tradicional (azul-claro)*** *– modelos lineares de causação centrados em atos inseguros (Heinrich, pirâmide de acidentes e Teoria do Dominó);* ***(ii) Fatores Humanos – marcos fundadores (verde)*** *– ergonomia, psicologia de engenharia e design centrado no humano;* ***(iii) Ciência da Segurança (azul)*** *– perspectivas organizacionais e sistêmicas;* ***(iv) Nova Segurança (dourado)*** *– marco único que agrupa as Novas Visões do erro humano (2002), a Engenharia de Resiliência (2006), o Safety-II e a Segurança Incremental (2014–2025), o Safety Differently (2014) e o HOP (2019);* ***(v) grandes acidentes industriais (vermelho)*** *– eventos catalisadores de mudança paradigmática; e* ***(vi) acidentes em Óleo & Gás (vermelho-marinho, com pictograma de plataforma offshore)*** *– setor de referência deste compêndio. A posição cronológica horizontal corresponde ao ano de publicação da obra teórica ou de ocorrência do acidente. A quebra de eixo entre 1950 e 1970 indica o intervalo de menor densidade de marcos relevantes para esta exposição. O marco da Nova Segurança é representado por um intervalo (2002–2025), e não por um ponto, por reunir movimentos que se consolidam ao longo de duas décadas, sobretudo a partir de 2010. As categorias indicam a tradição de origem predominante de cada marco, e não fronteiras entre campos: na construção sistêmica integrada neste compêndio (Seção 1.1), as perspectivas da Ciência da Segurança e a Nova Segurança dialogam com Fatores Humanos e integram o Ecossistema de Fatores Humanos (Parte III); o HOP, em particular, é tratado como expressão aplicada de Fatores Humanos (ver Seção 1.2.6).*

Esta pluralidade histórica é o que estrutura a ***Parte II*** *deste compêndio. Cada uma das perspectivas centrais visualizadas na figura é retomada em seção própria, com seus pressupostos, conceitos fundamentais, forças e limitações explicitados: a Teoria dos Acidentes Normais – NAT (Seção 2.1), a Teoria da Alta Confiabilidade – HRO (Seção 2.2), o modelo Rasmusseniano de migração aos limites (Seção 2.3), a Engenharia de Resiliência (Seção 2.4) e a Dependência de Trajetória (Seção 2.5). Os demais movimentos da* ***Nova Segurança*** *– Novas Visões do erro humano, Safety Differently, Safety-II/Segurança Incremental e HOP atravessam transversalmente várias dessas perspectivas e são tratados no contexto ao longo das Partes II e III.*

1.2.6 Da Atribuição do Erro Humano à Compreensão Sistêmica do Desempenho Humano

Os marcos apresentados nas seções anteriores podem ser lidos como um único movimento epistemológico: **o deslocamento de uma interpretação predominantemente individual do erro para uma compreensão sistêmica do desempenho humano**. No paradigma tradicional, acidentes são explicados pela identificação de quem errou, de qual regra foi descumprida ou de qual comportamento deveria ter sido diferente. Ao longo do século XX, porém, linhas de investigação diversas convergiram para essa leitura sistêmica: Fatores Humanos e a Ergonomia mostraram como o projeto de tarefas e de equipamentos condiciona o desempenho (já em Fitts e Jones, 1947); a teoria dos sistemas e a dos acidentes normais trataram o acidente como propriedade emergente de sistemas complexos e acoplados; a sociologia das organizações evidenciou a incubação de falhas e a

normalização do desvio; e os estudos de confiabilidade organizacional (HRO) e de engenharia de resiliência deslocaram a atenção para as condições latentes, para a migração do sistema sob pressões conflitantes e para a variabilidade cotidiana do desempenho (Perrow, Turner, Reason, Rasmussen, Hollnagel, Woods e Dekker, entre outros). Consolidou-se, assim, o entendimento de que as pessoas não podem ser analisadas separadamente do sistema em que atuam. A **Figura 1.2.5** traduz esse entendimento: a pessoa é a camada mais interna do próprio sistema sociotécnico, não a sua exceção. Nessa leitura, o desempenho, e o que se rotula como «erro», emerge das interações entre a ação individual e as condições que a cercam – da tarefa e tecnologia, da equipe e local de trabalho, da organização e do contexto –, as quais a própria ação, por sua vez, ajuda a moldar.



Figura 1.2.5 – A pessoa no sistema sociotécnico: As setas assinalam a ampliação do foco da análise, que parte da ação individual e alcança as condições do sistema sem dele sair. **Fonte:** autor, a partir de Rasmussen (1997), Wróbel (2021), DOE (2009) e IOGP (2019).

Esse deslocamento permite reexaminar criticamente uma das afirmações mais difundidas e mal compreendidas do campo: a de que aproximadamente **80% dos acidentes** seriam "**causados por erro humano**". Documentos de referência setoriais, como o *Human Performance Improvement Handbook* do *US Department of Energy* e o IOGP Report 453, retomam essa cifra não para responsabilizar o

indivíduo, mas para deslocar a análise em direção ao sistema: ao decompor a parcela classificada como "erro humano", associam a maior parte, da ordem de **70%, a fraquezas organizacionais latentes** e a fração restante, da ordem de **30%, à ação do trabalhador** mais próximo do evento (DOE, 2009; IOGP, 2019). Relações como 80/20 ou 70/30, contudo, carecem de sustentação científica robusta e não encontram consenso na literatura (Wróbel, 2021): valem como heurísticas, não como medidas. Sua riqueza não está nos percentuais, mas no deslocamento que provocam: em vez de tomar a parcela atribuída ao humano como o problema, reconhecer que, por trás dela, estão as condições de organização sociotécnica do trabalho. O que importa, afinal, é a perspectiva sistêmica, que supera a própria dicotomia entre "falha humana" e "falha do sistema".

Coerente com essa leitura, a investigação de um acidente não deve encerrar-se no "erro humano", mas prosseguir perguntando por que aquela ação ou decisão fez sentido para quem a tomou e quais condições do sistema a tornaram provável. O próprio IOGP Report 453 ilustra esse ponto ao reexaminar 350 incidentes inicialmente rotulados como possível descumprimento de regra: constatou que cerca de **90% decorriam de fatores do sistema**, tais como procedimentos pouco claros, limitações de capacidade e de recursos, problemas de rotulagem, alarmes ou ferramentas, e apenas uma parcela mínima de transgressão deliberada; padrão semelhante (da ordem de **95% relacionados ao sistema**) é relatado para a construção civil (IOGP, 2019). Esses fatores não são abstrações: materializam-se em decisões e arranjos verificáveis, dimensionamento de efetivo, backlog de manutenção e de gestão de mudanças (MOC), prioridades orçamentárias, desenho de contratos e interfaces entre organizações, distribuição de responsabilidades e qualidade da comunicação (IOGP, 2020). À medida que a análise se afasta do operador e amplia seu foco, tornam-se visíveis os fatores organizacionais enraizados nas estruturas das empresas, precisamente o alargamento representado na **Figura 1.2.5**. No setor de energia, esses arranjos assumem forma particularmente crítica na terceirização de atividades essenciais e nas interfaces entre contratantes e contratadas, que estruturam parte significativa do trabalho real e recebem tratamento dedicado na Seção 4.7 (Integração do Ecossistema Setorial).

A relação entre Fatores Humanos (FH) e Desempenho Humano (HP)

O termo Desempenho Humano (*Human Performance* – HP), com suas variantes *Human and Organizational Performance* (HOP) e *Human Performance Improvement* (HPI), ganhou ampla circulação na indústria de energia impulsionado por grupos de trabalho da IOGP, por programas de empresas do setor e, no plano das referências setoriais internacionais, pelo IOGP Report 810 (IOGP, 2026). Essa difusão é bem-vinda: aproxima lideranças e equipes operacionais dos princípios que a ciência da segurança vem consolidando há décadas. Ela também tem gerado, entre os praticantes, uma confusão recorrente: a de que HP constituiria um domínio distinto ou mesmo um sucessor de Fatores Humanos (HF ou FH). A literatura é clara ao situar HP como objeto inscrito no campo mais amplo e interdisciplinar de Fatores Humanos (Shorrock, 2019), leitura que este compêndio acompanha. A precisão importa porque, quando FH e HP são tratados como campos paralelos ou concorrentes, abre-se espaço para que o foco no indivíduo, que a ciência da segurança procura superar, retorne sob um novo rótulo (Dekker, 2019; Shorrock, 2019a).

CONCEITOS ADOTADOS NESTE COMPÊNDIO

Fatores Humanos *é o campo científico interdisciplinar que confere nome e unidade a esta obra, com um corpo consolidado de teorias, métodos e práticas, institucionalizado desde o final da década de 1940 (Shorrock, 2019; ver Seção 1.1).* **Desempenho Humano** *designa, a um só tempo, (i) um objeto de estudo – o que as pessoas fazem, como fazem e sua contribuição para os resultados do sistema – e (ii) uma abordagem aplicada, voltada à liderança e à operação, que mobiliza conceitos produzidos no âmbito de Fatores Humanos e da ciência da segurança. O desempenho humano interessa a diversas disciplinas; o que distingue Fatores Humanos é tomá-lo a partir da relação interativa pessoa-sistema e do desempenho do sistema como um todo (IEA, 2000; Shorrock, 2019), razão pela qual a Seção 1.1.1 abre definindo Fatores Humanos como a influência mútua entre os seres humanos e o sistema de trabalho do qual fazem parte. O próprio Relatório IOGP 810 adota essa relação ao definir HP como a capacidade de indivíduos executarem tarefas com sucesso, eficiência e segurança, contribuindo para o desempenho global do sistema, e FH como o estudo de como fatores do trabalho, indivíduos e*

organizações influenciam o comportamento e o desempenho (IOGP, 2026, pp. 6, 34). Nesse sentido, as práticas reunidas sob o rótulo de HP – reconhecer o erro como normal, afastar a culpa como ferramenta de gestão, deslocar a atenção para as condições de trabalho e aprender com o trabalho normal – expressam, em linguagem voltada à ação, princípios que pertencem ao escopo de Fatores Humanos em sua concepção sistêmica contemporânea.

A relação, portanto, é de contenção: o escopo de HP inscreve-se no de Fatores Humanos.

Três argumentos sustentam essa relação. Primeiro, **de escopo**: Fatores Humanos concerne às interações entre as pessoas e os demais elementos de um sistema (IEA, 2000), o que abarca integralmente o objeto de HP. A recíproca é parcial: ao tratar do projeto de equipamentos, ambientes e tarefas, o próprio IOGP Report 810 recorre à Engenharia de Fatores Humanos (HFE) e remete ao IOGP Report 454 – isto é, busca em Fatores Humanos o componente de projeto que é central ao campo (IOGP, 2020, 2026). Segundo, **de fundamento teórico**: os princípios de HP derivam de tradições desenvolvidas no âmbito de Fatores Humanos e da ciência da segurança – a psicologia do erro de Reason, na linhagem nuclear do HPI (DOE, 2009), e a Engenharia de Sistemas Cognitivos, a Nova Visão e a Engenharia de Resiliência, na linhagem do HOP (Conklin, 2019; Le Coze, 2022; ver Partes II e III). O IOGP Report 810 explicita essa filiação ao indicar, como leitura complementar, a crítica de Hollnagel e Dekker (2025) aos usos reducionistas de "fatores humanos" e sua defesa de uma visão sistêmica. Terceiro, **de estatuto**: HP não reúne os atributos de uma disciplina autônoma – formação acadêmica própria, rotas reconhecidas de qualificação, associações profissionais e código de conduta –, e constituí-lo como campo separado seria, na avaliação de Shorrock (2019), desnecessário e pouco útil, dado que diversas disciplinas já se ocupam do desempenho humano.



Leituras restritivas de Fatores Humanos e o risco de fragmentação

A percepção de que HP e Fatores Humanos seriam domínios muito diferentes costuma apoiar-se em uma leitura restritiva de Fatores Humanos, reduzida à ergonomia física ou à engenharia de projeto (HFE). A concepção sistêmica ampla adotada neste compêndio (Seção 1.1) dissolve essa oposição. A proliferação de rótulos concorrentes carrega, além disso, um risco prático: Le Coze (2022) associa parte da confusão conceitual em torno das "novas visões" à expansão do mercado de segurança (ver Seção 1.2.5), e este compêndio adota como princípio a busca por sinergias em vez do fomento a divisões entre escolas (Le Coze, 2024; ver Seção 3.1). Situar HP no âmbito de Fatores Humanos é coerente com esse princípio: a contenção de escopo não implica hierarquia de valor. HP ocupa lugar legítimo no Ecossistema de Fatores Humanos, com zonas de contato próprias, por exemplo, com a Cultura Justa e a Aprendizagem Operacional.

Salvaguarda contra o retorno do foco comportamental

Quando desacoplado de sua base sistêmica e reduzido a um conjunto de ferramentas de modificação de comportamento aplicadas de modo prescritivo, o discurso de HP pode resvalar para uma lógica comportamentalista e individualizante – a mesma que a Nova Visão procura superar. Shorrock (2019a) aponta isso como um dos riscos centrais do movimento de HP: reforçar treinamento, coaching, supervisão e segurança baseada em comportamento em detrimento de abordagens de projeto e de sistema. Hopkins (2006) demonstrou que programas centrados no comportamento da linha de frente tendem a tratar o comportamento inseguro como a causa que mais importa, relegando a segundo plano os controles situados mais acima na hierarquia de controles e o comportamento

gerencial – o mais determinante para a cultura de segurança. Merle e Largier (2025) documentam, no setor nuclear francês, um deslizamento das ferramentas de *human performance improvement* de uma "segurança gerida" para uma "segurança regrada", com seu uso convertido em regra de aplicação automática. O IOGP Report 810 converge com essa cautela ao afirmar que HP deve ser compreendido como mudança na forma de entender o papel humano nos sistemas, e não como programa ou iniciativa (IOGP, 2026, p. 6). Ancorar HP explicitamente no campo de Fatores Humanos é a melhor salvaguarda contra esse retrocesso.

Síntese

Fatores Humanos é o campo; **Desempenho Humano** é um de seus objetos centrais e uma de suas expressões aplicadas. HP é bem-vindo como "porta de entrada" voltada à liderança e à operação, sendo compreendido como uma expressão setorial de Fatores Humanos. É por essa razão que este compêndio se organiza em torno de Fatores Humanos e do conceito de Ecossistema de Fatores Humanos (Parte III): um campo suficientemente amplo para acomodar HP, HOP, HFE, HRA, Segurança de Processos e as demais abordagens, articuladas por zonas de contato em vez de disputas de rótulo.

1.3 Os Limites da Segurança Tradicional e a Escala de Amalberti

1.3.1 O Paradoxo dos Sistemas Quase Totalmente Seguros

René Amalberti, psicólogo cognitivo e pesquisador francês de referência nos campos de Fatores Humanos e segurança, dedicou décadas investigando uma questão fundamental: **Até que ponto as estratégias tradicionais de segurança, baseadas na adição de regras, controles e treinamentos, são capazes de continuar produzindo ganhos efetivos em segurança à medida que os sistemas se tornam mais complexos e maduros?**

Em seu artigo seminal *The paradoxes of almost totally safe transportation systems* (2001), Amalberti demonstrou que quando sistemas atingem níveis muito baixos de risco, três fenômenos emergem:

- **As soluções que melhoraram a segurança não devem ser otimizadas além do nível atual** – a otimização linear pode comprometer o registro de segurança já obtido;
- **Erros desempenham papel essencial na aquisição e efetividade da segurança** – o sistema cognitivo humano depende do contato com variabilidade para manter sua capacidade de detecção e recuperação;
- **Mais regras e proteções podem tornar sistemas mais caros e, paradoxalmente, menos seguros** – ao sobrecarregar operadores e reduzir flexibilidade adaptativa.

> *"Mais regras e proteções podem sempre ser criadas. Mas podem servir para tornar as coisas tanto mais caras quanto, em última análise, menos seguras"* — Dekker (2019, p. 214), sintetizando Amalberti.

1.3.2 A Escala de Risco de Fatalidade

O trabalho de Amalberti (2001, 2013) estabelece uma classificação de atividades humanas segundo o risco de fatalidade por exposição. Esta escala logarítmica varia de 10^{-2} (muito inseguro) a 10^{-6} (ultraseguro) e permite posicionar diferentes setores industriais em um continuum de segurança.



Figura 1.3.1: Escala de Risco de Fatalidade nas Atividades Humanas. **Fonte:** Adaptado de Amalberti (2001, 2013).

O posicionamento da **indústria de óleo e gás** no nível 10^{-4} ("seguro") indica que o setor já opera sistemas significativamente seguros, mas ainda está distante dos sistemas "ultra-seguros", como a aviação civil comercial e a indústria nuclear (10^{-6}), setores que constituem os exemplos clássicos da Teoria da Alta Confiabilidade (HRO), detalhada na Seção 2.2. Esta diferença de duas ordens de magnitude, representando aproximadamente 100 vezes mais risco por exposição, tem implicações profundas para as estratégias de melhoria.

1.3.3 Efeitos Paradoxais do Excesso de Regras e Burocracia

Um dos insights mais importantes do trabalho de Amalberti é a demonstração empírica de que o impacto das regras e procedimentos na segurança diminui à medida que o sistema sociotécnico se torna mais seguro. Conforme ilustrado na Figura 1.3.2, esta relação não é linear: em atividades de alto risco (como o alpi-

nismo no Himalaia), a introdução de regras básicas produz ganhos substanciais; contudo, em sistemas maduros que já operam em níveis elevados de segurança, a adição de mais regras produz ganhos marginais cada vez menores – e pode, paradoxalmente, introduzir novos riscos.

Amalberti (2001) descreveu este fenômeno como a "armadilha do excesso de regulação" (*trap of over-regulation*):

> *"Regulações cumulativas terão, então, o efeito de não mudar nada nas operações (o sistema está estabilizado), mecanicamente aumentam as violações, aumentam a relutância e a opacidade no reporte de incidentes e adicionam ruído à estratégia de monitoramento de segurança"* — Amalberti (2001, p. 121).

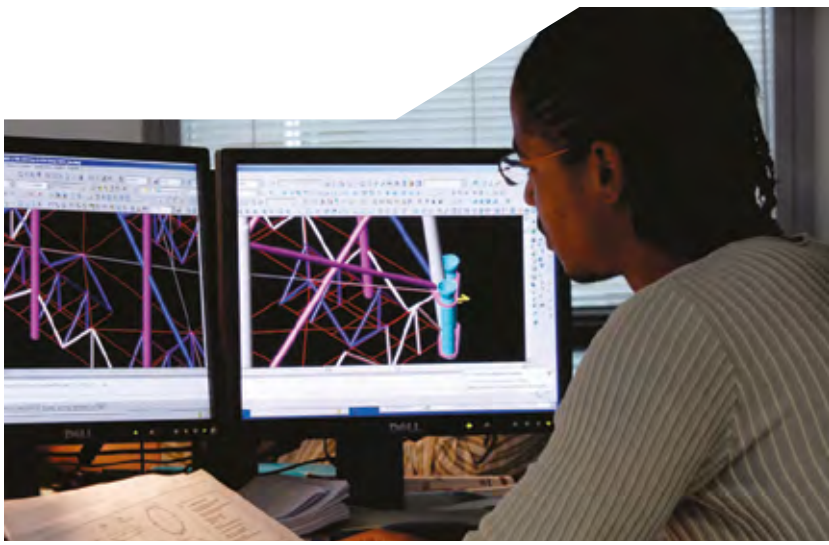
A proliferação de procedimentos cria o que Rae, Weber e Dekker (2018) denominaram safety clutter – o acúmulo de trabalho rotulado como "segurança" que não contribui para a segurança operacional, mas consome recursos e atenção que poderiam ser direcionados para riscos genuínos. Em sistemas saturados de procedimentos, operadores fazem escolhas inevitáveis entre eficiência e minuciosidade – o Princípio ETTO de Hollnagel (2009). O resultado é um ciclo contraproducente: mais regras geram mais violações documentáveis, que justificam ainda mais regras, enquanto a capacidade adaptativa do sistema é progressivamente erodida.

> *"Quanto mais regras existem, mais fácil se torna mostrar que pelo menos algumas delas não são cumpridas"* — Dekker (2019, p. 332).





Figura 1.3.2: Efetividade decrescente das intervenções baseadas em regras. **Fonte:** Adaptado de Amalberti (2001) e Dekker (2019).



1.4 Fatores Humanos como Jornada de Aprendizagem Organizacional

A compreensão dos limites da segurança tradicional, apresentada nas seções anteriores, conduz a uma questão inevitável: se mais regras, procedimentos e controles não são suficientes para alcançar níveis superiores de segurança, qual caminho seguir?

A resposta não está em uma solução única, mas em uma **jornada de aprendizagem organizacional**. Implementar Fatores Humanos de forma efetiva não significa adotar apenas um novo conjunto de ferramentas ou metodologias, mas desenvolver a **capacidade de aprendizagem contínua** – de compreender, questionar e aprimorar continuamente a relação entre pessoas, tecnologia e organização. Existe, porém, uma **relação íntima entre o modo como uma organização explica seus acidentes e o modo como ela os previne** (Henriqson, 2023). Mudar o modelo explanatório é pré-requisito para mudar o modelo preventivo – e esse reconhecimento é o que torna a jornada possível.

Esta jornada não é linear nem possui ponto de chegada final. Ela opera através de um mecanismo fundamental – **princípios orientam práticas; práticas transformadas reconfiguram cultura** – e envolve movimentos simultâneos e interdependentes: **engajar lideranças** na mudança de modelo mental, **disseminar fundamentos** para criar linguagem comum, **conectar-se ao trabalho real** para compreender como as coisas realmente acontecem, **alinhar sistemas e processos** para que reforcem (e não contradigam) os princípios declarados, e **desenvolver capacidades adaptativas** que permitam à organização antecipar e responder a desafios futuros. Estes movimentos são detalhados na **Parte IV** deste compêndio.

A jornada, contudo, não começa necessariamente **adicionando** – começa frequentemente **questionando**. Organizações maduras examinam criticamente o que já fazem antes de adicionar novas iniciativas, avaliando se práticas existentes ainda servem aos propósitos para os quais foram criadas. Este processo de

avaliação crítica de práticas – detalhado na Parte IV – demanda deliberação da alta liderança, seja através de estrutura de governança específica ou de comitês estratégicos já constituídos pela organização.

1.4.1 Perguntas para Reflexão Organizacional

Antes de embarcar nesta jornada, algumas perguntas podem ajudar organizações a avaliar seu ponto de partida:

Dimensão	Pergunta Orientadora
Modelo mental	Como nossa liderança explica acidentes e incidentes? Predomina a busca por "culpados" ou a compreensão sistêmica?
Trabalho real	Conhecemos genuinamente como o trabalho acontece na prática – não apenas como imaginamos ou prescrevemos?
Aprendizagem	Nossos sistemas geram aprendizado real ou apenas conformidade documentada?
Coerência	Nossas políticas de consequência, métricas e incentivos reforçam ou contradizem os princípios que declaramos?

Tabela 1.4.1: Perguntas orientadoras para reflexão organizacional inicial.



A implementação de Fatores Humanos pode ser orientada por questões que ajudam organizações a avaliar suas práticas atuais e identificar oportunidades de desenvolvimento:

Dimensão	Perguntas Orientadoras
O que deixar de fazer?	Quais práticas rotuladas como "seguras" não contribuem efetivamente para a segurança operacional? Onde estamos gerando conformidade burocrática sem valor real?
O que começar a fazer?	Como podemos conhecer melhor o trabalho como realmente realizado? Quais espaços de aprendizagem e melhorias ainda não existem?
O que fazer diferente?	Quais práticas poderiam ser mais efetivas se redesenhadas? Como nossas investigações poderiam gerar mais aprendizado?
Quais as barreiras?	O que impede a implementação de práticas mais efetivas? Quais pressupostos organizacionais precisam ser revisitados?

Tabela 1.4.2: Perguntas orientadoras para reflexão organizacional sobre práticas de Fatores Humanos.

1.4.2 O Caminho Adiante

As Partes II e III deste compêndio apresentarão as **perspectivas teóricas fundamentais** e as **abordagens complementares** que compõem o Ecossistema de Fatores Humanos – oferecendo o repertório conceitual necessário para compreender a complexidade dos sistemas sociotécnicos.

A **Parte IV – Framework Integrador para Aplicação Setorial** traduzirá esta riqueza conceitual em um **framework prático para transformação organizacional**. Lá, o leitor encontrará:

- Os **cinco movimentos** da jornada de Fatores Humanos e suas interdependências
- **Premissas fundamentais** que orientam a implementação, incluindo o papel crítico da Cultura Justa

- Ênfase em **Segurança de Processo** e prevenção de grandes emergências
- **Matriz de aplicação** das perspectivas teóricas para diferentes contextos e desafios
- Orientações para **integração do ecossistema setorial** – contratantes, contratadas e regulador
- Articulação com os requisitos da **NT 10/2023 da ANP**

A jornada de Fatores Humanos é, essencialmente, uma jornada de **aprendizagem organizacional**. E toda jornada de aprendizagem começa com um primeiro passo: a disposição genuína de questionar o que achamos que sabemos.

Referências da Parte I

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. (2023). *Nota Técnica nº 10/2023/SSO-CSO/SSO/ANP-RJ*. ANP.

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science, 37*(2–3), 109–126. https://doi.org/10.1016/S0925-7535(00)00045-X

Amalberti, R. (2013). *Navigating safety: Necessary compromises and trade-offs – Theory and practice*. Springer. https://doi.org/10.1007/978-94-007-6549-8

Bills, K. (2023). *Reading Barry Turner today: 'Man-made disasters' and contemporary safety science* [Dissertação de mestrado, Lund University].

Bridger, R. S. (2021). *Introduction to human factors and ergonomics* (5ª ed.). CRC Press.

Bruno, J. C. (2022). Fatores humanos na indústria de petróleo e gás: Uma perspectiva crítica. *Revista Brasileira de Segurança Industrial, 15*(2), 45–62.

Center for Chemical Process Safety. (2019). *Process safety glossary*. American Institute of Chemical Engineers.

Conklin, T. (2019). *The 5 principles of human performance: A contemporary update of the building blocks of human performance for the new view of safety*. PreAccident Media.

Dekker, S. W. A. (2002). *The field guide to human error investigations*. Ashgate.

Dekker, S. W. A. (2014). *Safety differently: Human factors for a new era*. CRC Press.

Dekker, S. W. A. (2019). *Foundations of safety science: A century of understanding accidents and disasters*. CRC Press. https://doi.org/10.4324/9781351059794

Edmondson, A. C. (2019). *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. Wiley.

Fitts, P. M., & Jones, R. E. (1947). *Analysis of factors contributing to 460 "pilot-error" experiences in operating aircraft controls* (Report No. TSEAA-694-12). Aero Medical Laboratory, Air Materiel Command.

Gibson, J. J. (1961). The contribution of experimental psychology to the formulation of the problem of safety. In *Behavioral approaches to accident research* (pp. 77–89). Association for the Aid of Crippled Children.

Haddon, W. (1970). On the escape of tigers: An ecologic note. *American Journal of Public Health, 60*(12), 2229–2234.

Haddon, W. (1980). The basic strategies for reducing damage from hazards of all kinds. *Hazard Prevention, 16*(5), 8–12.

Health and Safety Executive. (1999). *Reducing error and influencing behaviour* (HSG48, 2ª ed.). HSE Books.

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

Henriqson, E. (2023). *Nova visão de segurança: Princípios, práticas, cultura e gestão da mudança* [Palestra]. Nova Visão de Segurança Brasil, 30 set. 2023.

Henriqson, E. (2026). [Contribuição original ao Compêndio — detalhar conforme veículo de publicação].

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

Hollnagel, E. (2012). *FRAM: The functional resonance analysis method*. Ashgate.

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

Hollnagel, E. (2025). *From safety to safely: Principles and practice of systemic potentials management*. Routledge.

Hollnagel, E. (2026). *Decremental and incremental safety cultures: Safety-I and Safety-II revisited*. CRC Press.

Hollnagel, E., & Dekker, S. W. A. (2025). The ironies of "human factors". *Theoretical Issues in Ergonomics Science, 26*(3), 349–359. https://doi.org/10.1080/1463922X.2024.2443976

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.

Hopkins, A. (2006). What are we to make of safe behaviour programs? *Safety Science, 44*(7), 583–597. https://doi.org/10.1016/j.ssci.2006.01.001

International Association of Oil & Gas Producers. (2018). *Demystifying*

human factors: Building confidence in human factors investigation (IOGP Report 621). IOGP.

International Association of Oil & Gas Producers. (2020). *Human factors engineering in projects* (IOGP Report 454, 2ª ed.). IOGP.

International Association of Oil & Gas Producers. (2026). *Human performance* (IOGP Report 810). IOGP.

International Association of Oil & Gas Producers. (2019). *Safety leadership in practice: A guide for managers* (IOGP Report 453). IOGP.

International Association of Oil & Gas Producers. (2020). *Understanding and managing human factors in the wells sector* (IOGP Information Sheet). IOGP.

International Ergonomics Association. (2000). *Definition of ergonomics*. https://iea.cc/what-is-ergonomics/

Le Coze, J.-C. (Ed.). (2019). *Safety science research: Evolution, challenges and new directions*. CRC Press.

Le Coze, J.-C. (2022). The 'new view' of human error: Origins, ambiguities, successes and critiques. *Safety Science, 154*, Artigo 105853. https://doi.org/10.1016/j.ssci.2022.105853

Le Coze, J.-C. (2024). *Evolution of safety* [Apresentação]. Rio de Janeiro.

Lee, J. D., Wickens, C. D., Liu, Y., & Boyle, L. N. (2017). *Designing for people: An introduction to human factors engineering* (3ª ed.). CreateSpace.

Merle, I., & Largier, A. (2025). Shifting visions of human performance improvement tools – Risks and potential outcomes. *Safety Science, 181*, Artigo 106671. https://doi.org/10.1016/j.ssci.2024.106671

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Rae, A. J., Weber, D. E., & Dekker, S. W. A. (2018). Safety clutter: The accumulation and persistence of 'safety' work that does not contribute to operational safety. *Policy and Practice in Health and Safety, 16*(2), 194–211. https://doi.org/10.1080/14773996.2018.1491147

Rasmussen, J. (1980). What can be learned from human error reports? In K. Duncan, M. Gruneberg, & D. Wallis (Eds.), *Changes in working life* (pp. 97–113). Wiley.

Rasmussen, J. (1986). *Information processing and human-machine interaction: An approach to cognitive engineering*. North-Holland.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Reason, J. (1990). *Human error*. Cambridge University Press.

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.

Reason, J., Hollnagel, E., & Pariès, J. (2006). *Revisiting the "Swiss cheese" model of accidents* (EEC Note No. 13/06). Eurocontrol Experimental Centre.

Rijpma, J. A. (1997). Complexity, tight-coupling and reliability: Connecting normal accidents theory and high reliability theory. *Journal of Contingencies and Crisis Management, 5*(1), 15–23. https://doi.org/10.1111/1468-5973.00033

Rijpma, J. A. (2003). From deadlock to dead end: The normal accidents–high reliability debate revisited. *Journal of Contingencies and Crisis Management, 11*(1), 37–45. https://doi.org/10.1111/1468-5973.1101004

Roscoe, S. N. (1997). The adolescence of engineering psychology. In *Human factors history monograph series* (Vol. 1). Human Factors and Ergonomics Society.

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærø, I. (2010). *Organisational accidents and resilient organisations: Six perspectives* (Report SINTEF A17034, Revisão 2). SINTEF Technology and Society.

Shorrock, S. (2017a, 11 de agosto). Four kinds of 'human factors': 1. The human factor. *Humanistic Systems*. https://humanisticsystems.com/2017/08/11/four-kinds-of-human-factors-1-the-human-factor/

Shorrock, S. (2017b, 12 de agosto). Four kinds of 'human factors': 2. Factors of humans. *Humanistic Systems.* https://humanisticsystems.com/2017/08/12/four-kinds-of-human-factors-2-factors-of-humans/

Shorrock, S. (2017c, 18 de setembro). Four kinds of 'human factors': 3. Factors affecting humans. *Humanistic Systems.* https://humanisticsystems.com/2017/09/18/four-kinds-of-human-factors-3-factors-affecting-humans/

Shorrock, S. (2017d, 7 de outubro). Four kinds of 'human factors': 4. Socio-technical system interaction. *Humanistic Systems.* https://humanisticsystems.com/2017/10/07/four-kinds-of-human-factors-4-socio-technical-system-interaction/

Shorrock, S. (2019a, 24 de abril). 'Human factors' and 'human performance':

What's the difference? *Humanistic Systems.* https://humanisticsystems.com/2019/04/24/human-factors-and-human-performance-whats-the-difference/

Shorrock, S. (2019b, 1º de outubro). What human factors isn't: 4. A cause of accidents. *Humanistic Systems.* https://humanisticsystems.com/2019/10/01/what-human-factors-isnt-4-a-cause-of-accidents/

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of U.S. Black Hawks over northern Iraq*. Princeton University Press.

Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. *Harvard Business Review, 85*(11), 68–76.

Turner, B. A. (1978). *Man-made disasters*. Wykeham Publications.

Turner, B. A., & Pidgeon, N. F. (1997). *Man-made disasters* (2ª ed.). Butterworth-Heinemann.

U.S. Department of Energy. (2009). *Human performance improvement handbook, Volume 1: Concepts and principles* (DOE-HDBK-1028-2009). U.S. Department of Energy.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.

Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: Assuring high performance in an age of complexity*. Jossey-Bass.

Westrum, R. (1993). Cultures with requisite imagination. In J. A. Wise, V. D. Hopkin, & P. Stager (Eds.), *Verification and validation of complex systems: Human factors issues* (pp. 401–416). Springer.

Wróbel, K. (2021). Searching for the origins of the myth: 80% human error impact on maritime safety. *Reliability Engineering & System Safety, 216*, Artigo 107942. https://doi.org/10.1016/j.ress.2021.107942.




F3
F2



Parte II

Perspectivas teóricas fundamentais: Estado da Arte

Autor: Eder Henriqson



A evolução do campo de Fatores Humanos, apresentada na Parte I deste compêndio, revela uma trajetória consistente: a transição de visões reducionistas, centradas no indivíduo como fonte de falhas, para perspectivas sistêmicas que reconhecem a crescente complexidade dos sistemas sociotécnicos contemporâneos. Esta mesma trajetória caracteriza o amadurecimento da Ciência da Segurança, cujas perspectivas teóricas fundamentais constituem o objeto desta segunda parte.

As perspectivas que compõem o estado da arte em segurança dos sistemas não oferecem uma resposta única – oferecem um repertório. São abordagens parcialmente sobrepostas, parcialmente complementares e, em determinados aspectos, contraditórias (Rosness et al., 2010). Para o praticante, esta diversidade representa uma caixa de ferramentas conceituais: cada perspectiva ilumina aspectos distintos dos sistemas sociotécnicos, permitindo identificar vulnerabilidades e oportunidades que permaneceriam invisíveis sob uma única abordagem. Não é limitação do campo, mas uma de suas riquezas.

A apresentação das perspectivas adota ordem cronológica, espelhando a evolução histórica traçada na Seção 1.2 (Figura 1.2.4) e convergindo com obras de referência como Dekker (2019) e Rosness et al. (2010). A sequência preserva o caráter dialético do desenvolvimento teórico: cada perspectiva responde, complementa ou tensiona as anteriores, e o leitor é convidado a perceber esse diálogo ao avançar pelas seções.

As cinco seções que se seguem apresentam as perspectivas fundamentais selecionadas pelo GT Fatores Humanos para orientar a análise e gestão de segurança na indústria de energia brasileira: a **Teoria dos Acidentes Normais** (NAT, Perrow, 1984), que explica por que acidentes podem ser inevitáveis em sistemas com alta

complexidade interativa e acoplamento estreito; a **Teoria da Alta Confiabilidade** (HRT/HRO, a partir de meados dos anos 1980), que demonstra como certas organizações operam tecnologias perigosas com registros extraordinários de segurança; a **Perspectiva Rasmusseniana** (Rasmussen, 1997), que modela a migração dinâmica das atividades em direção às fronteiras de segurança sob gradientes de pressão; a **Engenharia de Resiliência** (Hollnagel, Woods & Leveson, 2006), que reconceitua a segurança como capacidade adaptativa; e a **Dependência de Trajetória**, que reúne contribuições de Turner (1978), Vaughan (1996), Snook (2000) e Dekker (2011) para revelar como decisões aparentemente racionais acumulam vulnerabilidades ao longo do tempo.

Embora apresentada por último, a Dependência de Trajetória integra uma genealogia que se inicia em 1978 com *Man-Made Disasters* de Barry Turner – antecedendo, portanto, todas as demais perspectivas. Sua posição final é deliberada: opera como síntese transversal, uma lente temporal-sociológica que atravessa e articula as anteriores. A incubação de Turner antecipa o que NAT formalizará como acidente sistêmico; a normalização do desvio de Vaughan dialoga com a migração rasmusseniana; a deriva prática de Snook tensiona o ideal HRO de *mindful organizing*; e a síntese de Dekker (2011) – *drift into failure* – integra explicitamente o modelo de Rasmussen às tradições da Engenharia de Resiliência. Apresentá-la ao final permite ao leitor reconhecer estas conexões retrospectivamente.

A seleção pelo GT baseou-se em três critérios: relevância histórica e influência no desenvolvimento do campo; aplicabilidade ao contexto da indústria de energia, particularmente sistemas complexos e de alto risco; e complementaridade analítica. O leitor encontrará tensões produtivas entre algumas perspectivas – notadamente entre NAT e HRO – que não devem ser vistas como contradições a resolver, mas como lentes que enriquecem a análise.

As seções priorizam o rigor acadêmico, preservando as formulações originais de cada escola sem adaptações prescritivas. Cabe aos profissionais e organizações – não a este compêndio – realizar a análise crítica contextualizada que traduzirá conceitos teóricos em práticas adequadas às suas realidades. As perspectivas aqui apresentadas fundamentam não apenas a compreensão dos fenômenos de segurança, mas também as abordagens complementares da Parte III e o framework integrador da Parte IV.

2.1 Teoria dos Acidentes Normais (NAT)

Autores: Paula Freitas e Kaio Pimentel

Revisão e Figuras: Rafael Ceni de Almeida

2.1.1 Introdução e Contexto Histórico

A Teoria dos Acidentes Normais (*Normal Accident Theory* – NAT) emergiu em um contexto marcado por crescente inquietação social sobre os riscos das tecnologias modernas. Na madrugada de 28 de março de 1979, uma série de falhas aparentemente menores na usina nuclear de *Three Mile Island* (TMI), na Pensilvânia, culminou no mais grave acidente nuclear da história dos Estados Unidos. Este evento transformaria não apenas a indústria nuclear americana, mas também a compreensão acadêmica sobre acidentes em sistemas complexos

Charles Perrow (1925–2019), sociólogo organizacional então professor da Universidade de Yale, foi convidado pelo Social *Science Research Council* (SSRC), a pedido da comissária Cora Marrett da Comissão Presidencial sobre o Acidente em *Three Mile Island* (Comissão Kemeny), para preparar um relatório de análise organizacional do acidente. Trabalhando a partir das transcrições das audiências de maio, junho e julho de 1979, com prazo de três semanas, Perrow produziu um documento de aproximadamente quarenta páginas cujas ideias centrais – interações inesperadas, acoplamento estreito e complexidade interativa – viriam a se desenvolver, três anos e meio depois, no livro *Normal Accidents: Living with High-Risk Technologies* (Perrow, 1984, prefácio "*Abnormal Blessings*", 1999).

Ao analisar TMI, Perrow deparou-se com um padrão perturbador: o acidente não resultou de negligência grosseira, incompetência dos operadores ou falhas catastróficas de equipamentos. Pelo contrário, envolveu uma cascata de pequenas falhas – individualmente triviais – que interagiram de maneiras que ninguém havia antecipado e que, durante a escalada do evento, permaneceram incompreensíveis para os próprios operadores altamente treinados (Perrow, 1999, cap. 1).

A publicação de *Normal Accidents* insere-se em uma virada epistemológica na sociologia das organizações, que buscava compreender como estruturas organizacionais moldavam tanto falhas quanto rotinas operacionais. Ao contrário de perspectivas centradas em erro humano, Perrow desloca o foco para a **complexidade interativa** e o **acoplamento estreito**, defendendo que acidentes catastróficos são produto "normal" – no sentido de esperado, dadas as propriedades estruturais – da forma como tecnologias modernas são projetadas (Dekker, 2019, cap. 8). Conforme síntese de Dekker (2019, p. 268), Perrow argumentava que sistemas com alta complexidade interativa e acoplamento estreito tendem a produzir, com o tempo, "acidentes normais": acidentes que são a consequência normal de como o sistema foi projetado, construído e operado.

Esse enquadramento desafia concepções tradicionais de risco, pois sugere que, não importa o nível de competência individual, planejamento ou manutenção, certos sistemas são inerentemente propensos a falhar devido à imprevisibilidade das interações internas. Tal diagnóstico provocou intenso debate acadêmico, sobretudo com pesquisadores ligados às *High Reliability Organizations (HRO)*, que argumentariam que organizações altamente confiáveis podem, de fato, operar sistemas complexos com segurança excepcional (La Porte & Rochlin, 1994; Sagan, 1993).

2.1.2 Pressupostos Críticos

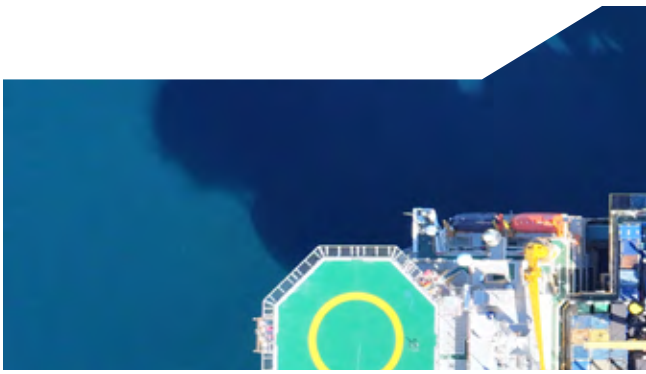
A Teoria dos Acidentes Normais fundamenta-se em um conjunto de pressupostos sobre a relação entre características estruturais dos sistemas e possibilidades de controle organizacional. Conforme sistematizado pelo relatório SINTEF (Rosness et al., 2010), três pressupostos constituem o núcleo da teoria:

- **Sistemas complexos requerem descentralização:** tecnologias com alta complexidade interativa geram tarefas não-rotineiras difíceis de programar ou padronizar. A organização deve conceder discrição considerável ao pessoal de níveis inferiores e encorajar interação direta entre eles. Este pressuposto reconhece que operadores na linha de frente frequentemente enfrentam situações inéditas que escapam aos procedimentos estabelecidos; quando interações inesperadas entre componentes pro-

duzem estados não antecipados, respostas criativas e adaptativas tornam-se necessárias, e a centralização excessiva impede a flexibilidade requerida.

- **Sistemas fortemente acoplados requerem centralização:** uma resposta rápida e coordenada é necessária quando perturbações se propagam rapidamente pelo sistema. Isso requer centralização, programação e treinamento intensivo de respostas de emergência, além de coordenação estrita para evitar conflitos entre atividades. Em sistemas onde processos são fortemente interdependentes e onde distúrbios propagam-se velozmente, não há tempo para consultas, deliberações ou improvisações; a coordenação deve ser pré-estabelecida e as respostas, automatizadas ou extensivamente treinadas.
- **Uma organização não pode ser centralizada e descentralizada ao mesmo tempo:** este é o dilema organizacional central. Sistemas que exigem ambas as formas de controle enfrentam uma contradição estrutural insolúvel. Se sistemas interativamente complexos exigem descentralização e sistemas fortemente acoplados exigem centralização, então sistemas que são simultaneamente complexos e fortemente acoplados enfrentam demandas organizacionais contraditórias. Como uma organização não pode satisfazer requisitos mutuamente excludentes, tais sistemas são inerentemente vulneráveis a "acidentes normais" – acidentes que emergem não de falhas específicas, mas das propriedades estruturais do próprio sistema (Perrow, 1999; Dekker, 2019).

Da combinação destes pressupostos emerge a **conclusão central**: sistemas com alta complexidade interativa *e* acoplamento estreito são inerentemente vulneráveis a acidentes que não podem ser prevenidos, independentemente da qualidade da gestão ou do treinamento.



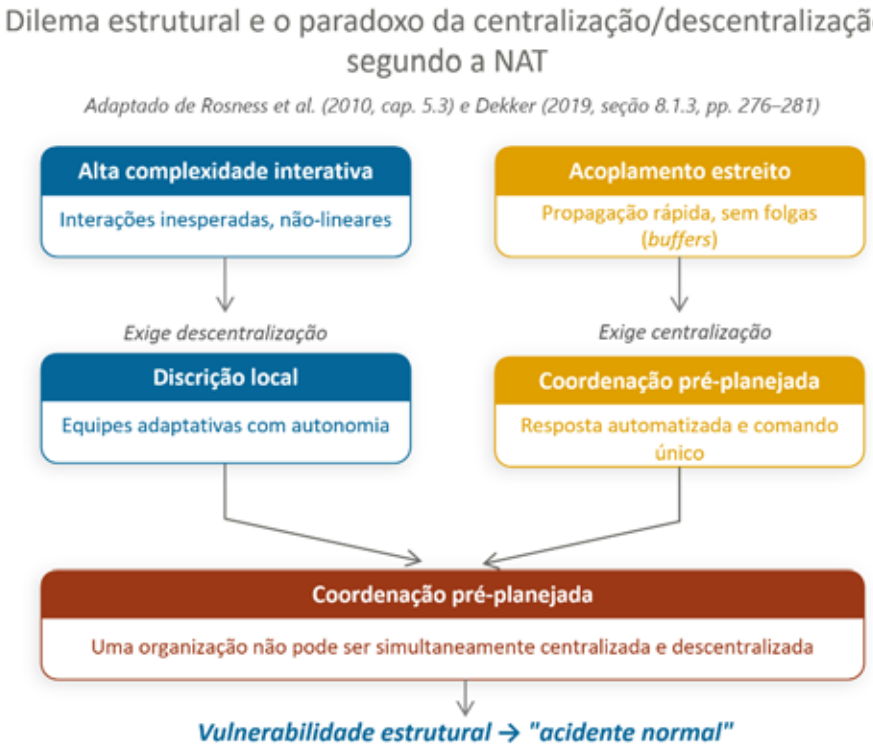


Figura 2.1.1: ***Dilema estrutural e o paradoxo da centralização/descentralização segundo a NAT.*** *Sistemas com alta complexidade interativa exigem descentralização, sistemas com acoplamento estreito exigem centralização, e nenhuma organização pode satisfazer simultaneamente ambas as demandas – gerando vulnerabilidade estrutural a "acidentes normais". Adaptado de Rosness et al. (2010, cap. 5.3) e Dekker (2019, seção 8.1.3, pp. 276–281).*

Nota terminológica: É crucial notar que «normal» aqui não significa frequente. Perrow enfatiza que acidentes de sistema são relativamente raros. O termo indica que, dadas as características estruturais, tais acidentes são inevitáveis no longo prazo – uma questão de "quando", não de "se".



2.1.3 Conceitos Fundamentais

Complexidade Interativa

A complexidade interativa refere-se ao grau em que componentes de um sistema interagem de modo inesperado, não linear e difícil de prever. Perrow contrasta sistemas **lineares** (onde interações seguem sequências previsíveis) com sistemas **complexos** (onde múltiplas interações ocorrem de formas inesperadas). Características de sistemas interativamente complexos incluem: proximidade física de componentes, subsistemas interconectados, múltiplas funções de um mesmo componente e informação indireta sobre o estado do sistema (Perrow, 1999, cap. 3).

Em sistemas altamente complexos, a diversidade de rotas de interação e a presença de múltiplas dependências ocultas tornam impossível antever todos os cenários de falha. Tais interações frequentemente escapam a representações tradicionais como árvores de falhas, justamente porque envolvem combinações não mapeadas de variáveis (Hopkins, 1999). Nessa perspectiva, operadores não conseguem compreender totalmente o estado do sistema, e pequenos desvios podem desencadear sequências inesperadas de eventos (Weick, 1990).

Acoplamento Estreito

O acoplamento estreito (*tight coupling*) caracteriza sistemas nos quais os processos são rígidos, altamente interdependentes e sensíveis ao tempo. Em sistemas fortemente acoplados, processos são dependentes do tempo e não podem esperar, sequências são invariantes, há apenas um caminho para atingir objetivos e há pouca folga possível em suprimentos e equipamentos (Perrow, 1999, cap. 3; Dekker, 2019, Tabela 8.2). Acoplamentos estreitos caracterizam-se por:

- Pouca margem de manobra;
- Falta de folgas operacionais – *buffers* (margens de tempo, estoques intermediários, capacidade ociosa) – que permitam absorver perturbações antes da propagação;
- Dependências rígidas entre etapas;
- Processos que não podem ser interrompidos ou desacelerados;

- Substituições de suprimentos, equipamentos ou pessoal impossíveis ou limitadas.

Perrow (1999) sustenta que, quando falhas se iniciam em sistemas estreitamente acoplados, a propagação é tão rápida que estratégias convencionais de controle entram em colapso, configurando as chamadas "trajetórias de acidente".

A Matriz Interação/Acoplamento

A matriz formulada por Perrow cruza dois eixos: **complexidade interativa** (linear/complexa) e **acoplamento** (solto/estreito). Sistemas considerados particularmente perigosos são aqueles que se situam no quadrante de **alta complexidade + acoplamento estreito** – usinas nucleares, armas nucleares e missões espaciais. Transporte marítimo e redes elétricas apresentam acoplamento estreito, mas interações mais lineares. Universidades e agências multiobjetivo têm acoplamento solto e interações complexas. Linhas de montagem e correios situam-se no quadrante mais "seguro" de acoplamento solto e interações lineares (Perrow, 1999, cap. 3; Dekker, 2019).

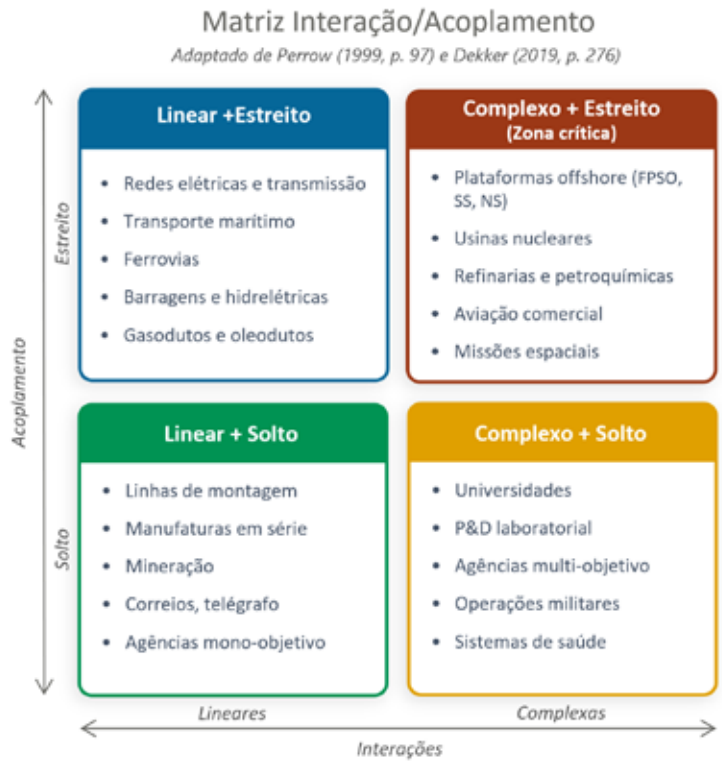


Figura 2.1.2: Matriz Interação/Acoplamento, adaptada de Perrow (1999, p. 97) e Dekker (2019, p. 276). *Sistemas no quadrante de alta complexidade interativa e acoplamento estreito (zona crítica) são, segundo a NAT, inerentemente vulneráveis a "acidentes normais". Exemplos do quadrante crítico foram contextualizados para a indústria de energia.*

Essa matriz tornou-se um instrumento conceitual central para análises de risco, apesar de seu caráter qualitativo (Rijpma, 1997). A matriz ilumina o fato de que não basta avaliar cada componente individualmente: o risco nasce das **interações**.

2.1.4 Base Empírica

A base empírica da NAT assenta-se em estudos de caso históricos e em releituras comparativas de grandes acidentes e quase-acidentes em sistemas sociotécnicos de alto risco. Esses estudos não visam apenas identificar causas pontuais, mas evidenciar padrões estruturais: combinações de complexidade interativa e acoplamento estreito que, sob certas condições, tornam acidentes de sistema praticamente inevitáveis no longo prazo (Perrow, 1984; 1999; Dekker, 2019).

Three Mile Island (1979) – caso paradigmático



No relato fundacional de Perrow (1984, cap. 1; 1999), TMI demonstra como falhas técnicas triviais – sensores, válvulas, alarmes – podem interagir de modo inesperado em um ambiente densamente interdependente, obscurecendo o *sensemaking* dos operadores e precipitando uma trajetória de acidente. A análise mostra que, mais do que "erro humano", foi a arquitetura do sistema – interfaces pouco transparentes, alarmes saturados e múltiplas dependências – que produziu a perda de controle. É por isso que TMI é frequentemente citado como "acidente normal": não um desvio raro explicável por um culpado, mas aquilo que se deve esperar quando um sistema combina alta complexidade com acoplamento estreito (Dekker, 2019). Vale observar, contudo, que Hopkins (1999, 2001) propõe leitura alternativa, segundo a qual TMI pode ser mais bem explicado por falhas gerenciais e regulatórias do que por inevitabilidade estrutural – debate ainda ativo na literatura.

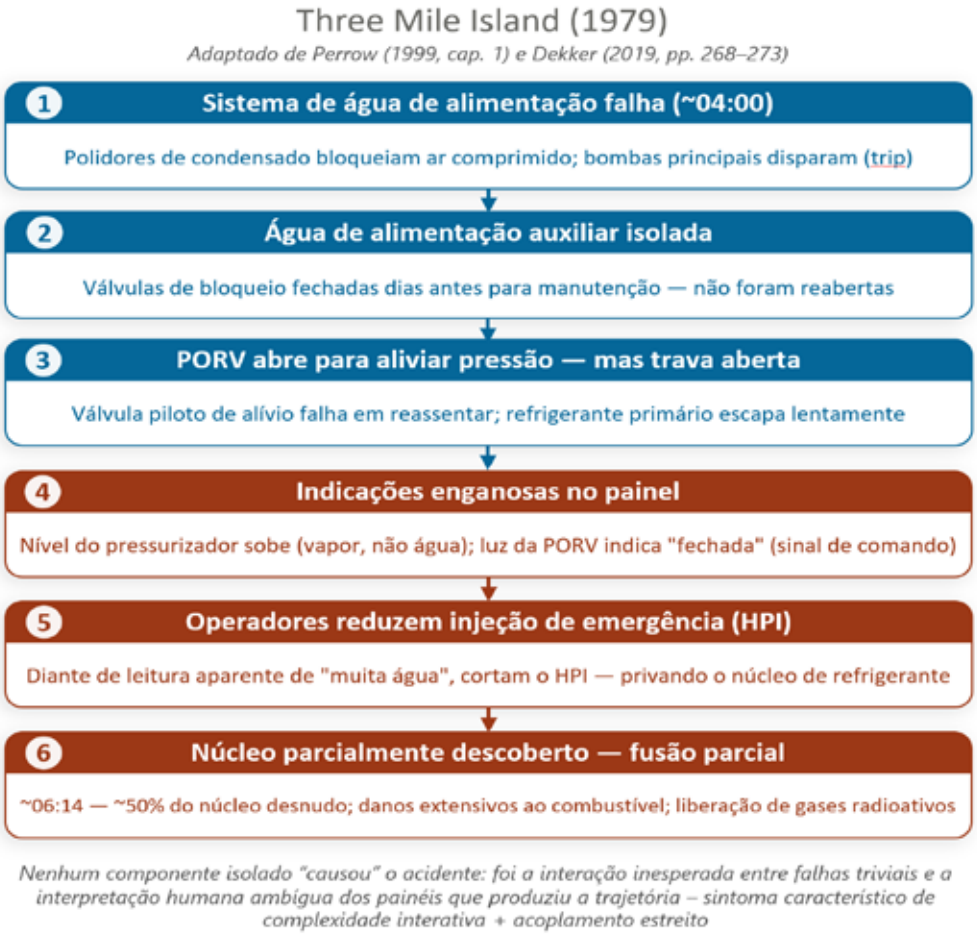


Figura 2.1.3: *Three Mile Island* (28 de março de 1979) como cascata de falhas interagentes. *Nenhum componente isolado "causou" o acidente: foi a interação entre falhas individualmente triviais (passos 1–3) com a interpretação humana ambígua dos painéis (passos 4–5) que produziu a trajetória catastrófica (passo 6). Adaptado de Perrow (1999, cap. 1, pp. 15–31) e Dekker (2019, pp. 268–273).*

Outros casos analisados em *Normal Accidents*

Em seu livro, Perrow analisou acidentes em usinas petroquímicas (cap. 4), sistemas de tráfego aéreo e operações aeronáuticas (cap. 5), transporte marítimo (cap. 6), barragens, minas e represas (cap. 6), armas nucleares, sistemas espaciais e engenharia genética (cap. 7) – sempre buscando demonstrar como combinações de complexidade interativa e acoplamento estreito produzem trajetórias de acidente similares, ainda que em domínios tecnológicos distintos.

Desastres em transporte e aviação – a dimensão dinâmica do acoplamento

Weick (1990), ao analisar o desastre de Tenerife (1977), introduz a noção de **vulnerabilidade sistêmica** e enfatiza como pressão temporal, estresse e ambiguidade podem aumentar momentaneamente o acoplamento e elevar a complexidade efetiva do sistema. Embora Tenerife não seja um "teste" direto da NAT, sua leitura mostra compatibilidade: em crise, mecanismos organizacionais (linguagem, autoridade, coordenação) mudam a topologia do sistema, aproximando-o do quadrante de risco elevado delineado por Perrow. Essa "dinamização" da NAT é recuperada em sínteses contemporâneas (Dekker, 2019).

Casos da indústria de energia sob a lente da NAT

Sínteses como a de Rosness et al. (2010, cap. 5) demonstram a utilidade analítica da NAT em setores como ferrovias e petróleo & gás, examinando os casos do acidente ferroviário de Åsta (Noruega, 2000) e do blowout na plataforma Snorre A (Mar do Norte, 2004). Em ambos, as interações inesperadas entre barreiras técnicas, rotinas organizacionais e decisões sob restrição temporal evidenciam propagação rápida de perturbações – uma assinatura empírica do acoplamento estreito. Esses exemplos sustentam que a NAT permanece útil para identificar onde *buffers* (folgas que absorvem perturbações antes da propagação) são limitados, interdependências são rígidas e a visibilidade do estado do sistema é insuficiente.

Catástrofes recentes e reafirmações do argumento de inevitabilidade

Na esteira de Fukushima (2011), o próprio Perrow (2011) reaplicou sua teoria, argumentando que a combinação de infraestruturas críticas colocalizadas, dependências ocultas (incluindo energia de emergência e resfriamento) e pressões político-regulatórias configura um espaço onde trajetórias de acidente podem escapar ao controle. Essa releitura empírica reforça o argumento central da teoria: em certos domínios, a inevitabilidade estrutural não é falha de gestão, mas propriedade do desenho sociotécnico.

2.1.5 Modelo de Causalidade de Acidentes

A NAT distingue entre dois tipos fundamentais de acidentes (Perrow, 1999; Rosness et al., 2010, cap. 5.1):

- **Acidentes de falha de componente:** causados pela falha de um ou dois componentes, sem interações inesperadas. Envolvem cadeias causais relativamente claras e podem ser identificados através de métodos padrão de análise de risco, como FMECA. Normalmente estão associados a sistemas com acoplamento solto ou baixa complexidade. São acidentes menos controversos do ponto de vista investigativo.
- **Acidentes de sistema ("acidentes normais"):** caracterizados por múltiplas interações inesperadas entre falhas. O "tamanho" da falha não é proporcional ao seu resultado – falhas menores podem produzir consequências catastróficas devido às características do sistema. Emergem de combinações de falhas aparentemente triviais em ambientes altamente complexos e estreitamente acoplados. Caracterizam-se por: múltiplas falhas interagindo de forma imprevisível, perda de visibilidade situacional, dificuldade de intervenção efetiva e propagação rápida e não linear.

Perrow argumenta que esses acidentes não são anomalias, mas consequências estruturais, sendo por isso chamados de "normais" ou "sistêmicos". Conforme afirmou, quando um operador é "confrontado por interações inesperadas e geralmente misteriosas entre falhas, dizer que ele deveria ter feito uma coisa em vez de outra só é possível após o fato" (Perrow, 1999, p. 9). Esta perspectiva recusa atribuir causalidade ao "erro humano", localizando-a nas propriedades estruturais do sistema. Hopkins (1999) destaca que tais acidentes desafiam atribuições tradicionais de culpa porque decorrem de propriedades sistêmicas.

2.1.6 Forças e Limitações

Forças

- **Fundação Sociológica Sólida:** a NAT representa uma das primeiras tentativas de integrar rigorosamente fatores técnicos e organizacionais em

uma teoria coerente de acidentes. Ao enraizar-se na sociologia organizacional, oferece profundidade analítica que transcende explicações puramente técnicas ou comportamentais (Perrow, 1984; Dekker, 2019).

- **Desculpabilização Sistemática do Operador:** a teoria fornece fundamentação teórica para resistir à tendência universal de culpar trabalhadores da linha de frente. Ao localizar a causalidade nas propriedades estruturais do sistema, desloca o foco de indivíduos "deficientes" para sistemas "inerentemente vulneráveis" (Weick, 1990).
- **Framework Analítico:** as dimensões de complexidade/acoplamento oferecem ferramentas conceituais para avaliar vulnerabilidades sistêmicas. A matriz de classificação permite comparações entre sistemas e identificação de zonas de maior risco (Rosness et al., 2010).
- **Vocabulário Conceitual:** a NAT estabeleceu terminologia amplamente adotada – "acoplamento estreito", "complexidade interativa", "acidentes de sistema". Este vocabulário estrutura conversações sobre segurança em múltiplas indústrias.
- **Humildade Epistêmica:** a teoria cultiva o reconhecimento de que nem todas as falhas podem ser antecipadas ou prevenidas – uma perspectiva importante contra o otimismo tecnológico ingênuo (Dekker, 2019).

Limitações

- **Imprecisão Conceitual:** os conceitos de "complexidade interativa" e "acoplamento estreito" são intuitivamente atraentes, mas difíceis de operacionalizar. Como Hopkins (1999) observou, é desafiador medir ou monitorar tais atributos, dificultando testes empíricos rigorosos e aplicações práticas.
- **Aplicabilidade Explanatória Limitada:** vários críticos argumentam que poucos acidentes de alto perfil das últimas décadas são verdadeiros "acidentes normais" no sentido estrito de Perrow. Hopkins (2014) sugere que a maioria resulta de má gestão, pressões de custo e fatores organizacionais claramente identificáveis – não de interações incompreensíveis.
- **Dificuldade Prescritiva:** é difícil derivar prescrições práticas para avaliação ou monitoramento de risco a partir da teoria. Reconhecer que um sistema é "interativamente complexo" oferece pouca orientação sobre o que fazer a respeito.
- **Tendência ao Fatalismo:** a conclusão de que certas tecnologias devem

ser abandonadas é vista por muitos como politicamente inaceitável ou excessivamente pessimista. Críticos argumentam que tal fatalismo pode desencorajar esforços de melhoria de segurança (Rijpma, 2003).

- **Estaticidade:** a teoria apresenta propriedades de sistemas como relativamente fixas. Desenvolvimentos subsequentes (Weick, 1990; Le Coze, 2015) sugeriram que complexidade e acoplamento podem variar dinamicamente conforme condições operacionais – em crises, sob estresse e em estados degradados, o acoplamento efetivo pode aumentar momentaneamente.

2.1.7 Debates e Controvérsias: NAT versus HRT

O debate entre a Teoria dos Acidentes Normais e a Teoria da Alta Confiabilidade (*High Reliability Theory – HRT*) constitui uma das controvérsias mais produtivas da ciência da segurança. Enquanto a NAT argumenta que acidentes em sistemas complexos são, no longo prazo, inevitáveis, a HRT demonstra que organizações podem alcançar níveis extraordinários de segurança através de práticas organizacionais específicas (Sagan, 1993; La Porte & Rochlin, 1994).

Scott Sagan (1993), em *The Limits of Safety*, cristalizou o debate enquadrando as teorias como perspectivas "pessimista" (NAT) e "otimista" (HRT). A obra de Sagan, ao testar empiricamente as duas teorias contra acidentes do programa nuclear militar dos EUA, deu enquadramento polêmico à controvérsia (Bourrier, 2011).

Pesquisadores da escola HRO, como La Porte e Rochlin (1994), argumentam que estudos de campo em operações nucleares, aeronáuticas e militares mostram desempenhos seguros sustentados por cultura organizacional, redundâncias e comunicação eficaz. Um ponto crucial de contestação é a afirmação de Perrow de que organizações não podem ser centralizadas e descentralizadas simultaneamente. La Porte e Rochlin (1994) sustentam que, nas HROs estudadas, **estruturas descentralizadas existem em estado latente ou transitório dentro de hierarquias centralizadas, sendo "acionadas sob demanda"** em momentos críticos – não como uma alternância simétrica entre dois modos, mas como uma arquitetura dialética em que a descentralização é tolerada justamente por seu caráter circunstancial.

Perrow (1999), em resposta, retruca que esses exemplos são exceções que confirmam a regra e, mesmo assim, permanecem vulneráveis a falhas catastróficas. Contudo, como argumentam Hopkins (1999) e Rijpma (1997, 2003), as perspectivas podem ser melhor entendidas como **complementares** do que contraditórias: a NAT alerta sobre vulnerabilidades estruturais inerentes a certos tipos de sistemas; a HRT indica como essas vulnerabilidades podem ser parcialmente gerenciadas. Rijpma (2003) propõe que o debate, após mais de duas décadas, evoluiu de um "impasse" para um terreno comum em que ambas as teorias contribuem para uma análise multinível de segurança.

2.1.8 Desenvolvimentos Recentes

Desde os anos 2000, a Teoria dos Acidentes Normais tem sido revisitada sob novas perspectivas teóricas e empíricas, impulsionada tanto pela ocorrência de acidentes de grande escala (Deepwater Horizon, 2010; Fukushima, 2011) quanto pelo avanço de campos como engenharia de resiliência, ciência de sistemas complexos e sociologia das organizações. O consenso emergente é que, embora a formulação original de Perrow (1984; 1999) permaneça altamente influente, ela requer atualização para lidar com as características dos sistemas modernos – cada vez mais digitais, distribuídos e opacos.

A releitura multiescalar de Le Coze (2015)

Um dos desenvolvimentos mais importantes foi a reinterpretação proposta por Jean-Christophe Le Coze (2015), no artigo *1984–2014. Normal Accidents. Was Charles Perrow Right for the Wrong Reasons?*, que propõe uma "leitura pós-NAT". O autor argumenta que os conceitos centrais da teoria – complexidade, acoplamento e inevitabilidade – precisam ser recolocados em uma perspectiva **multiescalar**, que articula três camadas analíticas frequentemente negligenciadas nas interpretações puramente tecnológicas da NAT: (i) a camada **cognitiva** (como operadores constroem sentido sob a complexidade), (ii) a camada **organizacional** (estruturas, culturas, decisões), e (iii) a camada **macrosistêmica** (governança, regulação, economia política).

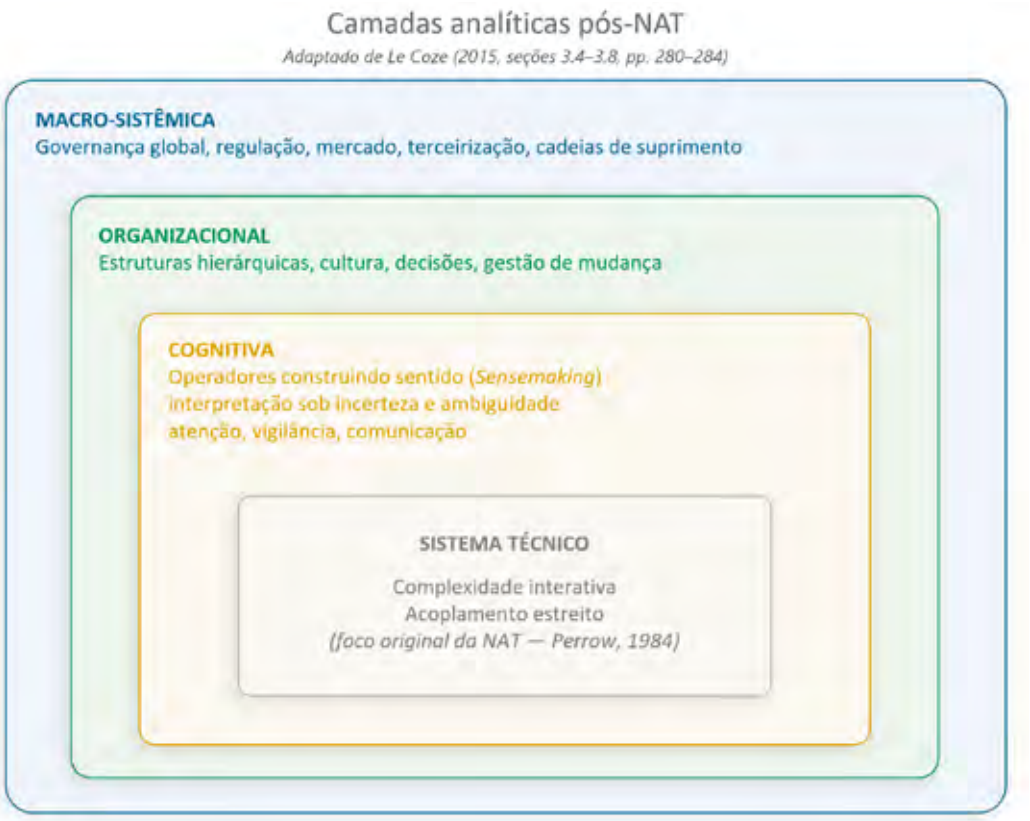


Figura 2.1.4. Camadas analíticas pós-NAT propostas por Le Coze (2015). *o sistema técnico – foco original de Perrow – está embutido em camadas cognitiva, organizacional e macro-sistêmica que precisam ser articuladas para compreender acidentes contemporâneos. Adaptado de Le Coze (2015, seções 3.4–3.8, pp. 280–284).*

Em vez de tratar acidentes como inevitáveis apenas por características técnicas estruturais, Le Coze (2015, 2021) sugere que a modernidade tardia introduziu novas camadas de risco: governança global fragmentada, terceirização crescente, dependência de software e cadeias de suprimento longas e opacas. Sistemas perigosos não seriam apenas mais complexos – seriam também mais difíceis de compreender e governar.

Os "acidentes racionais" de Downer (2024)

Outro avanço importante vem da obra de John Downer (2024), que desenvolve o conceito de **rational accidents** (acidentes racionais). Downer argumenta que decisões de engenharia – mesmo quando tomadas rigorosamente segundo métodos formais de qualificação e certificação – carregam incertezas profun-

das e inevitáveis. Acidentes catastróficos, nessa perspectiva, não decorrem de negligência ou erro, mas da própria natureza dos processos de validação tecnológica. O ponto complementa e aprofunda o argumento de Perrow: mesmo sob condições ideais de projeto e verificação, existem limites epistemológicos que tornam impossível prever todas as interações ou todos os modos de falha. A discussão contemporânea passa, assim, a combinar a **inevitabilidade estrutural** de Perrow, com a **inevitabilidade epistêmica** de Downer.

NAT, resiliência e dinâmica do acoplamento

Outro eixo de desenvolvimento envolve a conexão da NAT com teorias de resiliência. Dekker (2019) observa que a crítica contemporânea não rejeita a ideia de inevitabilidade, mas argumenta que sistemas complexos podem desenvolver capacidades adaptativas que modificam – embora não eliminem – o panorama de risco. Sob essa lente, a NAT não seria uma teoria sobre fracasso, mas uma teoria sobre **limites**: ela define o espaço de possibilidades dentro do qual abordagens resilientes precisam operar. Rosness et al. (2010) reforçam esse argumento ao mostrar como organizações modernas lidam com combinações de incerteza, variabilidade operacional e acoplamentos rígidos.



Adicionalmente, Hopkins (2014) observou que, embora a teoria continue sendo amplamente citada, com frequência isso representa mais uma "citação acadêmica ritual" do que aplicação substantiva. A NAT permanece influente como um framework conceitual, mesmo quando sua aplicabilidade específica é questionada. Desenvolvimentos em teoria da complexidade e sistemas adaptativos complexos têm oferecido novos vocabulários para fenômenos que Perrow identificou intuitivamente, como a imprevisibilidade de interações em sistemas fortemente acoplados.

A NAT contemporânea, portanto, é menos uma teoria sobre inevitabilidade absoluta e mais um arcabouço para compreender os **limites da previsibilidade e do controle** em sistemas sociotécnicos de alta criticidade.

2.1.9 Implicações para a Indústria de Energia

A indústria de óleo, gás e energia apresenta diversas características que a NAT identifica como vulnerabilidades estruturais: plataformas offshore são sistemas complexos com equipamentos densamente empacotados (aumentando a complexidade interativa), processos fortemente interdependentes (acoplamento estreito) e potencial catastrófico significativo.

Grande parte das vulnerabilidades operacionais não decorre de falhas isoladas, mas de interações complexas entre subsistemas críticos: processo, utilidades, automação, logística marítima, integridade estrutural e governança operacional. Nas plataformas offshore, a coexistência de **SIMOPS** (operações simultâneas – trabalhos a quente, içamento, perfuração, intervenções, comissionamento) intensifica a complexidade interativa, uma vez que pequenas perturbações em uma atividade podem alterar condições de outra, criando sequências de eventos imprevistas. As análises de risco tradicionais tendem a tratar essas atividades de maneira segmentada, subestimando o potencial de acoplamentos emergentes sob pressão operacional (Hopkins, 1999; Rosness et al., 2010).

A **gestão de integridade** também se alinha fortemente à NAT. Em *topsides* densamente compactados, alterações físicas aparentemente inofensivas – suportes adicionais, novos trechos de tubulação, derivações de instrumentação ou modificações temporárias (MOCs emergenciais) – podem gerar novas vias de interação não intencionais. Esses efeitos só se tornam visíveis quando múltiplos sistemas entram em "ressonância" operacional: por exemplo, vibrações estruturais que afetam sensores, que alteram automaticamente malhas de controle, que mudam condições de processo e, por fim, tensionam barreiras de integridade mecânica. Esse tipo de encadeamento é precisamente o fenômeno que a NAT descreve como interações inesperadas em sistemas complexos.

No ambiente marítimo associado ao *upstream*, a interação entre unidades flutuantes (FPSOs, MODUs, FSOs) e embarcações de apoio, somada às condições meteoceanográficas, cria outra camada de complexidade. Manobras próximas, *Dynamic Positioning* (DP), operações de *offloading* e transferência de fluidos ampliam a probabilidade de perturbações externas – colisões, perda de posicionamento, efeito de embarcação sobre *risers* e linhas flexíveis – se combinarem

com vulnerabilidades internas da planta, evidenciando a estrutura da NAT de sistemas que "falham pela interação entre partes que deveriam ser independentes".

Por fim, a crescente **digitalização** – sistemas de monitoramento em tempo real, *analytics*, automação avançada, redes OT/IT integradas – aumenta a opacidade informacional, pois os estados do processo passam a ser cada vez mais mediados por camadas de software. Em alinhamento ao argumento de Perrow e às atualizações contemporâneas (Dekker, 2019; Le Coze, 2015), a digitalização introduz novos caminhos pelos quais microfalhas podem se combinar rapidamente e silenciosamente, dificultando ao operador identificar onde o sistema se encontra em sua trajetória em direção ao acidente.

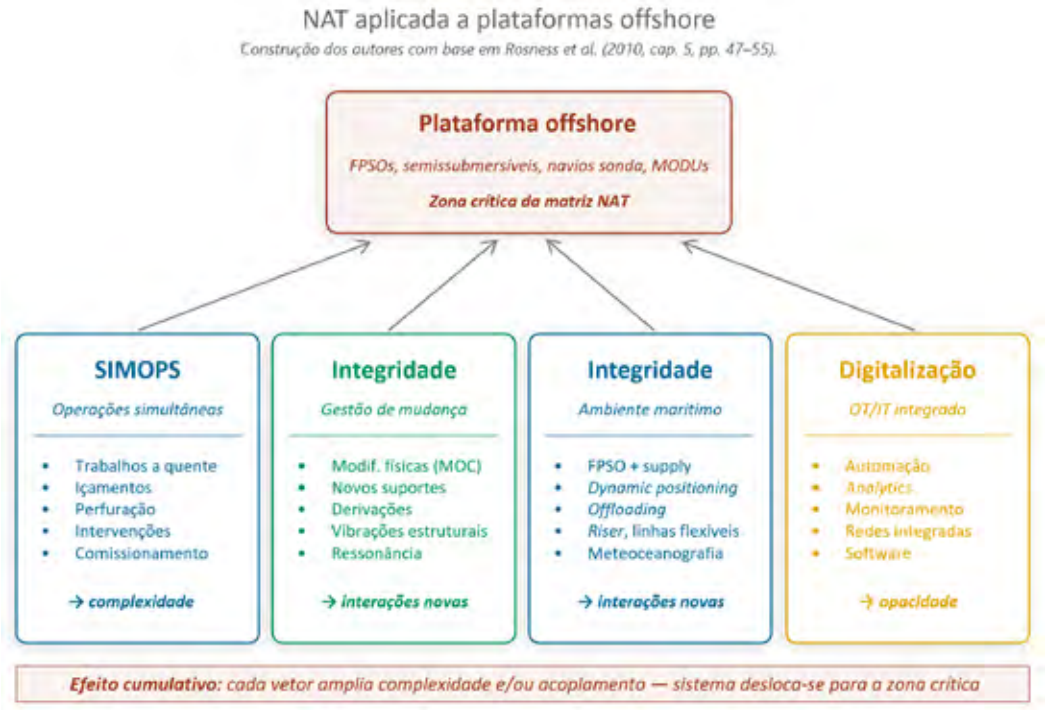


Figura 2.1.5. Aplicação da NAT a plataformas offshore. *Quatro vetores principais – SIMOPS, integridade e gestão de mudança, logística marítima e digitalização – ampliam, cada um a seu modo, a complexidade interativa e/ou o acoplamento efetivo do sistema, deslocando a plataforma para a zona crítica. Elaboração própria com base em Rosness et al. (2010, cap. 5, pp. 47–55).*

Contribuições da NAT

- **Análise de acoplamento:** framework para avaliar o grau de acoplamento entre sistemas e identificar onde introduzir "folgas" (*buffers*) que permitam intervenção humana ou automática antes da propagação total da perturbação.
- **Avaliação de complexidade interativa:** ferramenta conceitual para identificar onde interações inesperadas podem ocorrer – particularmente útil para revisões de projeto, análises de mudança (MOC) e planejamento de SIMOPS.
- **Humildade epistêmica:** talvez a contribuição mais duradoura. Reconhecimento de limites: nem todas as interações podem ser antecipadas; nem todos os cenários de falha podem ser imaginados; a análise de risco mais rigorosa permanece incompleta.

Cautelas na Aplicação

A aplicação da NAT não deve levar ao fatalismo. Conforme sugerido por Rosness et al. (2010), estratégias derivadas da teoria incluem: reduzir o grau de complexidade interativa onde possível, buscar formas de afrouxar acoplamentos, construir organizações descentralizadas para sistemas complexos e centralizar para sistemas fortemente acoplados. Quando nenhuma dessas estratégias é viável e o potencial catastrófico é alto, a teoria sugere reconsiderar a tecnologia – uma conclusão que, embora radical, merece consideração séria em avaliações de risco.

- **Evitar leituras fatalistas:** a NAT é um diagnóstico, não uma declaração para "não fazer nada"; interpretá-la de forma fatalista é equivocado, pois existem diferenças reais de desempenho entre organizações que operam tecnologias parecidas. O uso inteligente é reconhecer a tendência estrutural ao "inevitável" sem renunciar aos ganhos marginais importantes que vêm de boa engenharia e boa organização.
- **Não confundir regra empírica com mensuração:** "complexidade" e "acoplamento" são conceitos qualitativos com imprecisão operacional. Pretender medi-los como escala única pode gerar falsa precisão. A recomendação é usá-los para estruturar perguntas ("onde interações podem surpreender?", "quais dependências comuns existem?"), não para gerar pontuações absolutas.

- **Articular NAT com resiliência sem diluir limites:** estratégias de resiliência (adaptação, monitoramento, resposta) ajudam, mas não eliminam o risco inerente ao quadrante crítico da NAT. O ganho real está em deslocar o sistema para zonas menos perigosas, não em negar seus limites de controlabilidade.
- **Considerar o alto nível de abstração da teoria:** a formulação de Perrow é macrossociológica. Ela não fornece orientação prescritiva detalhada, não oferece métodos operacionais e não especifica critérios práticos para redesign. Sua função é diagnóstica, não prescritiva.
- **Evitar interpretar complexidade e acoplamento como propriedades fixas:** em muitas operações industriais – sobretudo em óleo e gás – o grau de acoplamento varia ao longo do tempo, dependendo do modo de operação (start-up, shut-down, SIMOPS, emergências). A complexidade efetiva também muda em função de sobrecarga cognitiva, estados degradados e falhas parciais de automação. Aplicar a NAT requer reconhecer a variabilidade operacional, não apenas a estrutura estática (Weick, 1990; Le Coze, 2015).

2.1.10 Quadro-Resumo: Teoria dos Acidentes Normais

Dimensão	Teoria dos Acidentes Normais (NAT)
Período de Surgimento	**1984 (publicação de Normal Accidents: Living with High-Risk Technologies)**
Principais Autores	**Charles Perrow (1925–2019), sociólogo organizacional, Yale University**
Fundamento Teórico	**Sociologia organizacional, teoria de sistemas, estudos de ciência e tecnologia.**
Pressuposto Central	**Acidentes são inevitáveis em sistemas que combinam alta complexidade interativa e acoplamento estreito, devido a dilema organizacional insolúvel (necessidade simultânea de centralização e descentralização).**

Dimensão	Teoria dos Acidentes Normais (NAT)
Concepção de Risco	Risco como propriedade estrutural da complexidade — acidentes emergem das características inerentes do sistema, não de falhas individuais.
Visão da Contribuição Humana	Operadores são confrontados por interações incompreensíveis; erro humano é sintoma, não causa.
Estratégias de Controle	Reduzir complexidade interativa, afrouxar acoplamentos, adequar estrutura organizacional; em último caso, abandonar a tecnologia.
Modelo de Causalidade	Acidentes de sistema resultam de múltiplas falhas interagindo de formas não antecipadas, propagando-se rapidamente em sistemas fortemente acoplados.
Forças	Fundação sociológica sólida; desculpabilização sistemática do operador; framework analítico influente; vocabulário conceitual amplamente adotado; humildade epistêmica.
Limitações	Conceitos imprecisos difíceis de operacionalizar; aplicabilidade limitada a acidentes reais; dificuldade prescritiva; tendência ao fatalismo; estaticidade.

Referências da Seção 2.1

Bourrier, M. (2011). *The legacy of the theory of high reliability organizations: An ethnographic endeavor* (Working Paper N°6/2011). Université de Genève. https://archive-ouverte.unige.ch/unige:14839

Dekker, S. W. A. (2019). *Foundations of safety science: A century of understanding accidents and disasters*. CRC Press / Routledge. https://doi.org/10.4324/9781351059794

Downer, J. R. (2024). *Rational accidents: Reckoning with catastrophic technologies*. MIT Press. https://doi.org/10.7551/mitpress/8844.001.0001

Hopkins, A. (1999). The limits of normal accident theory. *Safety Science, 32*(2–3), 93–102. https://doi.org/10.1016/S0925-7535(99)00015-6

Hopkins, A. (2001). Was Three Mile Island a 'normal accident'? *Journal of Contingencies and Crisis Management, 9*(2), 65–72. https://doi.org/10.1111/1468-5973.00155

Hopkins, A. (2014). Issues in safety science. *Safety Science, 67*, 6–14. https://doi.org/10.1016/j.ssci.2013.01.007

La Porte, T. R., & Rochlin, G. (1994). A rejoinder to Perrow. *Journal of Contingencies and Crisis Management, 2*(4), 221–227. https://doi.org/10.1111/j.1468-5973.1994.tb00046.x

Le Coze, J.-C. (2015). 1984–2014: Normal accidents. Was Charles Perrow right for the wrong reasons? *Journal of Contingencies and Crisis Management, 23*(4), 275–286. https://doi.org/10.1111/1468-5973.12090

Le Coze, J.-C. (2021). *Post normal accident: Revisiting Perrow's classic*. CRC Press / Taylor & Francis.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies* (2ª ed., com novo posfácio e postscript sobre o problema Y2K). Princeton University Press.

Perrow, C. (2011). Fukushima and the inevitability of accidents. *Bulletin of the Atomic Scientists, 67*(6), 44–52. https://doi.org/10.1177/0096340211426395

Rijpma, J. A. (1997). Complexity, tight-coupling and reliability: Connecting normal accidents theory and high reliability theory. *Journal of Contingencies and Crisis Management, 5*(1), 15–23. https://doi.org/10.1111/1468-5973.00033

Rijpma, J. A. (2003). From deadlock to dead end: The normal accidents–high reliability debate revisited. *Journal of Contingencies and Crisis Management, 11*(1), 37–45. https://doi.org/10.1111/1468-5973.1101004

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærø, I. (2010). *Organisational accidents and resilient organisations: Six perspectives* (Report SINTEF A17034, Revision 2). SINTEF Technology and Society.

Sagan, S. D. (1993). *The limits of safety: Organizations, accidents, and nuclear weapons*. Princeton University Press.

Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management, 16*(3), 571–593. https://doi.org/10.1177/014920639001600304

2.2 Teoria da Alta Confiabilidade e as Organizações de Alta Confiabilidade (HRT/HRO)

Autores: Priscilla Salles de Moraes e Rafael Ceni de Almeida

Revisão: Eder Henriqson

2.2.1 Introdução e Contexto Histórico

A Teoria da Alta Confiabilidade (High Reliability Theory – HRT) e o conceito de Organizações de Alta Confiabilidade (High Reliability Organizations – HROs) emergiram em meados dos anos 1980 como resposta a uma pergunta aparentemente simples: como certas organizações que operam tecnologias intrinsecamente perigosas, como porta-aviões nucleares, o controle de tráfego aéreo, entre outras, mantêm registros de segurança extraordinários por longos períodos? Na época, essa pergunta desafiava tanto o senso comum quanto a Teoria dos Acidentes Normais de Charles Perrow (1984), que sugeria a inevitabilidade de acidentes em sistemas complexos e fortemente acoplados (ver Seção 2.1).

A pesquisa em HRO nasceu na Universidade da Califórnia, em Berkeley, onde um grupo interdisciplinar de pesquisadores, conhecido como o grupo de Berkeley, iniciou um programa sistemático de investigação sobre organizações que pareciam desafiar as probabilidades estatísticas de acidentes. Conforme Bourrier (2011), o grupo reunia Todd La Porte, cientista político e líder intelectual; Karlene Roberts, psicóloga organizacional responsável por grande parte dos estudos de campo; Gene Rochlin, cientista político especializado em energia e recursos; e Paul Schulman, especialista em administração pública. Posteriormente, Karl Weick e Kathleen Sutcliffe retomaram e desenvolveram esses achados, contribuindo para a sistematização e a difusão desses achados em um modelo teórico de maior alcance (Weick et al., 1999; Weick & Sutcliffe, 2015).

> *"A Organização de Alta Confiabilidade (HRO) não é uma teoria descrita por um único autor. É, antes, um conjunto de princípios comuns ou afiliados que foram desenvolvidos ao longo do tempo e por diferentes autores. Embora os pesquisadores por trás dessas ideias compartilhem uma forma comum de olhar para organizações altamente complexas e perigosas, diferentes autores adicionaram ideias e percepções, o que levou a múltiplos modelos de HRO ou componentes da teoria"* (Dekker, 2019, p. 281).

O contexto histórico desta pesquisa é particularmente significativo. O grupo de Berkeley iniciou seus trabalhos dois a três anos após a publicação do influente livro *Normal Accidents* de Charles Perrow (1984). Tanto Perrow quanto La Porte haviam sido membros da comissão especial convocada pelo presidente Jimmy Carter após o acidente de Three Mile Island em 1979 (Bourrier, 2011). Os seis grandes temas que orientaram a agenda original do grupo são sintetizados por Bourrier (2011, p. 9): evolução das HROs como entidades; padrões estruturais e gestão da interdependência; dinâmica decisória sob alta confiabilidade; cultura organizacional da confiabilidade; inserção de novas tecnologias em sistemas de alto risco; e desenho de sistemas organizacionais com consequências críticas.

Sobre o método: Estudos de Operações Normais

Uma contribuição metodológica decisiva foi a opção do grupo por estudos etnográficos de operações normais – *Normal Operations Studies* – em contraste com a tradição dominante de análises retrospectivas de acidentes (Bourrier, 2011; Rochlin, 1996). Em vez de perguntar por que organizações falham, os pesquisadores foram a campo investigar como organizações bem-sucedidas mantêm o sucesso no cotidiano. Essa inversão metodológica está hoje na base de boa parte da pesquisa em Engenharia de Resiliência (ver Seção 2.4).



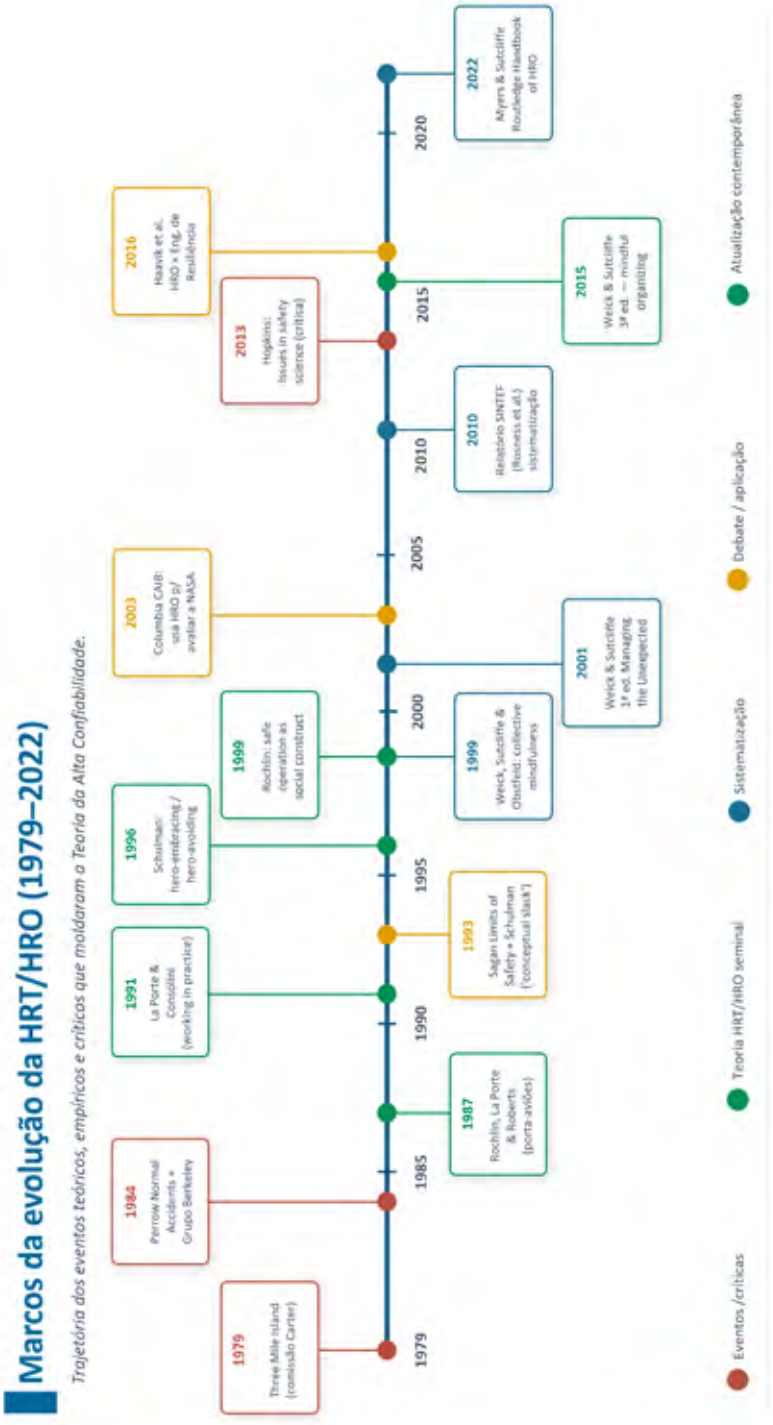


Figura 2.2.1: Marcos da evolução da Teoria da Alta Confiabilidade e das HROs. *Construção dos autores a partir de Bourrier (2011), Hopkins (2014), Weick & Sutcliffe (2015), Dekker (2019) e Myers & Sutcliffe (2022).*

2.2.2 Pressupostos Críticos

Rosness et al. (2010) sistematizam três hipóteses centrais que distinguem a HRT das demais perspectivas sobre acidentes organizacionais:

1. **Inevitabilidade do erro humano.** Não é factível eliminar totalmente as ações errôneas em sistemas complexos.
2. **Possibilidade de desempenho quase livre de falhas.** É possível alcançar desempenho quase perfeito por meio de redundância organizacional, de modo que praticamente todas as ações errôneas sejam recuperadas antes de causarem danos severos.
3. **Capacidade adaptativa frente a demandas extremas.** Algumas organizações conseguem reconfigurar-se espontaneamente, alternando entre uma estrutura formal-hierárquica em condições rotineiras e uma estrutura informal baseada em competências em condições críticas.

Esses pressupostos contrastam diretamente com os da Teoria dos Acidentes Normais. Enquanto Perrow argumentava que organizações não podem ser simultaneamente centralizadas e descentralizadas, a HRT – apoiada pelo trabalho empírico de La Porte e Consolini (1991) – sustenta que organizações reais alternam dinamicamente entre os dois modos conforme as demandas situacionais. Esta é a tese de fundo da expressão "*working in practice but not in theory*", que dá título ao artigo seminal de La Porte e Consolini (1991).

2.2.3 Conceitos Fundamentais

Definição de HRO

Roberts (1989, 1990) propôs classificar como HROs aquelas organizações que poderiam ter falhado repetidamente, com resultados catastróficos, mas não falharam. A definição não usa padrões absolutos de segurança, mas medidas relativas de desempenho – colisões em relação ao número de movimentos, interrupções em relação às horas de serviço. Hopkins (2014) e Bourrier (2011) observam, contudo, que essa formulação é insuficiente para identificar HROs

empiricamente: as organizações originalmente estudadas "não foram tanto selecionadas quanto oferecidas aos pesquisadores" (Mannarelli et al., 1996, p. 84, citado em Hopkins, 2014, p. 3). Essa dificuldade está na raiz da reconceituação posterior de HRO como ideal-tipo – um modelo de referência contra o qual organizações reais podem ser avaliadas, em vez de uma categoria a ser identificada de forma binária.

Redundância organizacional: dimensão estrutural e dimensão cultural

La Porte e Consolini (1991) mostraram que as HROs constroem confiabilidade humana coletiva pelo mesmo princípio com que engenheiros constroem sistemas confiáveis a partir de componentes imperfeitos: redundância. Os tripulantes têm tarefas e competências sobrepostas, mantêm contato visual direto e comunicação contínua, e a cultura encoraja intervenção mútua sobre erros e desvios. Rosness et al. (2010) ampliaram essa formulação ao distinguir duas dimensões inseparáveis da redundância organizacional (Figura 2.2.2):

1. **Dimensão estrutural-instrumental.** Possibilidade material de observação mútua: competências sobrepostas, rodízio de funções, diversidade e qualidade dos canais de comunicação (notadamente face a face, segundo Weick, 1987).
2. **Dimensão cultural.** Disposição e capacidade efetivas de trocar informações, oferecer feedback, reconsiderar decisões próprias e alheias, e intervir para recuperar ações errôneas – sem que isso seja interpretado como afronta à autoridade ou à autonomia profissional.



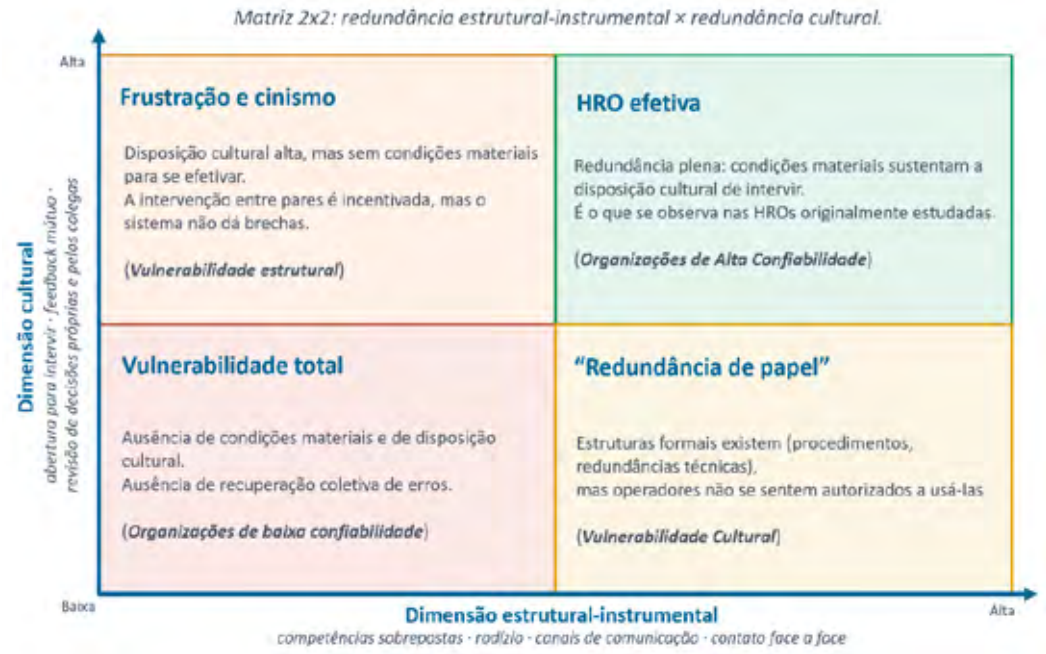


Figura 2.2.2: As duas dimensões da redundância organizacional. *Adaptado de Rosness et al. (2010, Fig. 5, p. 59), com integração de Rochlin (1999) e La Porte & Consolini (1991).*

As duas dimensões são necessárias e mutuamente dependentes. Organizações com forte redundância estrutural mas frágil dimensão cultural produzem "redundância de papel": os mecanismos formais existem, mas os operadores não se sentem autorizados a utilizá-los. O inverso – alta dimensão cultural com baixa redundância estrutural – tende a gerar frustração e cinismo, pois a disposição de intervir não encontra condições materiais para se efetivar.

Segurança como construção intersubjetiva contínua

Uma contribuição teórica fundamental de Rochlin (1999) foi conceituar a segurança operacional como construção intersubjetiva contínua – e não como ausência de acidentes ou mera gestão de riscos. Nas organizações estudadas, a segurança era um estado dinâmico mantido por engajamento ativo entre operadores e gestores:

> *"uma dialética autoconsciente entre a aprendizagem coletiva do sucesso e a crença profunda de que nenhuma aprendizagem pode ser considerada exaustiva" (Rochlin, 1999, p. 1549)*

Rochlin (1999) organiza essa construção em três propriedades observadas em todas as HROs estudadas:

- **Dualidade —** Capacidade de manter simultaneamente múltiplas representações do estado das operações – tipicamente, a representação de segurança em meio ao risco, ou de independência de ação em meio a regulação detalhada.
- **Comunicação contínua —** Fluxo constante de informação mesmo em períodos de baixa atividade operacional. Operadores experientes monitoram aquilo que à primeira vista parece tráfego trivial, porque é nele que sinais fracos de problemas iminentes costumam emergir.
- **Lócus coletivo de responsabilidade —** Erros são atribuídos à organização, não a indivíduos. A responsabilidade pelo desempenho seguro é tratada como uma propriedade emergente da coletividade.

Tipologia organizacional: *hero-embracing* e *hero-avoiding*

Schulman (1996) identificou que diferentes HROs lidam de modo radicalmente distinto com a ação individual heroica. Organizações hero-embracing – Corpo de Bombeiros, Forças Armadas em combate, equipes de resgate, despacho elétrico em emergência – celebram histórias de heróis como veículos de cultura organizacional e enfatizam resposta rápida e improvisação como chave para a confiabilidade. Organizações hero-avoiding – usinas nucleares, controle de tráfego aéreo, operação rotineira de plataformas – tratam "herói" e "cowboy" como termos pejorativos e protegem-se mais contra erros de hubris e comissão do que contra erros de timidez e omissão (Schulman, 1996, pp. 76–79). Ambas as estratégias são, segundo Schulman, adaptações racionais a ambientes técnicos e funcionais distintos.

Mindful organizing: os cinco princípios de Weick e Sutcliffe

Karl Weick e Kathleen Sutcliffe – na versão consolidada da 3ª edição de *Managing the Unexpected* (2015) – reformularam os achados da pesquisa HRO em um modelo de *mindful organizing*. A escolha do termo é deliberada: trata-se menos

de um estado mental (mindfulness) e mais de uma prática organizativa contínua – "esforço coletivo para induzir uma rica consciência de detalhe discriminatório e uma capacidade de ação" (Weick et al., 1999, p. 82, tradução nossa). Para os autores, *mindful organizing* é essencialmente sinônimo de *high reliability organizing* (Weick & Sutcliffe, 2015, p. 21). Cinco princípios estruturam essa prática, organizados em processos de antecipação (notar o inesperado antes que se manifeste) e processos de contenção ou de resposta (recuperar antes que o erro se propague):

- **Preocupação com falhas (antecipação).** Tratar quase-acidentes, sinais fracos e anomalias como sintomas de vulnerabilidades sistêmicas, não como evidências de competência. O sucesso atual é tratado como tornando o sucesso futuro menos provável.
- **Relutância em simplificar (antecipação).** Resistir a explicações simplistas; buscar entendimento profundo das situações; cultivar diversidade cognitiva e checagens cruzadas – o que Schulman, citado por Weick e Sutcliffe (2015, p. 76), chama de "partidários de perspectivas negligenciadas".
- **Sensibilidade às operações (antecipação).** Manter o quadro integrado das operações em tempo real, exigindo esforço ativo coletivo: o cuidado em monitorar o que está efetivamente acontecendo na linha de frente, e não apenas o que os relatórios indicam.
- **Compromisso com a resiliência (resposta).** Conter, recuperar e aprender com erros que inevitavelmente ocorrerão; combinação de antecipação e adaptação.
- **Deferência à expertise (resposta).** Em situações críticas, decisões fluem para quem detém o conhecimento situacional, independentemente da hierarquia formal.

Na 3ª edição (Weick & Sutcliffe, 2015, Cap. 2), os autores acrescentaram uma camada de elaboração: a infraestrutura do mindful organizing – sensemaking, organizing e managing operando em conjunto. O argumento é que os cinco princípios sozinhos não bastam; eles dependem de processos coletivos de fazer sentido das situações (sensemaking), de organizar continuamente atividades distribuídas (organizing) e de gerir o que emerge (managing). Esta elaboração resolve uma tensão que Hopkins (2014) já havia apontado: ao reformular a HRO como prática organizativa, e não como propriedade estática de certas organizações,

Weick e Sutcliffe transformam a teoria em um modelo regulativo – um padrão de referência aplicável a qualquer organização que opere sob incerteza.



Figura 2.2.3: Os cinco princípios do *mindful organizing* e o encadeamento causal até a operação segura. *Adaptado de Weick, Sutcliffe & Obstfeld (1999, 2008), Weick & Sutcliffe (2015, Cap. 2), Rochlin (1999) e Dekker (2019, Fig. 8.3).*



Outros conceitos correlatos

Dois conceitos complementares operacionalizam os princípios mais abstratos. O *Process Auditing* (Libuser, 1994, citado em Dekker, 2019, p. 298) refere-se à prática sistemática de testar equipamentos e procedimentos para identificar problemas de segurança antes que se manifestem; é frequentemente operacionalizado por mecanismos como "qualquer membro da equipe pode questionar a operação a qualquer momento" (Roberts et al., 2005). O *Conceptual Slack* (Schulman, 1993) designa a margem cognitiva e cultural que permite à organização manter, em paralelo, hipóteses conflitantes sobre o estado dos sistemas – sem fechar prematuramente o sentido de uma situação ambígua.

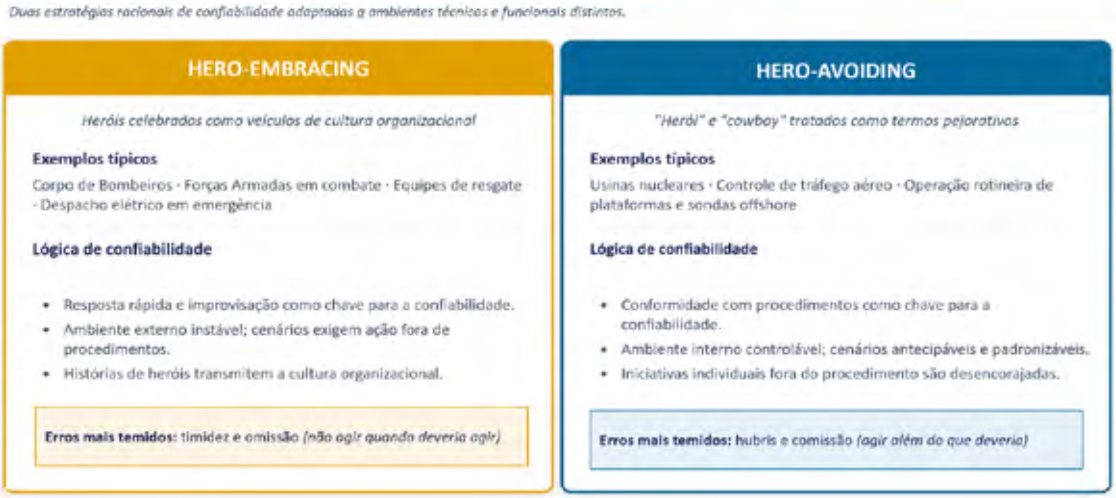


Figura 2.2.4: Tipologia de Schulman: organizações hero-embracing e hero-avoiding. *Adaptado de Schulman (1996, pp. 76–79).*

2.2.4 Estudos Empíricos Fundacionais

Os estudos empíricos originais do grupo de Berkeley focaram em três tipos de organização: porta-aviões nucleares da Marinha dos EUA, o sistema de controle de tráfego aéreo (FAA) e a gestão de redes elétricas (Pacific Gas & Electric Company). A seleção foi deliberada e dedutiva: organizações que os pesquisadores acreditavam exibir propriedades de alta confiabilidade foram escolhidas a priori (Bourrier, 2011, p. 9). É importante notar que a NASA, mesmo nos anos imediatamente posteriores ao desastre do Challenger, nunca foi considerada uma HRO pelo grupo de Berkeley (Bourrier, 2011).

O estudo mais emblemático foi realizado em porta-aviões nucleares. Rochlin, La Porte e Roberts (1987) descrevem-no como o ambiente mais extremo entre os estudados, operando "nas condições mais desafiadoras, no ambiente menos estável, e com a maior tensão entre preservar segurança/confiabilidade e maximizar eficiência operacional". A célebre descrição da operação, citada por Dekker (2019, p. 283), oferece a imagem mais nítida do problema:

> *"Então você quer entender um porta-aviões? Bem, apenas imagine que é um dia movimentado, e você encolhe o Aeroporto de São Francisco para apenas uma pista curta e um portão. Faça os aviões decolarem e pousarem ao mesmo tempo, na metade do intervalo atual, balance a pista de um lado para outro, e exija que todos que partirem pela manhã retornem no mesmo dia. [...] Então molhe tudo com água salgada e óleo, e tripule com jovens de 20 anos, metade dos quais nunca viu um avião de perto. Ah, e a propósito, tente não matar ninguém" (Rochlin et al., 1987, p. 77).*

Uma das medidas de confiabilidade utilizadas foi o *crunch rate* – quando duas aeronaves se tocam durante o movimento no convés de voo. Esta taxa era de 1 em 7.000 a 10.000 movimentos, considerada excepcionalmente baixa dadas as circunstâncias (Roberts, 1989). Os pesquisadores identificaram "camadas e camadas de atividades" que permitiam ajustes flexíveis para atingir objetivos, incluindo treinamento intenso, redundância para todos os processos, e tomada de decisão adaptativa.

Uma das métricas adotadas foi a "taxa de colisões" (*crunch rate*) – eventos em que duas aeronaves se tocam durante o movimento no convés. La Porte e Consolini (1991, p. 21) reportam, para um período de seis meses, mais de 10.000 pousos bem-sucedidos com cabo de retenção (*arrested landings*) e aproximadamente 600 movimentos diários, com *crunch rate* de cerca de 1 em 7.000. Esse índice tornou-se uma referência empírica para a formulação inicial da HRT. Os pesquisadores identificaram "camadas e camadas de atividades" (Roberts, 1990, p. 167) que permitiam ajustes flexíveis: treinamento intensivo, redundância para todos os processos e tomada de decisão adaptativa.

2.2.5 Modelo de Causalidade de Acidentes

A HRT não apresenta um modelo explícito de causalidade de acidentes; sua orientação é, deliberadamente, inversa – buscar entender o que faz organizações bem-sucedidas funcionarem (Rosness et al., 2010). Há, contudo, um modelo causal implícito que pode ser reconstruído a partir das obras seminais: acidentes resultam de erros não recuperados a tempo, em sequências nas quais os mecanismos de detecção e contenção (redundância estrutural e cultural; *mindful organizing*; reconfiguração espontânea) falharam.

Dekker (2019, §8.2.3) propõe um enquadramento mais radical: a HRO inaugura a família de teorias que entendem segurança como presença de capacidade, e não como ausência de acidentes. Esta é uma inversão epistemológica significativa em relação à tradição centrada em causas-raiz: a pergunta deixa de ser "o que deu errado?" e passa a ser "que capacidade está presente quando dá certo, e como sustentá-la?". Essa também é a base da continuidade entre HRO e Engenharia de Resiliência, discutida em 2.2.8.

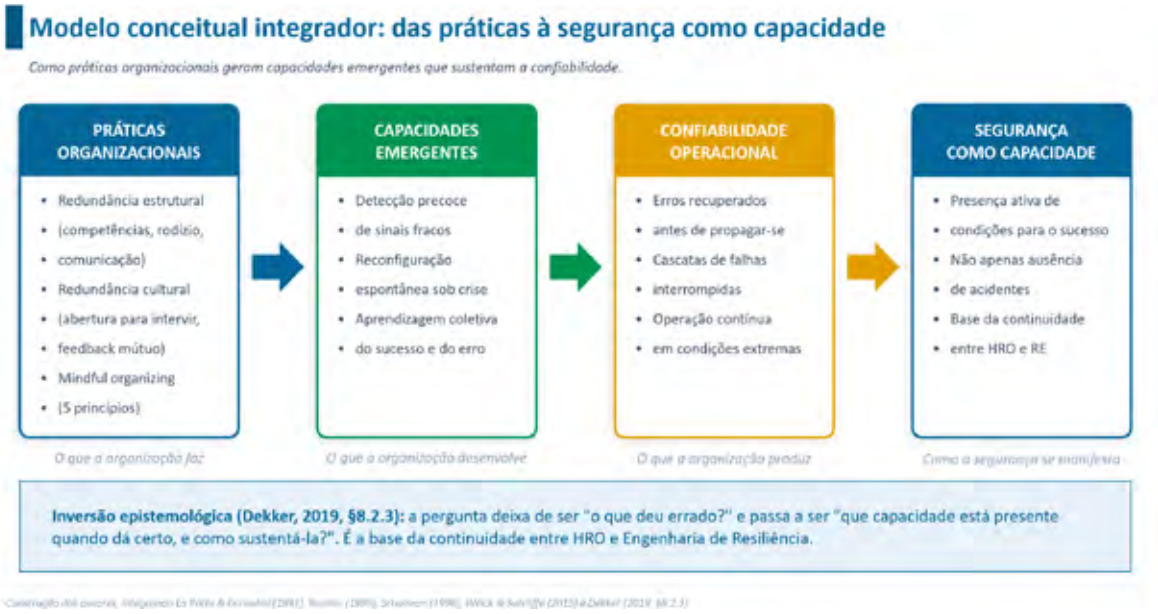


Figura 2.2.5: Modelo conceitual integrador: como práticas organizacionais geram segurança. *Construção dos autores, integrando La Porte & Consolini (1991), Rochlin (1999), Schulman (1996), Weick & Sutcliffe (2015) e Dekker (2019, §8.2.3).*

2.2.6 Forças e Limitações

Forças

- **Fundação empírica robusta.** Baseada em estudos etnográficos detalhados em organizações reais que operam sob condições extremas, com permanência prolongada dos pesquisadores em campo (Bourrier, 2011).
- **Perspectiva otimista.** Demonstra a possibilidade de excelência em segurança operacional e oferece orientação concreta para organizações que buscam melhorar.

- **Características práticas e replicáveis.** Identifica características organizacionais concretas que podem ser objeto de design organizacional deliberado.
- **Deslocamento do foco analítico.** Desloca a atenção dos fatores técnicos ou individuais para os processos organizacionais coletivos.
- **Framework avaliativo.** O modelo de *mindful organizing* de Weick e Sutcliffe (2015) oferece instrumento de diagnóstico amplamente aplicado em saúde, energia e aviação.

Limitações

- **Identificação empírica.** Hopkins (2014) argumenta que não há forma objetiva de identificar HROs a priori. O caso da NASA – classificada como HRO em 1989 (Roberts & Rousseau) e como não-HRO em 2001 (Roberts & Bea) – ilustra a dificuldade (Hopkins, 2014, p. 4).
- **Risco de captura do pesquisador.** Perrow (1994), citado por Hopkins (2014, p. 3), advertiu sobre o risco de pesquisadores serem "capturados" pelas organizações que estudam, perdendo a objetividade crítica diante do impacto sensorial de operações complexas.
- **Transferibilidade limitada.** La Porte (1996), em Dekker (2019, p. 285), concluiu que as características identificadas podem ser necessárias, mas não suficientes para garantir alta confiabilidade.
- **Altos custos de implementação.** Treinamento extensivo, redundâncias técnicas e organizacionais, e desenvolvimento contínuo de competências exigem investimentos substanciais e proteção contra pressões de custo (Rosness et al., 2010).
- **Implementação superficial.** Myers e Sutcliffe (2022) observaram que a maioria dos esforços de adoção de princípios HRO permanece superficial, o que resulta em uma compreensão rasa dos blocos fundamentais de confiabilidade.
- **Tensão descritivo-prescritivo.** A teoria oscila entre descrever o que HROs fazem e prescrever o que organizações deveriam fazer, criando ambiguidade analítica.

2.2.7 Debates e Controvérsias: NAT versus HRT

O debate entre NAT e HRT foi um dos mais produtivos da ciência da segurança. *The Limits of Safety* (Sagan, 1993) cristalizou a controvérsia enquadrando as teorias como perspectivas "pessimista" e "otimista" sobre segurança organizacional (Bourrier, 2011). Em síntese, NAT alerta sobre vulnerabilidades estruturais inerentes a sistemas complexos e fortemente acoplados; HRT indica como tais vulnerabilidades podem ser parcialmente gerenciadas por características e processos organizacionais específicos.

Hopkins (1999) e Rijpma (1997, 2003) argumentaram que as duas perspectivas são mais complementares do que contraditórias. Para Perrow (1994) – em comentário no próprio *Journal of Contingencies and Crisis Management* onde o debate se travou – "se este intercâmbio entre Sagan, La Porte e eu não fizer nada para avançar a teoria nesta área, ficarei surpreso e muito desapontado" (p. 212). A síntese contemporânea desse debate, conduzida pelo lado da NAT, é desenvolvida em maior profundidade na Seção 2.1.7. Para os fins desta seção, basta reter que: (i) a HRT contesta a tese perrowiana da impossibilidade de coexistência entre centralização e descentralização; (ii) ambas as teorias compartilham a preocupação com sistemas de alto risco; e (iii) a Parte IV do Compêndio articula um quadro integrador para o contexto brasileiro de energia.

2.2.8 Desenvolvimentos Recentes e Aplicações

A HRT continuou a evoluir após os estudos fundacionais. Weick e Sutcliffe (2015), na 3ª edição de Managing the Unexpected, transformaram achados descritivos em um framework aplicável e introduziram a noção de infraestrutura do *mindful organizing – sensemaking, organizing* e *managing* operando em conjunto. Roberts e colaboradores expandiram a aplicação para contextos de saúde (Roberts et al., 2005). Libuser, em colaboração com Roberts, formulou um conjunto operacionalizável de dez elementos de uma HRO – *process auditing*, sistema de recompensa apropriado, prevenção da degradação da qualidade, percepção do risco, comando e controle, migração da tomada de decisão, redundância de pessoas e hardware, gestores seniores com a visão integrada, regras e procedimentos formais, e treinamento (Libuser, 1994, em Dekker, 2019, p. 298).

Relação entre HRO e Engenharia de Resiliência

Haavik et al. (2019), em uma das análises mais rigorosas da literatura recente, argumentam que HRO e Engenharia de Resiliência (RE) compartilham preocupações com adaptação e capacidade organizacional, mas diferem em quatro dimensões fundamentais (Figura 2.2.6):

- **Assimetria versus simetria.** A HRO parte de uma assimetria: estuda organizações que se destacam por sucesso extraordinário. A RE adota uma simetria epistemológica: sucesso e falha são manifestações dos mesmos mecanismos (variabilidade do desempenho e ressonância funcional).
- **Normatividade.** A HRO é mais normativa, identificando características desejáveis para emulação. A RE é mais descritiva, focando em compreender a natureza da variabilidade no trabalho como ela é, sem prescrever um modelo.
- **Interlocutor (addressee).** A HRO dirige-se principalmente aos níveis gerencial e estratégico (estrutura, cultura, desenho organizacional). A RE dirige-se ao nível operacional (*sharp end*, equipes da linha de frente), onde a variabilidade adaptativa é mais visível.
- **Origem disciplinar.** A HRO emerge da ciência política, administração pública e comportamento organizacional. A RE emerge da engenharia de sistemas, dos Fatores Humanos e da psicologia industrial. As diferentes filiações disciplinares moldam o que cada perspectiva consegue ver.

Hopkins (2014) chegou a questionar se a RE oferece algo substantivamente novo além do que a HRO já apresentava – argumento contestado por Haavik et al. (2019), que sustentam que as duas perspectivas são complementares e não substituíveis. Em suas palavras: "HRO tende a estudar como organizações funcionam, enquanto RE estuda como o trabalho funciona – o mesmo fenômeno empírico visto através de lentes diferentes". O detalhamento da Engenharia de Resiliência encontra-se na Seção 2.4 deste Compêndio.



Quadro comparativo: HRT/HRO × NAT × Engenharia de Resiliência

Três perspectivas, três lentes sobre o mesmo fenômeno empírico.

	NAT *Teoria dos Acidentes Normais*	HRT/HRO *Alta Confiabilidade*	RE *Engenharia de Resiliência*
Pergunta central	Por que acidentes ocorrem em sistemas complexos?	Por que algumas organizações conseguem evitar acidentes?	Como o trabalho dá certo no dia-a-dia, apesar das pressões?
Postura epistemológica	Assimétrica (foco no fracasso)	Assimétrica (foco no sucesso)	Simétrica (sucesso e fracasso da mesma origem)
Caráter analítico	Estrutural-determinista	Normativa (modelo regulativo)	Descritiva da variabilidade
Interlocutor	Sociedade e formuladores de política	Gestores e desenho organizacional	Linha de frente (sharp end)
Origem disciplinar	Sociologia organizacional	Ciência política, administração pública	Engenharia de sistemas, fatores humanos
Conceitos-chave	Complexidade interativa · Acoplamento estreito	Mindful organizing · Redundância · Deferência à expertise	Variabilidade · Ressonância funcional · WAD/WAI
Implicação prática	Reduzir complexidade ou abandonar tecnologia	Adotar princípios HRO e cultura de confiabilidade	Apoiar trabalho-como-realizado e capacidade adaptativa

Síntese de Haavik et al. (2016): *"HRO tende a estudar como organizações funcionam, enquanto RE estuda como o trabalho funciona — o mesmo fenômeno empírico visto através de lentes diferentes."*

Síntese a partir de Haavik et al. (2016), Perrow (1984/1999), Rosness et al. (2010, Tabela 3) e Dekker (2019, Tabela 8.3).

Figura 2.2.6: Quadro comparativo HRT/HRO, NAT e Engenharia de Resiliência. *Síntese a partir de Haavik et al. (2019), Perrow (1984/1999), Rosness et al. (2010, Tabela 3) e Dekker (2019, Tabela 8.3).*

Aplicações Notáveis

- **Investigação do desastre do ônibus espacial Columbia (CAIB, 2003):** o conselho utilizou HRO como referência principal para avaliar a NASA, concluindo que a organização estava muito distante do modo como HROs operam (Dekker, 2019, p. 287).
- **Investigação da explosão de Buncefield (Reino Unido, 2005):** o comitê recomendou explicitamente a adoção de princípios HRO.
- **Aplicações em saúde:** a Joint Commission criou em 2009 o Center for Transforming Health Care, com o objetivo declarado de transformar a saúde em indústria de alta confiabilidade.

2.2.9 Implicações para a Indústria de Energia

A HRT oferece referências valiosas para a indústria de óleo, gás e energia, que opera sistemas complexos com potencial catastrófico semelhantes aos estudados pelos pesquisadores originais. Conforme a escala de risco de Amalberti (2001), a

indústria de óleo e gás opera no nível de 10^{-4} fatalidades por pessoa exposta por ano – patamar que demanda abordagens sofisticadas de gestão de segurança. A relevância para o contexto offshore é particularmente direta: Rosness et al. (2000), em estudo prévio ao relatório SINTEF, aplicaram as categorias HRO a uma plataforma de produção offshore norueguesa, identificando "considerável grau de redundância organizacional", mas também sua vulnerabilidade a pressões de redução de pessoal e terceirização.

Contribuições Potenciais



- ***Mindful organizing*.** Os cinco princípios fornecem um framework para desenvolver a capacidade de detectar e responder a sinais fracos de perigo, particularmente relevantes em operações com sondas e plataformas.
- **Deferência à expertise.** Princípio especialmente relevante para operações offshore, onde trabalhadores da linha de frente – sondador, encarregado de plataforma, técnicos de poço – frequentemente possuem o conhecimento crítico sobre condições locais que decisões remotas não conseguem capturar.
- **Redundância organizacional bidimensional.** A formulação de Rosness et al. (2010) é especialmente útil para o contexto Petrobras: chama atenção para a fragilidade da redundância "de papel" quando há rotatividade alta, equipes terceirizadas ou cultura de subordinação que inibe a intervenção entre pares.
- **Cultura de confiabilidade.** Referência para o desenvolvimento de uma cultura organizacional que prioriza segurança, com mecanismos formais (process auditing, reporte de quase-acidentes) e culturais (deferência à expertise, comunicação contínua) operando em conjunto.
- **Aprendizagem com quase-acidentes.** Fundamentação teórica para programas de reporte e análise de eventos, ancorada no princípio da preocupação com falhas: quase-acidentes e sinais fracos são tratados como precursores de vulnerabilidades sistêmicas, e não como ruído a ser filtrado.

Cautelas na Aplicação

A aplicação dos princípios HRO requer adaptação cuidadosa ao contexto específico. Roberts et al. (2005) enfatizam que os processos HRO podem falhar facilmente se não receberem atenção, tempo e investimento constantes. Hopkins (2014) alerta que HRO funciona melhor como ideal ou modelo de referência, e não como receita a ser simplesmente implementada. Myers e Sutcliffe (2022) observam que implementações superficiais tendem a falhar em gerar resultados duradouros. No contexto brasileiro, é especialmente relevante a observação de Rosness et al. (2000) sobre os efeitos do downsizing e da terceirização sobre as condições materiais e culturais da redundância organizacional: redução de pessoal pode remover condições instrumentais; terceirização pode minar a confiança e abertura mútuas necessárias para a dimensão cultural da redundância.

2.2.10 Quadro-Resumo: Teoria da Alta Confiabilidade

Dimensão	Teoria da Alta Confiabilidade (HRT/HRO)
Período de Surgimento	Meados da década de 1980 (Berkeley, Califórnia); sistematização nos anos 2000, com reformulação na 3ª ed. de Managing the Unexpected (Weick & Sutcliffe, 2015).
Principais Autores	Todd La Porte, Karlene Roberts, Gene Rochlin, Paul Schulman, Karl Weick, Kathleen Sutcliffe. Críticos: Charles Perrow, Scott Sagan, Andrew Hopkins. Sistematizadores: Mathilde Bourrier, Torgeir Haavik, Ragnar Rosness.
Fundamento Teórico	Comportamento organizacional, ciência política, administração pública, teoria da contingência; estudos etnográficos de **"***Normal Operations***"** em organizações que operam tecnologias perigosas com sucesso extraordinário.
Pressuposto Central	Erros humanos são inevitáveis, mas o desempenho quase-perfeito é possível por meio de redundância organizacional bidimensional (estrutural e cultural), mindful organizing e reconfiguração espontânea; segurança como presença de capacidade, não como ausência de acidentes.

Dimensão	Teoria da Alta Confiabilidade (HRT/HRO)
Concepção de Risco	Sistemas complexos podem ser altamente confiáveis; o risco é gerenciável através de excelência organizacional e da gestão da incerteza por *mindful organizing*.
Visão da Contribuição Humana	Humanos como solucionadores de problemas e fonte de confiabilidade; deferência à expertise independentemente da hierarquia formal.
Estratégias de Controle	Redundância técnica, social e procedimental; *mindful organizing* (cinco princípios) sustentado pela infraestrutura de *sensemaking*, *organizing e managing*; descentralização funcional sob demanda; treinamento intensivo; comunicação contínua; *process auditing*.
Modelo de Causalidade	Implícito: acidentes como erros/falhas não recuperados a tempo; foco em explicar o sucesso em vez da falha.
Forças	Fundação empírica robusta; perspectiva otimista; características concretas; deslocamento do foco de fatores individuais para processos organizacionais; framework avaliativo aplicável.
Limitações	Dificuldade de identificação empírica de "verdadeiras" HROs; altos custos; risco de implementação superficial; tensão entre elementos descritivos e prescritivos; risco de captura do pesquisador.

Referências da Seção 2.2

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. Safety Science, 37(2–3), 109–126. https://doi.org/10.1016/S0925-7535(00)00045-X

Bourrier, M. (2011). The legacy of the theory of high reliability organizations: An ethnographic endeavor (Working Paper No. 6/2011). Université de Genève.

Columbia Accident Investigation Board. (2003). Report of the Columbia Accident Investigation Board, Volume 1. NASA.

Dekker, S. W. A. (2019). Foundations of safety science: A century of understanding accidents and disasters. CRC Press. https://doi.org/10.4324/9781351059794

Haavik, T. K., Antonsen, S., Rosness, R., & Hale, A. (2019). HRO and RE: A pragmatic perspective. Safety Science, 117, 479–489. https://doi.org/10.1016/j.ssci.2016.08.010

Hopkins, A. (1999). The limits of normal accident theory. Safety Science, 32(2–3), 93–102. https://doi.org/10.1016/S0925-7535(99)00015-6

Hopkins, A. (2014). Issues in safety science. Safety Science, 67, 6–14. https://doi.org/10.1016/j.ssci.2013.01.007

La Porte, T. R. (1994). A strawman speaks up: Comments on The Limits of Safety. Journal of Contingencies and Crisis Management, 2(4), 207–211.

La Porte, T. R. (1996). High reliability organizations: Unlikely, demanding and at risk. Journal of Contingencies and Crisis Management, 4(2), 60–71.

La Porte, T. R., & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenges of high-reliability organizations. Journal of Public Administration Research and Theory, 1(1), 19–48.

Libuser, C. B. (1994). Organization structure and risk mitigation [Doctoral dissertation, University of California, Los Angeles].

Myers, C. G., & Sutcliffe, K. M. (2022). High reliability organizing: Foundations and recent developments. In K. M. Sutcliffe & C. G. Myers (Eds.), Routledge Handbook of High Reliability Organizing. Routledge.

Perrow, C. (1984). Normal accidents: Living with high-risk technologies. Basic Books.

Perrow, C. (1994). The limits of safety: The enhancement of a theory of accidents. Journal of Contingencies and Crisis Management, 2(4), 212–220.

Perrow, C. (1999). Normal accidents: Living with high-risk technologies (2ª ed.). Princeton University Press.

Rijpma, J. A. (1997). Complexity, tight-coupling and reliability: Connecting normal accidents theory and high reliability theory. Journal of Contingencies and Crisis Management, 5(1), 15–23.

Rijpma, J. A. (2003). From deadlock to dead end: The normal accidents-high reliability debate revisited. Journal of Contingencies and Crisis Management, 11(1), 37–45.

Roberts, K. H. (1989). New challenges in organizational research: High reliability organizations. Industrial Crisis Quarterly, 3(2), 111–125. https://doi.org/10.1177/108602668900300202

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. Organization Science, 1(2), 160–176. https://doi.org/10.1287/orsc.1.2.160

Roberts, K. H., & Bea, R. (2001). Must accidents happen? Lessons from high reliability organizations. Academy of Management Executive, 15(3), 70–79.

Roberts, K. H., & Rousseau, D. M. (1989). Research in nearly failure-free, high-reliability organizations: Having the bubble. IEEE Transactions on Engineering Management, 36(2), 132–139.

Roberts, K. H., Madsen, P., Desai, V., & Van Stralen, D. (2005). A case of the birth and death of a high reliability healthcare organisation. Quality and Safety in Health Care, 14(3), 216–220.

Rochlin, G. I. (1996). Reliable organizations: Present research and future directions. Journal of Contingencies and Crisis Management, 4(2), 55–59.

Rochlin, G. I. (1999). Safe operation as a social construct. Ergonomics, 42(11), 1549–1560. https://doi.org/10.1080/001401399184884

Rochlin, G. I., La Porte, T. R., & Roberts, K. H. (1987). The self-designing high-reliability organization: Aircraft carrier flight operations at sea. Naval War College Review, 40(4), 76–90.

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærø, I. (2010). Organisational accidents and resilient organisations: Six perspectives (Report SINTEF A17034, Revision 2). SINTEF Technology and Society.

Rosness, R., Håkonsen, G., Steiro, T., & Tinmannsvik, R. K. (2000). The vulnerable robustness of high reliability organisations: A case study report from an offshore oil production platform. Paper presented at the 18th ESReDA Seminar, Karlstad, Sweden, 15–16 June 2000.

Sagan, S. D. (1993). The limits of safety: Organizations, accidents, and nuclear weapons. Princeton University Press.

Schulman, P. R. (1993). The negotiated order of organizational reliability. Administration & Society, 25(3), 353–372.

Schulman, P. R. (1996). Heroes, organizations and high reliability. Journal of Contingencies and Crisis Management, 4(2), 72–82. https://doi.org/10.1111/j.1468-5973.1996.tb00079.x

Weick, K. E. (1987). Organizational culture as a source of high reliability. California Management Review, 29(2), 112–127.

Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. Administrative Science Quarterly, 38(3), 357–381.

Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). John Wiley & Sons.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. Research in Organizational Behavior, 21, 81–123.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. In A. Boin (Ed.), Crisis management (Vol. 3, pp. 31–66). Sage.

2.3 Perspectiva Rasmusseniana: Objetivos Conflitantes e Migração aos Limites

Autores: Hannah Martins e Fabiano Lima

Revisão e Figuras: Rafael Ceni de Almeida

2.3.1 Introdução e Contexto Histórico

Jens Rasmussen (1926–2018), engenheiro dinamarquês do Risø National Laboratory, foi um dos fundadores da engenharia de sistemas cognitivos e figura central na ciência da segurança contemporânea. Seu trabalho seminal, *Risk Management in a Dynamic Society: A Modelling Problem* (Rasmussen, 1997), sintetiza décadas de pesquisa interdisciplinar sobre gestão de riscos em sistemas sociotécnicos complexos. Sua relevância para a evolução da ciência da segurança é amplamente reconhecida na literatura de referência (Dekker, 2019; Le Coze, 2015).

A trajetória intelectual de Rasmussen partiu de estudos sobre controle de sistemas técnicos, passou pela interface humano-máquina e análise de erros, incorporou ciência organizacional e gestão e, finalmente, alcançou direito e legislação. Esse percurso foi catalisado pelos desastres industriais dos anos 1980 – Bhopal (1984), Challenger (1986), Chernobyl (1986), Zeebrugge (1987), Clapham Junction (1988) e Piper Alpha (1988) – e pelos workshops internacionais do Banco Mundial sobre gestão de risco, que reuniram especialistas de engenharia, psicologia, ciências sociais e direito (Rasmussen & Batstone, 1989). Os relatórios desses acidentes evidenciaram a insuficiência de modelos centrados em falha técnica isolada ou erro humano, abrindo espaço para uma agenda de pesquisa sobre o funcionamento normal de sistemas sociotécnicos sob pressão competitiva.

A perspectiva Rasmusseniana representa uma mudança paradigmática: de acidentes como *"situações de baixa probabilidade tipicamente relacionadas a situações*

complexas causadas por várias condições e eventos anormais coincidentes" (Rasmussen, 1979, conforme Le Coze, 2015, p. 132) para a visão de que *"parece haver uma migração natural em direção às fronteiras de desempenho aceitável em qualquer organização de trabalho ativa"* (Rasmussen, 1997, p. 189). A segurança passa a ser compreendida como um problema de controle dinâmico em uma sociedade em constante mudança.

2.3.2 Pressupostos Críticos

A perspectiva Rasmusseniana fundamenta-se em cinco pressupostos articulados, que a distinguem de abordagens tradicionais centradas em falha pontual:

1. **Graus de liberdade e busca adaptativa:** o comportamento humano é moldado por objetivos e restrições, mas muitos graus de liberdade permanecem abertos e são fechados por busca adaptativa guiada por critérios como carga de trabalho, custo-efetividade e risco de falha. Como observou Rasmussen, "em situações da vida real, um grande grau de liberdade é deixado ao ser humano mesmo quando o objetivo geral é declarado de forma inequívoca" (Rasmussen & Jensen, 1974).
2. **Auto-organização:** a estruturação dos processos de trabalho constitui um processo evolutivo de auto-organização, "simplesmente porque a busca otimizadora é a única forma pela qual o grande número de graus de liberdade em uma situação complexa pode ser resolvido" (Rasmussen, 1990a, p. 1186). A articulação entre graus de liberdade e auto-organização deriva diretamente dos princípios cibernéticos de Ashby (1956, 1962) e constitui a matriz teórica que distingue a tradição Rasmusseniana.
3. **Gradientes de pressão persistentes:** gradientes em direção à eficiência (pressão gerencial por produtividade) e ao menor esforço (tendência individual de buscar formas mais econômicas de execução) empurram sistematicamente as atividades em direção às fronteiras de segurança. Rasmussen (1997) emprega uma analogia termodinâmica: assim como gradientes de temperatura dirigem o fluxo de calor, gradientes organizacionais dirigem a migração do comportamento.
4. **Degradação sistêmica de defesas:** em sistemas projetados segundo a estratégia de defesa em profundidade, as defesas tendem a degradar-se

sistematicamente quando a pressão por custo-efetividade domina, pois a violação local de uma defesa não produz efeito imediato visível e, portanto, pode não ser observada em ação (Rasmussen, 1997, pp. 189–190).

5. **Tomada de decisão distribuída:** decisões com impacto na segurança são tomadas por múltiplos atores em diferentes níveis, com conhecimento incompleto. Os tomadores individuais "não conseguem visualizar o quadro completo nem julgar o estado das defesas que dependem de decisões tomadas por outros atores em outros departamentos e organizações" (Rasmussen, 1997, p. 189).

2.3.3 Conceitos Fundamentais

A partir desses pressupostos, Rasmussen desenvolveu um conjunto integrado de conceitos que explicam não apenas como acidentes ocorrem, mas, sobretudo, como são preparados ao longo do tempo por meio de adaptações rotineiras, decisões localmente racionais e pressões organizacionais persistentes.

Modelo de Migração

Três fronteiras delimitam o espaço de operação organizacional: a fronteira do comportamento financeiramente aceitável (fracasso econômico), a fronteira da carga de trabalho aceitável e a fronteira do desempenho funcionalmente aceitável (segurança). Dois gradientes persistentes – pressão gerencial por eficiência e tendência individual ao menor esforço – empurram sistematicamente as operações em direção à fronteira de segurança. Para representar a variabilidade local, Rasmussen empregou uma analogia termodinâmica:

> *"A atividade será caracterizada por variações locais induzidas pela situação dentro do espaço de trabalho, evocando os 'movimentos Brownianos' das moléculas de um gás" (Rasmussen, 1997, p. 189)*

A analogia não é meramente ilustrativa: assim como a termodinâmica modela comportamento em termos de condições de fronteira e gradientes de campo (em vez de partículas individuais e suas trajetórias), Rasmussen propõe que o comportamento organizacional seja modelado em termos de fronteiras e gradientes,

não de tarefas, atos e erros individuais (Rasmussen, 1997, p. 190). Vale registrar a ressalva de Le Coze (2015, p. 134, nota 9): a metáfora dos "movimentos brownianos" pode sugerir aleatoriedade, mas o que Rasmussen descreve são explorações adaptativas guiadas por critérios subjetivos (carga de trabalho, custo-efetividade, risco), não flutuações aleatórias – a analogia opera no nível da distribuição do comportamento, não de seu mecanismo causal.

A Figura 2.3.1 representa esse modelo: o comportamento organizacional, animado por experimentos locais para melhorar o desempenho ('movimentos brownianos'), encontra-se sob a ação simultânea da pressão gerencial por eficiência e do gradiente em direção ao menor esforço. Sem contragradientes efetivos – campanhas de cultura de segurança, instrumentação que torne os limites visíveis, monitoramento ativo do desempenho de segurança –, o sistema migra incrementalmente em direção à fronteira de desempenho funcionalmente aceitável. A fronteira percebida pelos atores raramente coincide com a fronteira real, gerando margens de erro que se reduzem silenciosamente.

Falácia da defesa em profundidade

Em sistemas com defesas funcionalmente redundantes, Rasmussen (1997) identifica um efeito paradoxal:

> *"A violação local de uma das defesas não produz efeito imediato visível e, portanto, pode não ser observada em ação. Nesta situação, a fronteira de comportamento seguro de um ator particular depende da possível violação de defesas por outros atores" (Rasmussen, 1997, pp. 189–190)*



Consequentemente, *"é frequentemente concluído por investigações de acidentes que o acidente particular estava de fato esperando para ser liberado"* (Rasmussen, 1997, p. 190). Se uma causa raiz específica fosse evitada por uma medida de segurança adicional, o acidente provavelmente seria liberado por outra causa em outro momento. Esta interpretação relativiza a noção de "causa raiz" e impõe atenção sistêmica à degradação silenciosa das camadas de proteção.

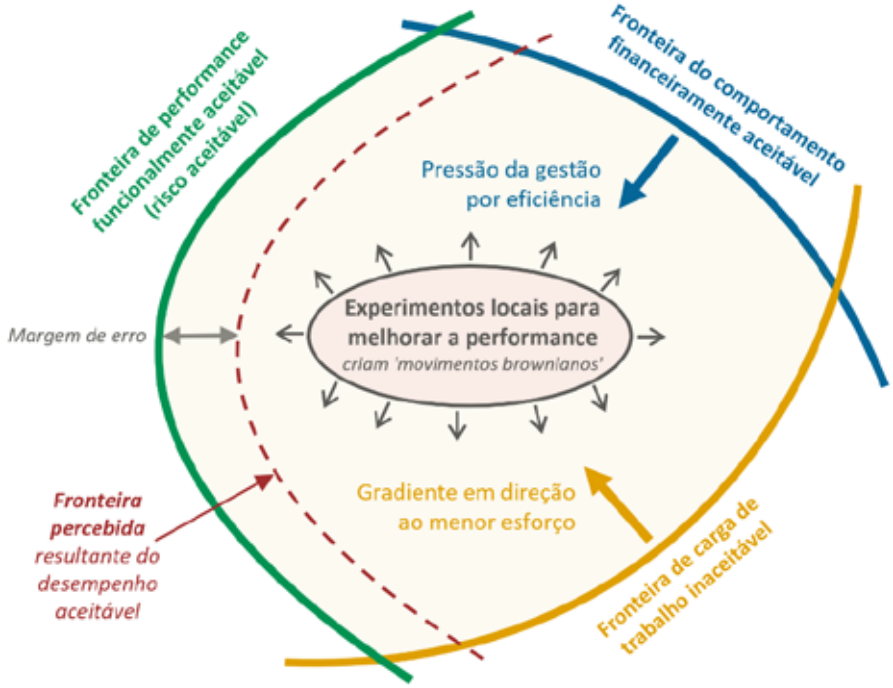


Figura 2.3.1: Migração em direção às fronteiras de desempenho seguro. *O espaço de operação é delimitado por três fronteiras: a fronteira de performance funcionalmente aceitável (risco aceitável), a fronteira do comportamento financeiramente aceitável e a fronteira de carga de trabalho inaceitável. Sob gradientes persistentes – pressão gerencial por eficiência e gradiente em direção ao menor esforço –, o comportamento organizacional tende a migrar em direção à fronteira de performance funcionalmente aceitável. Os experimentos locais para melhorar o desempenho produzem variações análogas aos 'movimentos brownianos' das moléculas de um gás. A fronteira percebida pelos atores, resultante do desempenho aceitável (linha tracejada), raramente coincide com a fronteira real, gerando uma margem de erro variável. Adaptado de Rasmussen (1997, p. 190, Fig. 3).*

Fronteiras condicionais e singularidades

Em sistemas com decisão distribuída, Rosness et al. (2010, pp. 82–83), sintetizando Rasmussen (1994), introduzem uma distinção topológica crítica: o espaço de operação é delimitado por duas fronteiras concêntricas. A fronteira interna delimita o estado de coisas incondicionalmente seguro – seguro independentemente do comportamento dos demais atores. A fronteira externa delimita o estado de coisas localmente e condicionalmente aceitável – onde a segurança depende das ações simultâneas de outros atores no sistema. Um único ator pode entrar na área entre as duas fronteiras sem desencadear risco inaceitável. Contudo, quando dois ou mais atores entram simultaneamente nessa área, o risco torna-se inaceitável – estas

coincidências são denominadas singularidades (Rosness et al., 2010, p. 82). As singularidades caracterizam-se por mudanças dramáticas no desempenho do sistema e são frequentemente percebidas, em retrospecto, como "surpresas básicas".

A Figura 2.3.2 ilustra essa configuração. Atores que migram independentemente – operadores, equipes de manutenção, contratadas, supervisores de turnos diferentes – podem, individualmente, cruzar a fronteira interna (do estado incondicionalmente seguro) sem que isso configure risco inaceitável: passam a operar em modo de segurança condicional, dependente das ações dos demais. Contudo, a coincidência dessas migrações com a invisibilidade prática dessa fronteira interna para cada ator cria as condições para uma singularidade. O fenômeno é particularmente característico de organizações em que a tomada de decisão é distribuída e em que cada ator dispõe apenas de informação parcial sobre o estado do sistema (Rasmussen, 1997).

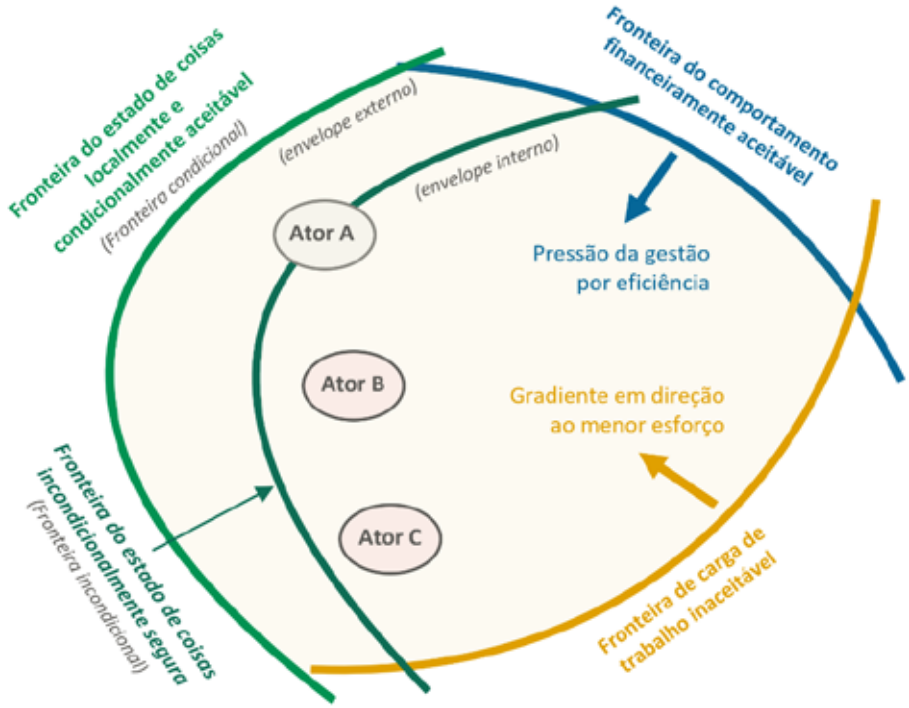


Figura 2.3.2: Adaptação em uma organização complexa, onde vários atores migram independentemente dentro do espaço de desempenho aceitável. *Duas fronteiras concêntricas delimitam esse espaço: o envelope externo é a fronteira do estado de coisas localmente e condicionalmente aceitável (composta pelas curvas do comportamento financeiramente aceitável e da carga de trabalho inaceitável); o envelope interno é a fronteira do estado de coisas incondicionalmente segura. Um único ator pode entrar na área entre as duas fronteiras sem*

desencadear risco inaceitável. Contudo, quando dois ou mais atores (A, B, C) entram simultaneamente nessa área, emergem singularidades – coincidências caracterizadas por mudanças dramáticas no desempenho do sistema, frequentemente percebidas como 'surpresas básicas'. Adaptado de Rosness et al. (2010, p. 82, Fig. 9), com base na obra de Rasmussen (1994).

Nota: *a fronteira tracejada interna na Figura 2.3.1 (fronteira percebida) e a fronteira interna na Figura 2.3.2 (fronteira do estado incondicionalmente segura) representam conceitos distintos. A primeira é subjetiva – resulta da percepção dos atores sobre o desempenho aceitável. A segunda é objetiva – define o limite além do qual a segurança passa a depender das ações dos demais atores. Ambas têm em comum, contudo, a propriedade de raramente serem visíveis para os atores no momento da decisão, o que é parte central do argumento Rasmusseniano sobre a invisibilidade prática das fronteiras de segurança.*

> *"O colapso catastrófico do sistema é uma característica normal de sistemas que possuem propriedades de auto-organização e, ao mesmo tempo, dependem de proteção contra combinações raras de condições individualmente afetadas pela adaptação" (Rasmussen, 1990b)*

Erro como experimento mal-sucedido

Diferentemente das abordagens taxonômicas predominantes, Rasmussen conceituou o erro a partir de uma perspectiva naturalística, enraizada em estudos empíricos de trabalho real:

> *"Para otimizar o desempenho e desenvolver habilidades suaves e eficientes, é muito importante ter oportunidades para realizar experimentos de tentativa e erro; e os erros humanos podem, de certa forma, ser considerados experimentos mal-sucedidos com consequências inaceitáveis. Tipicamente, são classificados como erros humanos apenas porque são realizados em um ambiente 'unkind' (hostil)" (Rasmussen, 1982, pp. 313–314)*

Um ambiente hostil é definido como aquele em que não é possível observar e reverter os efeitos de variações inapropriadas no desempenho antes que conduzam a consequências inaceitáveis. Esta visão naturalística reconhece o erro como parte do processo cognitivo normal de variabilidade adaptativa, em contraste com a abordagem taxonômica desenvolvida em paralelo por Reason (Le Coze, 2015, p. 128). Essa

redefinição desloca o foco analítico do indivíduo para o desenho do sistema, a qualidade dos feedbacks disponíveis e as margens de tolerância à variabilidade.

AcciMap: Metodologia de Análise Multinível.

O AcciMap (Rasmussen & Svedung, 2000) é uma ferramenta para mapear a natureza distribuída da tomada de decisão em sistemas sociotécnicos. Diferentemente de gráficos convencionais de causa-consequência, o AcciMap identifica todos os tomadores de decisão que influenciaram as condições do acidente por meio de suas atividades normais de trabalho, organizando-os em seis níveis hierárquicos:

- **Nível 1 – Governo, políticas e orçamento:** decisões legislativas, políticas públicas e alocação de recursos macroeconômicos.
- **Nível 2 – Órgãos reguladores e associações:** normas técnicas, regulamentação setorial e fiscalização.
- **Nível 3 – Governo local, planejamento e orçamento:** decisões no nível municipal ou regional sobre licenças, infraestrutura e aplicação de normas.
- **Nível 4 – Gestão da empresa:** políticas corporativas, alocação de recursos, estratégia comercial e cultura organizacional.
- **Nível 5 – Gestão técnica e operacional:** planejamento operações, procedimentos, manutenção, treinamento e supervisão.
- **Nível 6 – Processos físicos, atividades dos atores, equipamentos e ambiente:** ações dos operadores na linha de frente, condições de equipamento e ambiente imediato de trabalho.

Os três níveis superiores capturam fatores sistêmicos do *blunt-end*, distantes da operação; os três inferiores representam o *sharp-end*, onde as consequências se materializam (Salmon et al., 2020). Esquemas de classificação subsequentes (Branford, 2007; Goode et al., 2017) propuseram rótulos consolidados – por exemplo, agrupando os níveis 1–3 como "fatores sistêmicos e regulatórios" e os níveis 4–5 como "fatores organizacionais e de gestão" – visando facilitar a análise e a comparabilidade entre estudos.

Le Coze (2015, pp. 134–135) identifica três limitações importantes na aplicação do AcciMap: (i) a tomada de decisão em níveis superiores frequentemente resulta de

processos coletivos difíceis de decompor graficamente em ações individuais; (ii) o formato em caixas e setas tende a simplificar causalidades circulares e dinâmicas de retroalimentação em representações lineares; e (iii) há tendência ao uso da ferramenta como meio de comunicação de achados de investigação, em detrimento de seu propósito original como ferramenta analítica de cognição distribuída. Apesar dessas limitações, o AcciMap promove uma visão sociotécnica explícita de acidentes e segurança, sendo coerente com a premissa fundamental de que o risco é construído progressivamente no funcionamento cotidiano das organizações.

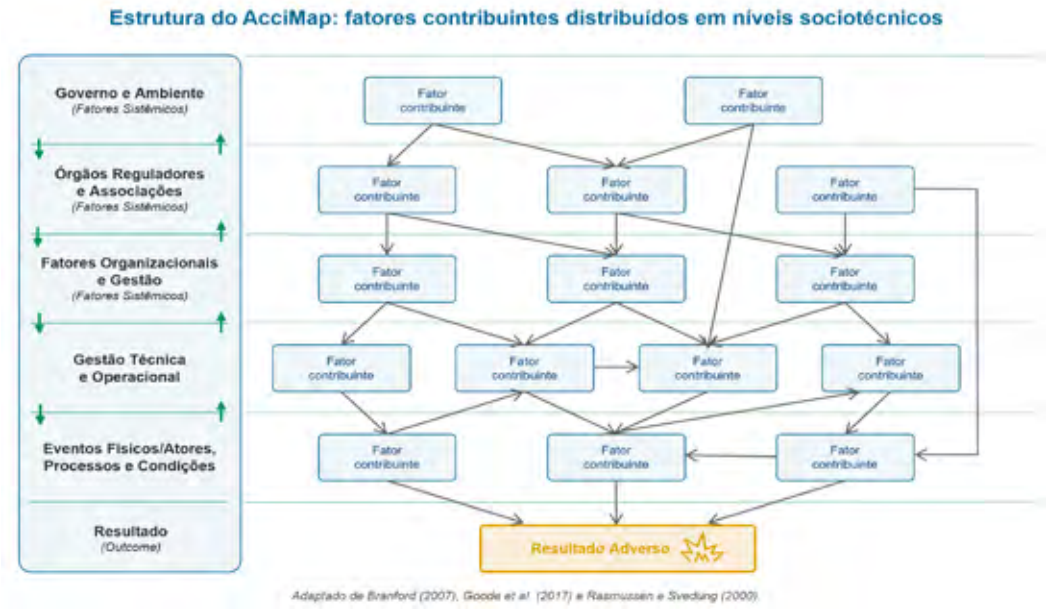


Figura 2.3.3: Estrutura do AcciMap com fatores contribuintes distribuídos em níveis sociotécnicos. *As caixas representam decisões, ações ou condições a serem identificadas a partir do relatório de investigação; as setas indicam relações de influência ou efeito colateral que cascateiam pelos níveis até produzir o resultado adverso. Adaptado de Branford (2007), Goode et al. (2017) e Rasmussen e Svedung (2000).*

2.3.4 Base Empírica

A perspectiva Rasmusseniana foi desenvolvida ao longo de décadas de pesquisa em sistemas de alto risco – energia nuclear, indústria de processos, transporte e outros domínios sociotécnicos complexos. Rasmussen (1997, p. 189) analisou acidentes como Bhopal, Flixborough, Zeebrugge e Chernobyl, concluindo que:

> *"Relatórios de tribunais de vários acidentes (...) demonstram que não foram causados por coincidência de falhas e erros humanos independentes, mas por uma migração sistemática do comportamento organizacional em direção ao acidente, sob influência de pressão por custo-efetividade em ambiente competitivo agressivo" (Rasmussen, 1997, p. 189)*

Le Coze (2015) documenta a aplicação do AcciMap por Rasmussen ao acidente de Clapham Junction, demonstrando como procedimentos de verificação redundante degradaram-se gradualmente sob pressão de tempo e restrições de força de trabalho. Na indústria de óleo e gás, o quase-*blowout* do Snorre A (28 de novembro de 2004), na plataforma norueguesa operada pela Statoil/Norsk Hydro, foi posteriormente analisado sob a perspectiva Rasmusseniana, evidenciando migração de práticas, degradação de barreiras e singularidade na coincidência de adaptações locais (Rosness et al., 2010).

A análise empírica desses casos sustenta uma conclusão central: acidentes graves raramente decorrem da coincidência aleatória de falhas independentes, mas resultam de adaptações sucessivas de diferentes atores ao longo do tempo, todas razoáveis em seus contextos locais, mas que coletivamente empurram o sistema para além de suas fronteiras de segurança. Acidentes deixam de ser anomalias inesperadas e passam a ser compreendidos como consequências possíveis – e até esperadas – do funcionamento normal de organizações complexas (Rasmussen, 1997; Le Coze, 2015).

2.3.5 Modelo de Causalidade de Acidentes

Na perspectiva Rasmusseniana, acidentes não são causados por eventos discretos, mas emergem de processos dinâmicos e históricos de migração e adaptação. A causalidade não é pontual nem localizada, mas distribuída no tempo e nos diversos níveis organizacionais que participam do controle do sistema. Quatro dimensões caracterizam esse modelo:

- **Migração gradual:** atividades migram incrementalmente em direção às fronteiras de segurança por meio de adaptações locais que parecem racionais no momento de sua execução. Reforçadas por sucessos ime-

diatos, essas adaptações tornam-se rotineiras, normalizando práticas cada vez mais próximas dos limites.

- **Cruzamento irreversível de fronteiras:** o acidente se materializa quando o sistema ultrapassa uma fronteira que não pode mais ser compensada pelos mecanismos de controle existentes. Como observa Rasmussen (1997, p. 190), "o palco para um curso acidental de eventos é muito provavelmente preparado ao longo do tempo pelos esforços normais de muitos atores em seus respectivos contextos diários de trabalho, respondendo à demanda permanente de ser custo-efetivo".
- **Interação entre atores:** decisões tomadas em diferentes níveis hierárquicos interagem de forma não linear. Em sistemas distribuídos, ações de um ator podem deslocar as fronteiras de segurança para outros atores sem que estes percebam (Rasmussen, 1997).
- **Singularidades:** acidentes resultam tipicamente de coincidências em que múltiplos atores excedem suas fronteiras condicionais simultaneamente, criando combinações específicas e raras que excedem a capacidade de absorção do sistema. Essas singularidades emergem da estrutura organizacional e das práticas normais de trabalho, mas sua materialização depende de uma convergência particular que torna o evento difícil de prever, mesmo quando os mecanismos gerais de migração são conhecidos.

2.3.6 Forças e Limitações

A perspectiva Rasmusseniana destaca-se por oferecer um enquadramento poderoso para compreender acidentes em sistemas sociotécnicos complexos, sobretudo porque desloca a análise de falhas isoladas para processos graduais de adaptação, coordenação e perda de controle. Ao mesmo tempo, justamente por operar em nível elevado de abstração e por exigir leitura multinível, esse enquadramento impõe desafios de aplicação empírica, comunicação e tradução em práticas de gestão. A avaliação de suas forças e limitações deve ser entendida menos como juízo de invalidação e mais como indicação das condições necessárias ao seu uso rigoroso.

Forças

- **Perspectiva sistêmica dinâmica:** captura a natureza adaptativa e evolutiva de sistemas sociotécnicos.
- **Integração de múltiplos níveis:** conecta decisões em níveis macro (regulatório, gerencial) com comportamentos no nível micro (operacional).
- **Reconhecimento de *trade-offs*:** explicita as tensões entre segurança, eficiência e carga de trabalho.
- **Ferramentas analíticas:** o AcciMap oferece metodologia prática para análise multinível de acidentes.

Limitações

- **Complexidade conceitual:** modelo abstrato pode ser difícil de operacionalizar na prática.
- **Capacidade preditiva limitada:** embora explique como a migração ocorre, oferece previsão limitada sobre quando os acidentes ocorrerão.
- **Visibilidade das fronteiras:** na prática, as fronteiras de segurança raramente são visíveis aos atores, limitando a aplicabilidade direta do modelo.
- **Periferização dos elementos sociológicos:** Le Coze (2015, p. 133) argumenta que tanto a vertente "Elluliana" quanto a "Ashbyana" – esta última fundada pelo próprio Rasmussen – contêm tendências "associais". A matriz cibernético-funcionalista que estrutura a obra de Rasmussen, embora transdisciplinar em sua ambição, deixou em posição periférica os conceitos de poder, cultura, política e construção social do risco, mais centrais nas tradições derivadas de Turner, Vaughan e Weick.

2.3.7 Debates e Controvérsias

Os debates em torno da obra de Rasmussen não decorrem de sua irrelevância, mas precisamente, de sua influência. Ao propor que acidentes graves são preparados no funcionamento normal das organizações e não apenas desencadeados por falhas pontuais, Rasmussen tensiona pressupostos clássicos de causalidade

linear, previsibilidade e atribuição individual de culpa. Isso abriu um campo produtivo de controvérsias sobre o estatuto explicativo do modelo, o alcance do conceito de migração e os limites das ferramentas como o AcciMap para representar dinâmicas recursivas e fortemente interdependentes.

O primeiro debate envolve a tensão entre causalidade linear e não-linear: se acidentes são características dinâmicas de sistemas complexos, ignorar causalidades circulares pode ser problemático, embora a multiplicidade de eventos inter-relacionados desafie qualquer tentativa de previsão (Le Coze, 2015).

Le Coze (2015, p. 133, Fig. 7) distingue três linhas de interpretação da "normalidade" dos acidentes:

- **Linha "Elluliana" (Ellul → Perrow):** centrada na ideia de tecnologia que escapa ao controle; ênfase no acoplamento estreito e na complexidade técnica.
- **Linha "Kuhniana" (Kuhn → Turner → Vaughan, com Weick em ramo paralelo):** centrada em processos sociais de construção de sentido, normalização do desvio e colapso de sentido.
- **Linha "Ashbyana" (Ashby → Rasmussen → Snook → Hollnagel):** centrada em adaptação, auto-organização, graus de liberdade e migração gradual em direção às fronteiras de desempenho aceitável. Snook estende a linha por meio do conceito de *practical drift*, e Hollnagel, por meio das ideias de ressonância funcional e do *trade-off ETTO*.

Rasmussen (1994) propôs que as perspectivas de Acidentes Normais (NAT) e de Organizações de Alta Confiabilidade (HRT) são complementares, não competidoras – sua visão de migração organizacional às fronteiras oferece uma interpretação própria desse debate. Le Coze (2015) caracteriza o legado de Rasmussen como "um programa forte para um problema difícil": o desafio transdisciplinar de compreender e antecipar acidentes por meio de análise funcional que atravesse níveis e disciplinas.

O debate contemporâneo também envolve a suficiência do AcciMap para representar causalidades não lineares: embora a ferramenta seja valiosa para explicitar decisões distribuídas, autores posteriores observam que toda representação

em caixas e setas tende a simplificar circuitos de retroalimentação, acoplamentos dinâmicos e relações circulares características de sistemas complexos (Le Coze, 2015, pp. 134–135).

2.3.8 Desenvolvimentos Recentes

A contribuição de Rasmussen não se limitou ao estudo histórico de acidentes; foi incorporada e reelaborada em diferentes correntes da ciência da segurança contemporânea. Seu legado aparece tanto em abordagens voltadas ao projeto de sistemas e à engenharia de controle quanto em correntes que enfatizam variabilidade do desempenho, adaptação cotidiana, resiliência e deriva prática. Em comum, essas vertentes preservam a ideia central de que segurança não é simples ausência de erro, mas resultado da capacidade de manter o sistema dentro de envelopes operacionais aceitáveis, apesar de pressões competitivas, mudanças tecnológicas e objetivos conflitantes.

O modelo STAMP (*Systems-Theoretic Accident Model and Processes*), desenvolvido por Nancy Leveson, foi *"diretamente projetado sobre o modelo sociotécnico"* de Rasmussen (Le Coze, 2015, p. 138; Leveson, 2011, 2012), traduzindo a ênfase em controle, feedback e restrições para uma arquitetura de engenharia de sistemas e para métodos analíticos como o STPA. A metodologia AcciMap continua sendo aplicada em análises de acidentes em diversos setores, com refinamentos metodológicos e integrações com STAMP.

Amalberti (2001) articulou, no contexto de sistemas ultrasseguros (taxa de acidentes catastróficos próxima de 10^{-7}), os "paradoxos" que surgem quando estratégias incrementais de redução de risco passam a comprometer a própria capacidade adaptativa do sistema. Sua representação do espaço de ação operável – contido entre fronteiras de regulações, mercado e regras de segurança – e da migração operacional para regiões de violações e desvios remete diretamente ao modelo de Rasmussen (1997), oferecendo uma extensão para o caso de sistemas que já atingiram patamares muito elevados de segurança (Amalberti, 2001, p. 121, Fig. 2).

2.3.9 Implicações para a Indústria de Energia

Na indústria de energia, e em particular no setor de óleo e gás, a utilidade da perspectiva Rasmusseniana é acentuada pela presença simultânea de processos perigosos, barreiras técnicas complexas, múltiplas camadas decisórias e pressões persistentes por continuidade operacional, custo e prazo. Nesses contextos, a segurança depende menos da adesão literal a procedimentos isolados e mais da capacidade institucional de tornar visíveis os limites de operação, detectar deslocamentos graduais, preservar defesas críticas e alinhar decisões tomadas por operadores, supervisores, manutenção, engenharia, contratadas, gestores e reguladores. A abordagem oferece, portanto, base fértil para auditorias operacionais, investigação de eventos, gestão de interfaces e desenho de mecanismos de governança que impeçam a migração silenciosa do sistema para estados de maior risco.

Contribuições

- **Tornar fronteiras visíveis:** investir em sistemas de instrumentação e indicadores que tornem os limites de segurança perceptíveis aos operadores antes que sejam ultrapassados.
- **Contrabalançar gradientes:** gestores devem monitorar desempenho de segurança com a mesma intensidade que desempenho econômico, criando contragradientes que equilibrem as pressões migratórias (cf. Figura 2.3.1).
- **Comunicação sobre *trade-offs*:** evitar colocar operadores em situações de duplo vínculo nas quais a segurança é declarada como prioridade ou valor, mas mensagens tácitas comunicam o oposto.
- **Responsabilização multinível:** tomadores de decisão de alto nível devem ser responsabilizados pelos riscos sistêmicos associados às suas decisões.
- **Gestão de interfaces:** procedimentos devem destacar interfaces com outras atividades em que há potencial de conflito, especialmente em ambientes com presença simultânea de múltiplas contratadas e turnos sobrepostos (cf. Figura 2.3.2).

2.3.10 Quadro-Resumo: Perspectiva Rasmusseniana

Dimensão	Perspectiva Rasmusseniana (Objetivos Conflitantes)
Período de Surgimento	1990s (artigo seminal de 1997).
Principais Autores	Jens Rasmussen, Inge Svedung.
Fundamento Teórico	Cibernética, teoria de sistemas, teoria de controle, análise de decisão. Integração de engenharia cognitiva com análise organizacional.
Pressuposto Central	Atividades migram sistematicamente em direção às fronteiras de segurança sob pressão de gradientes de eficiência e menor esforço.
Concepção de Risco	Risco como problema de controle dinâmico — a segurança emerge do controle de processos dentro de limites aceitáveis, não da eliminação da variabilidade.
Visão da Contribuição Humana	Humanos como adaptadores racionais locais; as decisões fazem sentido no contexto, mesmo quando contribuem para a deriva sistêmica.
Estratégias de Controle	Tornar as fronteiras visíveis, contrabalançar gradientes de pressão, comunicar sobre trade-offs, responsabilizar os tomadores de decisão de alto nível.
Modelo de Causalidade	Acidentes emergem de migração gradual e adaptações locais que coletivamente empurram sistema para além das fronteiras de segurança.
Forças	Perspectiva sistêmica dinâmica; integra múltiplos níveis; reconhece *trade-offs*; oferece ferramentas analíticas (AcciMap).
Limitações	Complexidade conceitual; capacidade preditiva limitada; dificuldade prática de tornar fronteiras visíveis; periferização dos elementos sociológicos.

Nota: A perspectiva Rasmusseniana compartilha pontos de contato com as teorias de dependência de trajetória (Seção 2.5), particularmente no fenômeno de deriva. Enquanto Rasmussen oferece um modelo sistêmico de **como** a migração ocorre (gradientes, fronteiras), Vaughan e Snook oferecem análises sociológicas **de por que organizações normalizam desvios** ao longo do tempo. As perspectivas são complementares: Rasmussen fornece o mecanismo; a dependência de trajetória fornece o processo histórico-social.

Referências da Seção 2.3

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science, 37*(2–3), 109–126. https://doi.org/10.1016/S0925-7535(00)00045-X

Ashby, W. R. (1956). *An introduction to cybernetics*. Chapman & Hall.

Ashby, W. R. (1962). Principles of self-organization. In H. Von Foerster & G. W. Zopf Jr. (Eds.), *Principles of self-organization* (pp. 255–278). Pergamon Press.

Branford, K. (2007). *An investigation into the validity and reliability of the AcciMap approach* [Doctoral dissertation, Australian National University]. https://doi.org/10.25911/5d77873ea2940

Dekker, S. (2019). *Foundations of safety science: A century of understanding accidents and disasters*. Routledge/CRC.

Dekker, S., Cilliers, P., & Hofmeyr, J.-H. (2011). The complexity of failure: Implications of complexity theory for safety investigations. *Safety Science, 49*(6), 939–945. https://doi.org/10.1016/j.ssci.2011.01.008

Goode, N., Salmon, P. M., Taylor, N. Z., Lenné, M. G., & Finch, C. F. (2017). Developing a contributing factor classification scheme for Rasmussen's AcciMap: Reliability and validity evaluation. *Applied Ergonomics, 64*, 14–26. https://doi.org/10.1016/j.apergo.2017.05.004

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.

Le Coze, J. C. (2015). Reflecting on Jens Rasmussen's legacy: A strong program for a hard problem. *Safety Science, 71*, 123–141. https://doi.org/10.1016/j.ssci.2014.03.015

Leveson, N. G. (2011). Applying systems thinking to analyze and learn from events. *Safety Science, 49*(1), 55–64. https://doi.org/10.1016/j.ssci.2009.12.021

Leveson, N. G. (2012). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.

Rasmussen, J. (1979). Notes on human error analysis and prediction. In G. Apostolakis & G. Volta (Eds.), *Synthesis and analysis methods for safety and reliability studies*. Plenum Press.

Rasmussen, J. (1982). Human errors: A taxonomy for describing human malfunction in industrial installations. *Journal of Occupational Accidents, 4*(2–4), 311–333. https://doi.org/10.1016/0376-6349(82)90041-4

Rasmussen, J. (1990a). The role of error in organizing behaviour. *Ergonomics, 33*(10–11), 1185–1199. https://doi.org/10.1080/00140139008925325

Rasmussen, J. (1990b). Human error and the problem of causality in analysis of accidents. *Philosophical Transactions of the Royal Society of London, B, 327*, 449–462. https://doi.org/10.1098/rstb.1990.0088

Rasmussen, J. (1993). Deciding and doing: Decision making in natural contexts. In G. Klein, J. Orasanu, R. Calderwood, & C. E. Zsambok (Eds.), *Decision making in action: Models and methods* (pp. 158–171). Ablex.

Rasmussen, J. (1994). Risk management, adaptation, and design for safety. In N. E. Sahlin & B. Brehmer (Eds.), *Future risks and risk management* (pp. 1–36). Kluwer Academic.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Rasmussen, J., & Batstone, R. (1989). *Why do complex organisational systems fail?* (Environment Working Paper No. 20). World Bank.

Rasmussen, J., & Jensen, A. (1974). Mental procedures in real-life tasks: A case study of electronic trouble shooting. *Ergonomics, 17*(3), 293–307. https://doi.org/10.1080/00140137408931355

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in a dynamic society*. Swedish Rescue Services Agency.

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærø, I. (2010). *Organisational accidents and resilient organisations: Six perspectives* (Report SINTEF A17034, Revision 2). SINTEF Technology and Society.

Salmon, P. M., Hulme, A., Walker, G. H., Waterson, P., Berber, E., & Stanton, N. A. (2020). The big picture on accident causation: A review, synthesis and meta-analysis of AcciMap studies. *Safety Science, 126*, 104650. https://doi.org/10.1016/j.ssci.2020.104650

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of U.S. Black Hawks over Northern Iraq*. Princeton University Press.

Tabibzadeh, M., Shafieezadeh, A., & Mokhtari, K. (2019). A systematic framework for root cause analysis of the Aban Plasco building collapse in Iran: Lessons learned from a high-impact incident. *Process Safety Progress, 38*(4), e12046. https://doi.org/10.1002/prs.12046

Vicente, K. J. (2004). *The human factor: Revolutionizing the way people live with technology*. Routledge.

2.4 Engenharia de Resiliência (RE)

Autores: Louize Dan, Guilherme Areias e Thais Santos

Revisão e Figuras: Rafael Ceni de Almeida

2.4.1 Introdução e Contexto Histórico

A Engenharia de Resiliência (Resilience Engineering – RE) emergiu formalmente em 2004, durante um simpósio realizado em Söderköping, na Suécia, no qual pesquisadores e especialistas se reuniram para discutir novas formas de compreender e gerenciar a segurança em sistemas sociotécnicos complexos. Como produto desse encontro, foi publicado o livro *Resilience Engineering: Concepts and Precepts* (Hollnagel, Woods, & Leveson, 2006), reconhecido como o marco fundacional do campo. O termo, porém, já havia sido usado por David Woods em 2003, em depoimento ao Senado norte-americano após o acidente do ônibus espacial Columbia, ao mostrar como a pressão por produção sintetizada no lema Faster, Better, Cheaper da NASA tornara o sistema progressivamente frágil (Woods, 2003; CAIB, 2003).

Os principais arquitetos teóricos da Engenharia de Resiliência são **Erik Hollnagel**, que desenvolveu os quatro potenciais, o *Functional Resonance Analysis Method (FRAM)* e o princípio *Efficiency-Thoroughness Trade-Off (ETTO)*; **David D. Woods**, que formulou os conceitos de extensibilidade graciosa e adaptabilidade sustentada; e **Nancy Leveson**, que contribuiu com a engenharia de sistemas e o modelo *Systems-Theoretic Accident Model and Processes (STAMP)*. As raízes do campo remontam à comunidade científica do *Risø National Laboratory*, na Dinamarca, onde, ao longo das décadas de 1980 e 1990, Jens Rasmussen, Hollnagel e Woods colaboraram no desenvolvimento da Engenharia de Sistemas Cognitivos, articulando uma compreensão dos acidentes como resultados de interações complexas entre níveis técnicos, humanos e organizacionais, sob pressões econômicas e operacionais (Bergström & Dekker, 2019).



Como sintetiza Hollnagel (2008), "a engenharia de resiliência difere mais na perspectiva que oferece sobre segurança do que nos métodos e abordagens práticas" (p. xi). Não se trata, portanto, de uma "nova engenharia". O termo designa, antes, a dimensão de projeto e gestão da abordagem: compreender, projetar e gerenciar sistemas sociotécnicos complexos de modo que considerem suporte às adaptações recorrentes pelo trabalho real (Bergström, van Winsen, & Henriqson, 2015). Isso vale tanto para as atividades da linha de frente (micro) quanto para as decisões organizacionais, as escolhas tecnológicas, a regulação e as políticas setoriais (macro). Já o termo de resiliência, originário da física dos materiais, onde indica o retorno à forma original após uma deformação, e depois de proteção pela ecologia e pela psicologia, deixa aqui de ser atributo de um componente isolado. A unidade de análise é sempre o sistema sociotécnico, e não, de forma isolada, o indivíduo, o equipamento ou o procedimento. Tal perspectiva não emergiu isoladamente: articula-se a quatro correntes teóricas anteriores que estruturaram sua fundamentação.

Ciência da complexidade. Reconhece que os sistemas sociotécnicos são dinâmicos, não lineares e formados por múltiplas interações interdependentes, nos quais o desempenho emerge da interação entre componentes humanos, técnicos e organizacionais, e não do funcionamento isolado de suas partes. Nessa perspectiva, tanto os sucessos quanto os eventos adversos são compreendidos como fenômenos emergentes, não plenamente explicáveis por cadeias simples de causa e efeito (Hollnagel et al., 2006).

Teoria de sistemas adaptativos. Parte do entendimento de que sistemas complexos não operam de forma estática ou plenamente previsível, mas dependem de processos contínuos de adaptação para lidar com variações, incertezas e pressões do ambiente. O desempenho humano e organizacional é inerentemente variável, e essa variabilidade não é interpretada como desvio indesejável, mas como condição necessária para que o sistema opere de forma eficaz em contextos parcialmente imprevisíveis (Hollnagel & Woods, 2005).

Engenharia de sistemas cognitivos. Desenvolvida por Hollnagel e Woods a partir da década de 1980, introduz o conceito de sistema cognitivo conjunto (*joint cognitive system*), no qual pessoas, tecnologias, procedimentos e organizações são tratados como uma unidade funcional integrada. O foco desloca-se da análise de

erros humanos para a compreensão de como o sistema percebe, interpreta, decide, antecipa e responde às demandas do ambiente (Hollnagel & Woods, 2005).

Comunidade Risø. Refere-se ao grupo de pesquisa associado ao *Risø National Laboratory*, cujos trabalhos, a partir da década de 1980, exerceram influência fundamental sobre a posterior Engenharia de Resiliência. Rasmussen, Hollnagel e Woods romperam com abordagens centradas na "falha humana" ao propor modelos sistêmicos de acidentes e ao introduzir conceitos como comportamento adaptativo, limites de operação segura e a importância de compreender o trabalho real (Bergström & Dekker, 2019; Hollnagel et al., 2006).

A partir desse conjunto de influências históricas e teóricas, a Engenharia de Resiliência estruturou-se sobre pressupostos que orientam a forma como o desempenho, a variabilidade e a adaptação são compreendidas no contexto da gestão da segurança em sistemas sociotécnicos complexos.

2.4.2 Pressupostos Críticos

O pressuposto central da Engenharia de Resiliência é a adoção de uma perspectiva distinta sobre o conceito de segurança, em contraposição à concepção tradicional que tende a defini-la a partir dos acidentes e falhas que ocorreram. A Engenharia de Resiliência propõe deslocar o foco para aquilo que, na maior parte do tempo, funciona adequadamente nos sistemas. Como sintetiza Hollnagel (2006):

> *"A segurança é a soma dos acidentes que não ocorrem. Enquanto a pesquisa sobre acidentes tem se concentrado nos acidentes que ocorreram e buscado entender por quê, a pesquisa em segurança deveria se concentrar nos acidentes que não ocorreram e tentar compreender por quê." (Hollnagel, 2006, p. 9)*

Essa abordagem constitui crítica aos modelos tradicionais de gestão da segurança, geralmente dominados por uma visão retrospectiva, orientada à prevenção de falhas passadas, e que tendem a desconsiderar as variabilidades presentes em sistemas sociotécnicos complexos, bem como a capacidade de adaptação dos processos e das pessoas. A Engenharia de Resiliência apresenta um conceito de gestão da

segurança que se concentra em compreender e apoiar a capacidade das pessoas em lidar com a complexidade e operar sob pressão para alcançar o sucesso.

Para tanto, articula três conceitos basilares: (1) a compreensão da falha como parte do funcionamento normal do sistema; (2) a necessidade de adaptação contínua; e (3) o reconhecimento da complexidade e das interações entre os diferentes componentes do sistema (Hollnagel, 2014). Nessa perspectiva, "a segurança é criada por meio de processos resilientes e proativos, em vez de barreiras e defesas reativas" (Hollnagel & Woods, 2005, p. 6).

Estudos sobre as bases do trabalho técnico demonstram que os trabalhadores atuam continuamente para antecipar situações que podem conduzir ao fracasso, desenvolvendo e sustentando estratégias sensíveis às falhas e buscando manter margens operacionais diante das constantes pressões por produtividade e rapidez. Realizar o trabalho de forma segura sempre foi – e continua sendo – parte integrante das práticas operacionais cotidianas (Woods & Cook, 2002).

Outro elemento central é o reconhecimento de que o trabalho imaginado – descrito em normas, procedimentos e planejamentos – difere do trabalho real, tal como é efetivamente realizado no contexto operacional. Esse desvio não é entendido como anomalia ou exceção, mas como fenômeno normal, que pode resultar tanto em falhas quanto em sucessos. Sistemas sociotécnicos complexos só funcionam porque pessoas e organizações se ajustam continuamente às condições variáveis do ambiente. Falhas, nessa perspectiva, não ocorrem simplesmente porque houve um desvio em relação ao trabalho imaginado, mas porque os mesmos ajustes que normalmente produzem sucesso deixam de ser suficientes em determinado contexto. O problema, portanto, não está na falha em si, mas no descompasso entre os ajustes realizados e as demandas específicas do contexto.

Para a Engenharia de Resiliência, torna-se essencial monitorar e aprender com a lacuna entre o trabalho real e o trabalho imaginado. A compreensão dos fatores que produzem essa lacuna pode impulsionar a aprendizagem organizacional e a melhoria contínua, reduzindo a dependência de soluções improvisadas ou da conformidade acrítica com políticas e procedimentos distantes da realidade operacional.

Quanto à contribuição humana, a Engenharia de Resiliência entende o indivíduo

não como fonte de erro a ser controlada, mas como fonte essencial de adaptação e resiliência, cuja flexibilidade permite compensar limitações de projetos, tecnologias e processos. Esses ajustes não podem ser totalmente pré-programados nem incorporados aos sistemas, dado que é inviável antecipar todas as situações possíveis no ambiente operacional.

Em contraposição às explicações excessivamente simplificadas – que tratam os sistemas a partir de recortes estáticos, buscam fatores separáveis ou modelam acidentes como cadeias lineares –, a perspectiva propõe uma abordagem sistêmica baseada em cinco pressupostos distintivos:

- **Intratabilidade dos sistemas complexos:** sistemas sociotécnicos complexos são parcialmente intratáveis e subespecificados – seus princípios de funcionamento são apenas parcialmente conhecidos, e o sistema muda enquanto é descrito – e seu desempenho é sempre variável, em função tanto da variabilidade do ambiente quanto da variabilidade dos subsistemas que os constituem. Como consequência, os resultados das ações podem diferir do pretendido, esperado ou requerido, mesmo quando as pessoas atuam de maneira competente e responsável (Bergström & Dekker, 2019).
- **Variabilidade como normalidade:** o desempenho normal e as falhas são compreendidos como fenômenos emergentes, resultantes da interação entre diferentes elementos do sistema. A Engenharia de Resiliência reconhece a existência da variabilidade e enfatiza sua necessidade para que o sistema cognitivo conjunto consiga lidar com a complexidade do mundo real. A adaptabilidade e a flexibilidade do trabalho humano constituem a principal razão da eficiência dos sistemas sociotécnicos (Hollnagel, 2008; Hollnagel & Woods, 2005).
- **Sucesso e falha têm a mesma origem:** falhas não são interpretadas como resultado de disfunções isoladas ou excepcionais, mas como manifestações do mesmo conjunto de mecanismos adaptativos que, normalmente, produzem resultados bem-sucedidos. Tanto acidentes quanto sucessos emergem da variabilidade e não podem ser plenamente explicados pelo funcionamento – ou mau funcionamento – de componentes isolados (Patriarca et al., 2021).
- **Trabalho-como-realizado (WAD) versus trabalho-como-imaginado**

(WAI): existe lacuna inevitável entre o trabalho descrito em procedimentos (*Work-as-Imagined*) e o trabalho efetivamente realizado em contextos complexos (*Work-as-Done*). Sob essa perspectiva, o desempenho confiável dos sistemas existe não porque foram projetados de forma perfeita ou porque as pessoas fazem exatamente o prescrito, mas porque as pessoas são flexíveis e adaptáveis. A gestão da segurança deve estar alinhada ao trabalho realizado, e não depender exclusivamente do trabalho imaginado (Hollnagel & Woods, 2005).

- **Segurança integrada ao negócio:** a segurança não pode ser isolada do processo produtivo central, nem vice-versa uma é pré-requisito da outra. Deve, portanto, ser alcançada pela melhoria dos processos do negócio, e não pela sua restrição, por meio de uma gestão ao mesmo tempo proativa e reativa (Hollnagel, Tveiten & Albrechtsen, 2010).

A partir desses pressupostos, a Engenharia de Resiliência desenvolve um conjunto de conceitos fundamentais que estruturam essa perspectiva e possibilitam sua aplicação por meio de modelos e ferramentas aplicáveis aos sistemas sociotécnicos complexos.

2.4.3 Conceitos Fundamentais

Hollnagel (2006) definiu inicialmente resiliência como "a capacidade de um sistema ou de uma organização de reagir e se recuperar de perturbações em um estágio inicial, com efeito mínimo sobre a estabilidade dinâmica" (p. 16). Formulações posteriores ampliaram o conceito: resiliência passa a ser a capacidade de um sistema de ajustar seu funcionamento antes, durante ou após mudanças, perturbações e oportunidades, de modo a sustentar as operações necessárias sob condições esperadas e inesperadas (Nemeth & Hollnagel, 2022). A Engenharia de Resiliência vai além do conceito clássico de resiliência ao considerar três deslocamentos: (1) a capacidade de absorver e se adaptar, e não apenas absorver sem mudança; (2) a flexibilidade para continuar operando sob novas condições, em vez de simplesmente retornar ao estado anterior; e (3) a adaptabilidade como competência organizacional dinâmica, e não como propriedade fixa ou processo predefinido.

Essa concepção distingue a resiliência de duas noções próximas: a **robustez**, que suporta perturbações conhecidas até certo limite, e a **confiabilidade**, estimada

a partir de condições definidas a priori a descrição da atividade e um "operador médio" que a executa (Marques et al., 2025). Um sistema pode, assim, ser confiável e, ainda assim, frágil e sujeito a um colapso abrupto (*brittleness*) diante do inesperado (Woods, 2015). A resiliência não substitui a confiabilidade, a robustez nem a análise de confiabilidade humana (Seção 3.4): complementa-as naquilo que escapa aos cenários previstos, sem dispensar a redução de precariedades e falhas conhecidas.

Nessa perspectiva, a Engenharia de Resiliência busca identificar e fortalecer as capacidades positivas das pessoas e das organizações que lhes permitem se adaptar de maneira eficaz e segura diante de circunstâncias variadas. O foco desloca-se da eliminação isolada de falhas para a compreensão e o fortalecimento das condições que sustentam o desempenho bem-sucedido ao longo do tempo (Bergström & Dekker, 2019).

Considerando que se atua em sistemas sociotécnicos complexos, torna-se necessário ir além da análise de modos de falha de componentes individuais e adotar uma visão funcional que compreenda as interdependências entre funções. Esses sistemas não são inerentemente seguros: precisam operar sob pressão competitiva, atender simultaneamente a múltiplos objetivos – muitas vezes conflitantes – e fazê-lo com recursos limitados. Sob essas circunstâncias dinâmicas, pessoas e organizações precisam criar segurança por meio de ajustes e adaptações no trabalho cotidiano (Bergström & Dekker, 2019; Hollnagel et al., 2006).

Quatro conjuntos de conceitos fundamentais estruturam o campo e são apresentados a seguir: (a) a distinção entre Safety-I e Safety-II, que redefine a forma de compreender a segurança; (b) os quatro potenciais de Hollnagel, que descrevem as capacidades necessárias para sustentar o desempenho; (c) os quatro modelos de resiliência de Woods, que organizam diferentes acepções do termo; e (d) o conjunto de ferramentas – FRAM, RAG e ETTO – que possibilitam operacionalizar essa perspectiva na gestão da segurança.

Safety-I e *Safety-II*

Hollnagel (2014) distingue duas abordagens para compreender e gerenciar a segurança. O ***Safety-I*** define segurança como ausência de eventos indesejados e

concentra seus esforços na prevenção daquilo que dá errado. O ***Safety-II***, por sua vez, define segurança como a condição na qual o número de resultados aceitáveis é o mais alto possível, direcionando o foco para assegurar que as coisas deem certo. A Tabela 2.4.1 sintetiza as principais diferenças entre as duas abordagens.

Tabela 2.4.1 — Principais diferenças entre Safety-I e Safety-II

Dimensão	*Safety-I*	*Safety-II*
Conceito de segurança	Ausência de acidentes, incidentes ou danos inaceitáveis.	Capacidade de ter sucesso sob condições variáveis.
Foco	O que deu errado; reduzir resultados negativos.	O que dá certo; maximizar resultados desejados.
Objetivo	Prevenir eventos adversos ou reconhecer riscos (resultados adversos potenciais).	Garantir que o trabalho cotidiano produza os resultados esperados.
Análise de acidentes	Resultam de falhas ou disfunções; identificar as causas e eliminá-las ou introduzir barreiras.	Resultam de variabilidades; compreender por que as coisas geralmente dão certo.
Visão sobre a gestão	Reativa – responder após falhas ou eventos indesejados.	Proativa – antecipar continuamente eventos e condições.
Visão sobre as pessoas	Fonte de erro; risco a ser controlado; problema a ser resolvido.	Fonte de adaptação, flexibilidade e eficiência; fonte de solução.
Visão sobre procedimentos	Prescrição e conformidade são centrais.	Procedimentos são recursos para apoiar o desempenho.
Gerenciamento de riscos	Identificar perigos e fortalecer barreiras.	Compreender as condições que tornam o trabalho difícil.

Nota. Adaptado de Hollnagel (2014) e Hollnagel, Wears e Braithwaite (2015).

Vale destacar, contudo, que não se trata de **Safety-I ou Safety-II**, mas de **Safety-I e Safety-II**. O Safety-I continua relevante para lidar com perigos conhecidos e

cenários estáveis e previsíveis, enquanto o Safety-II torna-se essencial quando os sistemas operam sob condições de complexidade, variabilidade e incerteza (Hollnagel, Wears, & Braithwaite, 2015). Conceitual e temporalmente distintas, as **duas perspectivas são complementares e igualmente necessárias** à construção de um trabalho ao mesmo tempo produtivo e seguro: a Engenharia de Resiliência não propõe abandonar o Safety-I, mas ampliá-lo com o Safety-II aprendendo tanto com os resultados indesejados quanto com a variabilidade do trabalho cotidiano que produz sucesso.

ATUALIZAÇÃO TERMINOLÓGICA (Hollnagel & Slater, 2026)

Em manifesto recente, Hollnagel propõe ***aposentar os rótulos Safety-I e Safety-II*** *que nomeiam a diferença sem descrevê-la e substituí-los por* **Segurança Decremental** *e* **Segurança Incremental***, termos cujos nomes já explicitam a estratégia de cada abordagem. A segurança decremental procura reduzir os resultados inesperados e inaceitáveis (a ausência de segurança), mantendo-os tão baixos quanto razoavelmente praticável (ALARP) – um custo reativo, que aprende de eventos raros e adiciona barreiras; a* **segurança incremental** *procura aumentar os resultados esperados e aceitáveis (a presença de segurança) – um investimento, produtivo, que aprende do trabalho cotidiano que dá certo ("dynamic non-events" de Weick). Não se trata de definições concorrentes, mas de caminhos alternativos para o mesmo resultado, o que reforça o ponto anterior: decremental e incremental. Nessa leitura, a Engenharia de Resiliência fornece as capacidades que sustentam a abordagem incremental, apresentadas a seguir neste compêndio (Hollnagel, 2025, 2026).*

Safety-I

O Safety-I baseia-se em uma visão de segurança desenvolvida aproximadamente ao longo das décadas de 1960 a 1980 no contexto da segurança industrial, quando os sistemas eram relativamente simples se comparados aos atuais. A dependência de tecnologias da informação era limitada, e as funções de suporte eram, em geral, escassas, simples e principalmente independentes entre si. O nível de inte-

gração entre subsistemas e setores era baixo e, na maioria dos casos, era possível compreender e acompanhar o que acontecia no sistema.

A concepção de segurança associada ao Safety-I desenvolveu-se com base nos seguintes pressupostos: (a) os sistemas e locais de trabalho são adequadamente projetados e mantidos; (b) os procedimentos são abrangentes, completos e corretos; (c) as pessoas comportam-se conforme o esperado e de acordo com o treinamento recebido; e (d) os projetistas conseguem prever todas as contingências relevantes e capacitam o sistema com recursos de resposta apropriados. Embora esses pressupostos nunca tenham sido plenamente válidos, eram considerados razoáveis no contexto industrial da década de 1970, mas tornaram-se inadequados para a realidade contemporânea (Hollnagel, 2014). Uma limitação central é o fato de o Safety-I não considerar o motivo pelo qual o desempenho humano, na maior parte do tempo, dá certo.

Safety-II

O Safety-II adota uma abordagem que reconhece os sistemas sociotécnicos complexos como característicos da realidade da indústria contemporânea. Nesses sistemas, pessoas e organizações precisam atuar de forma a lidar com a variabilidade presente no trabalho cotidiano. Nessa perspectiva, a variabilidade do desempenho não deve ser interpretada negativamente – como "não conformidade", "violação" ou "falta de adesão ao procedimento" – mas como fonte de solução adaptável.

As pessoas não são vistas como problema a ser resolvido ou padronizado, mas como fonte essencial de adaptação. Na prática, ajustam continuamente a forma como executam o trabalho às condições reais de operação, corrigindo falhas nos processos e criando segurança. Esses ajustes constituem uma contribuição humana essencial, sem a qual apenas as atividades mais triviais poderiam ser realizadas de forma segura e eficaz. Tentar alcançar a segurança por meio da restrição da variabilidade do desempenho afeta inevitavelmente a capacidade de atingir resultados desejados e revela-se uma estratégia contraproducente (Hollnagel, 2014).

A concepção de segurança associada ao Safety-II desenvolveu-se com base nos seguintes pressupostos: (a) os sistemas não podem ser decompostos, pois não

existem "elementos" ou "componentes" independentes; (b) as funções de um sistema não são separadas em "funcionais" e "disfuncionais" – o desempenho cotidiano é, e deve ser, flexível e variável; (c) os resultados surgem da variabilidade do desempenho humano, que constitui a origem tanto dos resultados aceitáveis quanto dos adversos; e (d) embora alguns resultados adversos possam ser atribuídos a falhas ou defeitos, são mais bem compreendidos como resultado de combinações da variabilidade no desempenho.

Os Quatro Potenciais da Resiliência

Hollnagel (2008) identificou quatro capacidades essenciais para que as organizações desenvolvam resiliência, que lhes permitem evitar que algo indesejado aconteça, impedir que um evento adverso se agrave e recuperar-se após sua ocorrência. A terminologia desses quatro elementos evoluiu ao longo do tempo: inicialmente denominados "quatro habilidades" (*four abilities*) em Hollnagel (2008), passaram a "quatro pilares" (*cornerstones*) em Hollnagel, Nemeth e Dekker (2009), depois a "capacidades" (*capabilities*) (Bergström & Dekker, 2019) e, mais recentemente, a "potenciais" (Hollnagel, 2018) e "potenciais sistêmicos" (Hollnagel, 2025). A mudança não é apenas de nome: "potencial" enfatiza algo que a organização exerce e precisa sustentar, e não um atributo que possui de forma permanente. A formulação original de Hollnagel (2008, p. xii) sintetiza-os em quatro habilidades essenciais:

1. **Responder** *(the ability to respond to the actual):* saber o que fazer – capacidade de lidar com eventos regulares e irregulares de forma efetiva, ajustando as respostas preparadas às condições reais e mantendo a continuidade das operações.
2. **Monitorar** *(the ability to flexibly monitor the critical):* saber o que observar – manter vigilância sobre ameaças potenciais e indicadores de desempenho do sistema e do ambiente operacional revendo periodicamente o que se monitora para não ficar preso à rotina.
3. **Antecipar** *(the ability to anticipate the potential):* saber o que esperar – preparar-se para desenvolvimentos futuros, possíveis surpresas e demandas emergentes inclusive no médio e no longo prazo.
4. **Aprender** *(the ability to learn from the factual):* saber o que aconteceu – extrair lições de experiências passadas, tanto de sucessos quanto de falhas,

e atualizar conhecimentos, competências e recursos – o que se materializa em mudanças de procedimentos, de papéis ou de prática de organização.



Hollnagel (2008) vincula essas habilidades aos três tipos de ameaça propostos por Westrum (2006): a ameaça regular, a ameaça irregular e o evento sem precedentes (unexampled event). A capacidade de responder lida com a ameaça regular, ao passo que a capacidade de antecipar dirige-se à ameaça irregular. A Figura 2.4.1 ilustra essas qualidades, mostrando que as capacidades não se relacionam de forma linear – embora possa haver sequência em situações específicas, o aspecto central da resiliência reside em sua exercitação contínua e simultânea (Hollnagel et al., 2006).

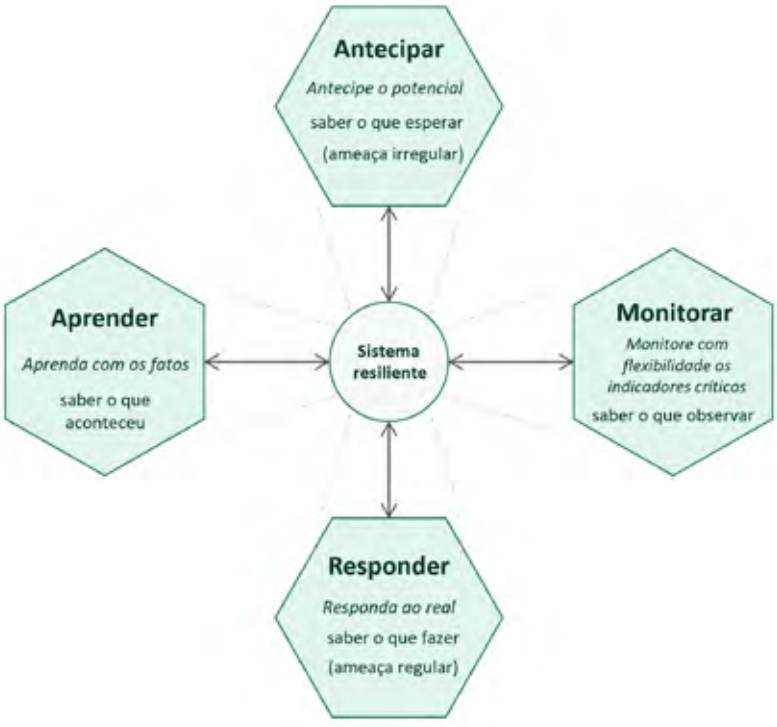


Figura 2.4.1: Qualidades requeridas de um sistema resiliente. *Adaptado de Hollnagel (2006, p. 350), com inclusão do potencial "aprender" conforme Hollnagel (2008, p. xii) e vinculação aos tipos de ameaça de Westrum (2006).*

Os quatro potenciais devem ser desenvolvidos de forma integrada: tornar-se resiliente é um processo contínuo, e não um estado a ser atingido, e consiste em manter entre eles um equilíbrio apropriado ao tipo de atividade e de situação (Hollnagel, 2018). Para a indústria de energia, fortalecer essas capacidades significa investir não apenas em tecnologia, mas também em processos organizacionais, liderança, treinamento e cultura que sustentem a adaptação segura ao longo do tempo.

Os Quatro Modelos de Resiliência de Woods (2015)

Paralelamente à formulação de Hollnagel, Woods (2015) organizou os usos do termo resiliência na literatura em quatro concepções distintas, das quais defende que a Engenharia de Resiliência deve adotar especialmente a terceira e a quarta (Bergström & Dekker, 2019).

1. **Resiliência como retorno** *(rebound):* recuperação para um estado anterior. Woods utiliza esse modelo como ponto de partida retórico para argumentar como a Engenharia de Resiliência se diferencia. Suas limitações incluem a preocupação com um estado anterior estável – "após um evento disruptivo, não há um passado estável ao qual retornar, pois o próprio evento altera o sistema" – e o paradoxo de tratar eventos disruptivos como surpresas fundamentais enquanto se aprende apenas com eventos passados (Woods, 2015).
2. **Resiliência como robustez** *(robustness):* capacidade de absorver – e não recuperar-se de – perturbações bem modeladas. Woods (2015, p. 6) adverte que "*a resiliência torna-se evidente quando o conjunto de perturbações não é bem modelado... confundir resiliência com robustez revela-se um erro*". Robustez funciona para distúrbios conhecidos, mas a resiliência diz respeito aos distúrbios não modelados.
3. **Resiliência como extensibilidade graciosa** *(graceful extensibility):* a pergunta central deixa de ser "como sistemas retornam?" e torna-se "como sistemas se esticam (adaptam) para lidar com surpresas?" (Woods, 2015, p. 7). Diferentemente da degradação graciosa, que se refere apenas a quebras, a extensibilidade graciosa pode ser positiva e levar ao sucesso. Woods propõe os termos descompensação (decompensation)

para o esgotamento das capacidades adaptativas, e antecipação para sua manutenção.

4. **Resiliência como adaptabilidade sustentada** *(sustained adaptability):* capacidade de manter a adaptabilidade ao longo do tempo. Woods (2015, p. 8) propõe três questões centrais para essa agenda: (a) que características de governança explicam diferenças entre redes que produzem adaptabilidade sustentada e aquelas que falham?; (b) que princípios de design permitiriam engenheirar tal capacidade?; (c) como saber se houve sucesso?

Esses quatro modelos não são alternativas excludentes, mas sim camadas conceituais. A Engenharia de Resiliência, na agenda de Woods, dedica-se especialmente a estudar a extensibilidade graciosa e a adaptabilidade sustentada, o que tem orientado sua atuação recente em domínios como tecnologia da informação, software e DevOps (Bergström & Dekker, 2019). Na indústria de óleo e gás, em que nenhuma operação é conduzida por uma única organização, essa agenda tem tradução direta: as questões de governança de redes formuladas por Woods (2015) aplicam-se à cadeia formada por operadora, contratadas, subcontratadas e regulador, cujas condições de contorno são definidas em grande parte por contratos e regulamentos (ver Seção 4.7.1).



Ferramentas (FRAM, RAG e ETTO)

Functional Resonance Analysis Method (FRAM)

O FRAM (Hollnagel, 2012) é uma metodologia para modelar sistemas sociotécnicos complexos em termos de funções e suas variabilidades. Em contraste com métodos tradicionais que buscam causas de falhas, o FRAM modela como funções interagem e como suas variabilidades podem se combinar – "ressonar" – para produzir tanto resultados desejados quanto indesejados. É uma ferramenta que pode ser empregada tanto retrospectivamente, para compreender como um evento ocorreu, quanto prospectivamente, para antecipar como variabilidades podem se combinar.

O método assume que os sistemas sociotécnicos podem ser observados a partir de quatro princípios:

- **Equivalência entre sucessos e falhas:** não há diferença no processo entre aquilo que dá certo e aquilo que dá errado; ambos emergem da mesma variabilidade do desempenho.
- **Ajustes aproximados:** em sistemas sociotécnicos complexos, a predefinição de todos os parâmetros é utópica; os elementos do sistema atuam sempre a partir de ajustes aproximados para cumprir suas funções.
- **Saídas emergentes:** o resultado de um sistema complexo não pode ser explicado pela soma de suas partes em relação linear de causa e efeito; ele emerge da interação entre as funções em diversos momentos.
- **Ressonância funcional:** pequenas variações nas diferentes funções interagem de forma combinada, gerando saídas emergentes que se propagam e amplificam ao longo da cadeia, podendo produzir resultados imprevisíveis.

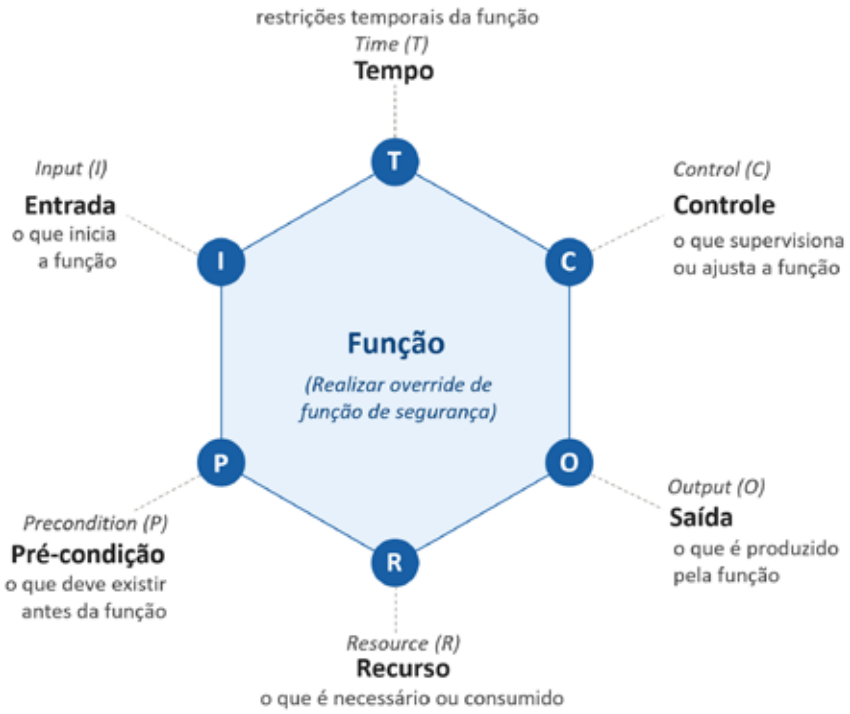


Figura 2.4.2: Hexágono FRAM com os seis aspectos da função. *Adaptado de Hollnagel (2012) e Patriarca et al. (2021, p. 486).*

Resilience Analysis Grid (RAG)

O RAG, proposto por Hollnagel (2011), é um método destinado à análise da capacidade de resiliência organizacional em sistemas sociotécnicos complexos, baseado na avaliação das quatro capacidades fundamentais – antecipar, monitorar, responder e aprender. Alinhado aos fundamentos da Engenharia de Resiliência e do Safety-II, o RAG apresenta um contraponto ao Safety-I ao adotar quatro deslocamentos: foco na capacidade do sistema de funcionar e se manter, e não em falhas; avaliação proativa em vez de análise reativa; consideração da complexidade das interações entre os elementos do sistema, em vez de causalidade linear; e avaliação da capacidade de adaptação em vez de conformidade.

O método utiliza um conjunto estruturado de questões para apresentar o perfil de resiliência do sistema, permitindo identificar fortalezas e lacunas (Hollnagel, 2011). As questões são formuladas a partir de cada um dos quatro potenciais, contemplando, por exemplo: a identificação de riscos emergentes (antecipar), a

observação de sinais de vulnerabilidade (monitorar), a existência de mecanismos para lidar com eventos inesperados (responder) e os processos de aprendizagem com eventos adversos e operações normais (aprender).

Cabe registrar uma ressalva metodológica importante: o gráfico em estrela tradicional do RAG não apresenta uma medida de resiliência per se; constitui, antes, um instantâneo qualitativo de como as capacidades de resiliência foram avaliadas em determinado momento no tempo (Patriarca et al., 2021). Trata-se de uma ferramenta de diagnóstico e diálogo organizacional, não de métrica objetiva. Seu valor cresce com o uso longitudinal: reaplicado com as mesmas perguntas e o mesmo grupo de respondentes, permite acompanhar a evolução dos potenciais (Hollnagel, 2018). O método tampouco define um limiar de "resiliência"; cabe à organização decidir o que aprimorar (Ljungberg & Lundh, 2013). Um dos principais desafios para sua aplicação mais ampla está na padronização, dado o componente subjetivo da avaliação. Aplicações recentes enfrentam esse desafio ancorando a avaliação na observação do trabalho cotidiano e nas práticas que sustentam cada potencial, o que revela também o que já funciona e pode ser fortalecido (Trancoso, Patriarca, & Henriqson, 2024).

Princípio *ETTO (Efficiency-Thoroughness Trade-Off)*

O princípio ETTO, proposto por Hollnagel (2009), formaliza o trade-off inevitável entre eficiência e minuciosidade, descrevendo como o desempenho humano e organizacional se adapta às condições reais de trabalho. Indivíduos e organizações precisam equilibrar continuamente eficiência e minuciosidade, dado que não é possível maximizar ambas simultaneamente. Eficiência associa-se à otimização de recursos, tempo e esforço; minuciosidade refere-se à execução cuidadosa, completa e aderente a regras e procedimentos.

O ETTO descreve um trade-off contínuo, inerente aos sistemas sociotécnicos complexos, no qual as decisões operacionais são influenciadas por restrições de tempo, metas de produtividade e limitações de recursos. Ajustes orientados à eficiência, embora necessários para o funcionamento do sistema, podem implicar a redução de margens de segurança. Em sua aplicação, o ETTO permite compreender decisões operacionais reais e identificar como pressões organizacio-

nais favorecem escolhas orientadas à eficiência em detrimento da minuciosidade, sobretudo em ambientes com elevada demanda por produtividade. Pode ser empregado na análise de acidentes – evidenciando que desvios e simplificações operacionais frequentemente representam adaptações racionais às condições de trabalho, e não falhas individuais isoladas – e também de forma prospectiva, apoiando a identificação de situações nas quais o equilíbrio entre eficiência e minuciosidade se torna crítico.

2.4.4 Base Empírica

A Engenharia de Resiliência desenvolveu-se por meio de estudos em diversos domínios sociotécnicos complexos, incluindo aviação, saúde, indústria nuclear, operações militares, sistemas marítimos e, mais recentemente, infraestrutura digital. Todos esses domínios compartilham complexidade elevada e a possibilidade de que eventos indesejados produzam consequências severas (Patriarca et al., 2021).

A aplicação na saúde tem sido particularmente produtiva, com a formação do *Resilient Healthcare Network* e múltiplas publicações sobre como princípios de resiliência podem melhorar a segurança do paciente. A área é especialmente sensível à abordagem, dada sua alta complexidade e variabilidade: cada paciente é único, o corpo humano pode reagir de forma distinta em cenários aparentemente idênticos, e o componente organizacional amplia a complexidade do sistema.

Woods e colaboradores desenvolveram estudos extensivos sobre capacidade adaptativa em operações de software e DevOps, examinando como engenheiros e Site *Reliability Engineers (SREs)* gerenciam a disponibilidade de sistemas críticos sob condições de incerteza e mudança contínua. Essa frente de pesquisa ampliou empiricamente os conceitos de extensibilidade graciosa e adaptabilidade sustentada, sustentando o argumento de que a resiliência em ambientes digitais não reside apenas na robustez do código ou na automação redundante, mas na capacidade humana de intervir e estender o alcance dos sistemas quando estes atingem os limites previstos (Bergström & Dekker, 2019). Desse programa resultou a teoria da extensibilidade graciosa, que descreve como a capacidade adaptativa é construída, sustentada, degradada e, eventualmente, perdida (Woods, 2018).

A convergência dessas evidências em domínios aparentemente distintos sustenta um insight comum: a segurança e a continuidade operacional não emanam da eliminação da variabilidade, mas da capacidade do sistema de absorvê-la, integrá-la e ajustar-se a ela.

2.4.5 Modelo de Causalidade de Acidentes

A Engenharia de Resiliência não oferece um modelo tradicional de causalidade de acidentes. Em vez disso, propõe que os acidentes emergem quando a variabilidade de desempenho excede a capacidade adaptativa do sistema. O conceito de ressonância funcional (Hollnagel, 2012) sugere que, quando as variabilidades de múltiplas funções se combinam de forma inesperada, podem produzir resultados que não poderiam ser previstos a partir da análise de funções individuais.

Observado pela lente de modelos lineares de causa e efeito, um ajuste local que precedeu a falha tende a ser apontado como sua causa. Mas, se o ajuste é inerente ao funcionamento do sistema e não há diferença qualitativa entre os ajustes que produzem sucesso e os que produzem falha, a análise tradicional revela-se limitada. Essa perspectiva desloca o foco analítico de "o que falhou" para "como a variabilidade normal se combinou e propagou". O acidente não é compreendido como produto de um sistema perfeito que se degradou, mas de um sistema complexo que operou com variabilidades esperadas e, em determinado contexto, viu suas combinações culminarem em desfecho indesejado.

Essa concepção rompe com a lógica da "causa raiz" e com a busca por uma "bala de prata" que tornaria o sistema infalível. Em vez de tentar eliminar a variabilidade – o que frequentemente engessa a operação e destrói a agilidade necessária ao trabalho real –, a abordagem amplia as margens de adaptabilidade e fortalece a capacidade do sistema de monitorar e antecipar como as variações interagem. Gerir a segurança, sob essa perspectiva, significa capacitar o sistema para absorver distúrbios e, quando preciso, falhar de forma segura – garantindo que, mesmo diante do inesperado, a organização disponha de recursos cognitivos e operacionais para retomar o equilíbrio funcional.

2.4.6 Forças e Limitações

Forças

- **Perspectiva positiva e proativa.** Foco em garantir o sucesso, e não apenas em prevenir falhas – privilegia o aprendizado a partir do trabalho que dá certo, e não apenas daquilo que dá errado.
- **Ferramentas práticas.** RAG e FRAM oferecem metodologias aplicáveis e alinhadas à perspectiva da Engenharia de Resiliência, em contraponto às metodologias tradicionais lineares.
- **Reconhecimento da realidade operacional.** A distinção entre *Work-as-Done* e *Work-as-Imagined* captura uma realidade frequentemente ignorada pelos sistemas formais de gestão e impulsiona as organizações a olharem para a execução real do trabalho, e não apenas para o que está prescrito.
- **Integração teórica.** Dialoga com correntes anteriores (NAT, HRO, sociotécnica) e contribui para a consolidação dos conceitos associados ao *Safety-II*.
- **Aprender com o sucesso.** Estudar por que as coisas dão certo, e não apenas quando dão errado, é uma diferenciação epistemológica significativa em relação às abordagens tradicionais.

Limitações

- **Dificuldade de medição.** Resiliência e capacidade adaptativa são difíceis de quantificar e por vezes parecem conceitos abstratos diante da perspectiva prática. O RAG, conforme já discutido, não constitui medida objetiva, mas instantâneo qualitativo, cujo valor está no acompanhamento longitudinal e no diálogo organizacional que suscita (Patriarca et al., 2021).
- **Desafios de tradução teoria-prática.** A abundância de conceitos e terminologia dificulta a adoção por praticantes e a aplicação consistente, sobretudo por conflitarem com a perspectiva tradicional. Como reconhece a própria comunidade RE, "*gestores querem ferramentas simples para tomar decisões... há necessidade de interpretação concisa em linguagem simples*" (*Resilience Engineering Association*, 2024).

- **Validação empírica em desenvolvimento.** Conceitos centrais ainda carecem de validação empírica robusta. Bergström e Dekker (2019) observam que a formulação original dos quatro potenciais "não foi particularmente orientada por dados ou literatura". A própria comunidade RE reconhece que, "*embora a RE seja rica em teorias, ainda não há evidência suficiente de que oferece benefícios substanciais*" (*Resilience Engineering Association, 2024*).

Três Armadilhas Analíticas (Bergström & Dekker, 2019)

As três armadilhas analíticas que se seguem foram sistematizadas por Bergström e Dekker (2019), mas sua origem é anterior e, em parte de sua autoria, brasileira: remontam ao estudo seminal de Bergström, van Winsen e Henriqson (2015), que, em revisão da literatura de segurança, evidenciou que o sujeito da resiliência tende a ser construído como o indivíduo, na linha de frente ou em níveis gerenciais, convocado a adaptar-se diante do risco para garantir o desempenho contínuo de sistemas inerentemente arriscados. A partir desse achado, os autores formularam três questões éticas que antecipam diretamente as armadilhas: (1) a resiliência deve ser vista como pessoas que prosperam apesar do risco, ou por causa dele?; (2) a teoria da resiliência deve servir de base para julgamento moral?; e (3) até que ponto a resiliência deve ser tratada como traço do indivíduo? Essas três perguntas estruturam, respectivamente, as armadilhas reducionista, moral e normativa.

Armadilha Reducionista

A armadilha reducionista consiste em construir a resiliência de modo a localizar suas capacidades adaptativas exclusivamente no nível micro do sistema, ou seja, na linha de frente (*sharp end*). Segundo Bergström e Dekker (2019, p. 420), "a Resiliência torna-se a promessa de que, por mais desafiadores que sejam os conflitos de objetivos, ou por mais dinâmicas e surpreendentes que sejam as ameaças, as capacidades adaptativas da linha de frente garantirão (e deverão garantir) o funcionamento do sistema como um todo". Trata-se, portanto, de uma leitura equivocada das raízes da teoria da complexidade – que afirma justamente

a impossibilidade de reduzir o comportamento macro do sistema ao comportamento micro de seus operadores.

Os autores ilustram a armadilha por meio do caso "*Pot Lids and Bicycle Bells*", ocorrido em 2010 no hospital Östra Sjukhuset, em Gotemburgo, Suécia. Diante de uma enfermaria de emergência superlotada e da ausência de campainhas para os pacientes em macas nos corredores, a equipe de enfermagem improvisou: passou a distribuir tampas de panela e talheres aos pacientes e, posteriormente, comprou campainhas de bicicleta para que estes pudessem chamar ajuda. A história tornou-se pública pela imprensa (Bergström & Dekker, 2019, pp. 418-419).

Vista pela ótica da linha de frente, é uma narrativa de resiliência: equipes mantendo o sistema em funcionamento sob grande pressão por meio de inventividade e adaptação. Vista, porém, da perspectiva da complexidade, trata-se de "resiliência apesar do sistema" – não «resiliência graças ao sistema». Quando o sucesso depende exclusivamente do improviso constante da linha de frente, o sistema não é resiliente; é, na verdade, extremamente frágil e opera em estado de descompensação adaptativa, no sentido empregado por Woods (2015). Para que a Engenharia de Resiliência seja eticamente sustentável, a adaptabilidade deve ser uma propriedade projetada e suportada pela organização – "resiliência por conta do sistema" –, e não recurso de última instância que consome a saúde e a capacidade cognitiva dos trabalhadores. Esse deslocamento já havia sido diagnosticado por Bergström, van Winsen e Henriqson (2015), para quem o discurso da resiliência corre o risco de transferir os riscos residuais dos sistemas sociotécnicos complexos para as costas do indivíduo – o operador da ponta ou as equipes –, convocados a mobilizar suas capacidades adaptativas para absorver perturbações perigosas e equilibrar múltiplos objetivos, muitas vezes conflitantes.

Armadilha Moral

A armadilha moral relaciona-se de modo estreito à reducionista, mas vai um passo adiante na responsabilização (*responsibilization*) dos atores da linha de frente pelo comportamento resiliente do sistema como um todo (Bergström & Dekker, 2019, pp. 420-422). Diferentemente da concepção descritiva original da



resiliência, a armadilha moral transforma o conceito em categoria normativa de *accountability* moral do operador.

Os autores exemplificam essa armadilha por meio da introdução, em 2015, do conceito de resiliência no framework regulatório de *Crew Resource Management (CRM)* da *European Aviation Safety Agency – EASA* (GM5 ORO.FC.115, em EASA Annex II to ED Decision 2015-022-R). Embora movida pelas melhores intenções, a regulamentação introduz no discurso operacional uma linguagem altamente normativa – "*overreactions*", "*inappropriate hesitation*", "*improper action*" e "*balanced response*" –, criando categorias de avaliação moral do piloto que ampliam, em vez de reduzir, as bases sobre as quais ele pode ser responsabilizado pelas falhas do sistema. Conforme observam Bergström e Dekker (2019, p. 422), "em vez de empoderar os pilotos para influenciar seu espaço discricionário, a resiliência fornece meios para responsabilizá-los ainda mais pelo comportamento do sistema no qual estão inseridos".

A advertência é clara: quando o sistema usa a linguagem da resiliência para deslocar a responsabilidade pelas pressões de produção, conflitos de objetivos e escassez de recursos para o indivíduo, o conceito perde seu poder analítico e converte-se em ferramenta de transferência de responsabilidade – fenômeno também descrito, no contexto brasileiro, por Bergström, van Winsen e Henriqson (2015). Como observam esses autores, há o risco de a resiliência tornar-se mais uma referência normativa para o julgamento moral após a falha – um recurso *ex post facto* para narrar que o acidente decorreu de quem "não foi resiliente o suficiente", isto é, de quem não seguiu os princípios (os quatro potenciais) da resiliência.

Armadilha Normativa

A armadilha normativa surge quando a noção de resiliência se estabelece como reivindicação normativa carregada de valor – implicando, no limite, que a resiliência é sempre desejável. Bergström e Dekker (2019, p. 424) sintetizam o efeito mais grave dessa armadilha: "*o discurso parece silenciar – ou mesmo abandonar – a questão Perrowiana sobre se deveríamos aceitar tais riscos em primeiro lugar*".

Em outras palavras, ao tratar a adaptabilidade como bem absoluto, a organização passa a aceitar a permanência em estados operacionais perigosos como condição inerente, em vez de questionar se determinadas atividades deveriam, em primeiro lugar, ser realizadas naquelas condições. A armadilha normativa pode, assim, transformar a resiliência em mecanismo de preservação de sistemas estruturalmente perigosos, no qual "sobreviver ao caos" passa a ser priorizado sobre estruturar a segurança na fonte. A questão ética central, portanto, é: existe um limite no qual a busca pela adaptação deve ser encerrada em favor da eliminação ou do controle das ameaças na origem?

2.4.7 Debates e Controvérsias

A consolidação da Engenharia de Resiliência suscitou debates relevantes no campo de Fatores Humanos, sobretudo em relação às Organizações de Alta Confiabilidade (HRO) e à Teoria dos Acidentes Normais (NAT), ambas já tratadas neste compêndio. O debate mais significativo concerne à relação entre RE e HRO.

Hopkins (2014) levantou a questão de forma direta, observando que a descrição de Woods (2009) sobre como um departamento de emergência hospitalar mobiliza recursos adicionais sob alta carga de trabalho é "poderosamente reminiscente" das descrições, na literatura HRO, sobre como centros de controle de tráfego aéreo recorrem a "pares de olhos adicionais" em períodos de pico (La Porte & Consolini, 1991). Para Hopkins, "o mesmo fenômeno está sendo descrito em ambos os casos". Sua crítica é mais ampla: a Engenharia de Resiliência apresenta-se como algo novo, mas, ao exame, é difícil identificar em que aspectos ela ultrapassa, de forma substantiva, a teoria HRO.

Haavik et al. (2019) abordam a questão a partir de uma perspectiva pragmática, posicionando RE e HRO como contrapontos comuns à Teoria dos Acidentes Normais. Enquanto Perrow (1984) sustenta que alguns sistemas de alta complexidade e acoplamento estreito não deveriam, em rigor, ser preservados, RE e HRO buscam, ambas, formas de manter o funcionamento desses sistemas. Em sua análise comparativa, os autores concluem que a pergunta "são realmente diferentes?" pode ser menos importante do que "que conhecimento produzem?" – sugerindo que ambas as abordagens contribuem para a compreensão da segurança e podem ser tomadas como complementares para um olhar sistêmico em Fatores Humanos.

Os defensores da Engenharia de Resiliência argumentam que, mesmo onde os conceitos se sobrepõem à HRO, a perspectiva oferece um framework integrativo e uma ênfase distintiva na variabilidade de desempenho e na capacidade adaptativa que transcende formulações anteriores. Importa observar que as três armadilhas analíticas discutidas na seção 2.4.6 – reducionista, moral e normativa – foram formuladas por Bergström e Dekker (2019), a partir da crítica seminal de Bergström, van Winsen e Henriqson (2015), e não a Haavik et al. (2019).

Vale registrar que os próprios proponentes dessa agenda crítica não postulam uma conclusão pessimista nem a repetição do antigo debate NAT/HRO. Bergström, van Winsen e Henriqson (2015) propõem um "debate crítico, porém construtivo" sobre os pressupostos, a epistemologia e sobretudo as implicações discursivas do uso da resiliência: menos "as abordagens são realmente diferentes?" e mais "que papel esse objeto cria para o sujeito cumprir?". Trata-se de leitura convergente com o princípio de pluralismo teórico adotado neste compêndio, que trata as perspectivas como repertório complementar, e não como escolas rivais.

2.4.8 Desenvolvimentos Recentes

A Engenharia de Resiliência tem se consolidado, ao longo das duas últimas décadas, como abordagem central para compreender e fortalecer a segurança em sistemas sociotécnicos complexos. Três eixos contemporâneos de desenvolvimento merecem destaque: a institucionalização do campo por meio da *Resilience Engineering Association (REA)* e o crescimento da comunidade *FRAMily*; a expansão empírica conduzida por Woods em domínios digitais; e a convergência com outras

perspectivas contemporâneas – *Safety Differently* e *Human and Organizational Performance (HOP)* – no movimento descrito como "New Views" da segurança.

Institucionalização: REA e FRAMily

A consolidação científica do campo foi acompanhada da criação da Resilience Engineering Association, cuja missão é promover pesquisa, intercâmbio acadêmico e aplicação prática dos princípios da RE. A REA contribuiu significativamente para dar coesão conceitual ao campo e para fomentar o diálogo entre pesquisadores e profissionais de diferentes setores (*Resilience Engineering Association*, 2024).

Em paralelo, destaca-se o crescimento da FRAMily, rede internacional de praticantes e pesquisadores que utilizam o *Functional Resonance Analysis Method*. A expansão da *FRAMily* reflete a aplicabilidade do método em múltiplos domínios, incluindo aviação, saúde, indústria de processos, operações marítimas e infraestruturas críticas (Patriarca et al., 2021). O FRAM não se limita à análise de acidentes: constitui ferramenta para apoiar a aprendizagem organizacional, a análise prospectiva e a compreensão do trabalho real em contextos complexos.

Woods e a aplicação em ambientes digitais

Como já antecipado na seção 2.4.4, Woods e colaboradores expandiram a investigação empírica da extensibilidade graciosa e da adaptabilidade sustentada para os contextos de tecnologia da informação, software e DevOps. Os estudos descrevem como engenheiros e SREs gerenciam a disponibilidade de sistemas críticos sob condições de incerteza e mudança contínua, e como a resiliência em ambientes digitais depende menos da robustez do código e da automação redundante do que da capacidade humana de intervir e estender o alcance dos sistemas além de seus limites previstos de projeto.

Integração com *Safety Differently* e *HOP*: as "*New Views*"

Desenvolvimentos recentes indicam convergência entre a Engenharia de Resiliência e outras perspectivas contemporâneas, como o *Safety Differently*, proposto por Sidney Dekker, e o *Human and Organizational Performance (HOP)*, associado a Todd

Conklin. Embora tenham trajetórias distintas, as três abordagens compartilham fundamentos conceituais centrais: rejeição de modelos punitivos baseados no erro individual, valorização do trabalho-como-realizado e reconhecimento das pessoas como fontes de adaptação, flexibilidade e recuperação, e não como meros agentes de risco. A Tabela 2.4.2 sintetiza pontos de contato entre as três perspectivas.

Tabela 2.4.2 — Pontos de contato entre Engenharia de Resiliência, Safety Differently e HOP

Eixo	Engenharia de Resiliência	Safety Differently	**HOP** (Human and Organizational Performance)
Pessoas como recurso	Pessoas ajustam continuamente suas ações para lidar com variabilidade, pressão e incerteza; a capacidade adaptativa mantém o sistema funcionando (Hollnagel et al., 2006).	Pessoas criam segurança o tempo todo, mesmo em sistemas imperfeitos (Dekker, 2015).	O erro humano é consequência do sistema, não falha moral ou individual (Conklin, 2012).
Trabalho real	A variabilidade operacional é normal e necessária para responder às condições reais (Hollnagel, 2014).	Segurança não é seguir regras cegamente, mas ajustar o trabalho para que ele funcione (Dekker, 2015).	Foca na compreensão do trabalho real antes de impor novos controles ou regras (Conklin, 2012).
Contexto sistêmico	Um sistema é seguro quando consegue antecipar, monitorar, responder e aprender (Hollnagel, 2008, 2011).	Troca o foco da "ausência de acidentes" para a presença de capacidades de adaptação (Dekker, 2015).	Enfatiza desempenho operacional seguro em condições normais, não apenas em falhas (Conklin, 2012).
Alinhamento Safety-II	Desempenho é influenciado por pressões de tempo, metas conflitantes e recursos disponíveis (Hollnagel, 2014).	Pessoas não escolhem errar; escolhem a melhor ação possível dentro das condições (Dekker, 2014).	Investigações devem revelar como o contexto guiou escolhas razoáveis (Conklin, 2012).

Eixo	Engenharia de Resiliência	Safety Differently	**HOP** (Human and Organizational Performance)
Just Culture	Punição reduz a capacidade de adaptação e de reporte do sistema (Hollnagel et al., 2006).	Ambiente punitivo destrói a confiança e a aprendizagem organizacional (Dekker, 2014).	Promove accountability equilibrada: aprender sem renunciar à responsabilidade (Conklin, 2019).
Liderança adaptativa	Liderança deve sustentar recursos, margens de segurança e flexibilidade (Hollnagel, 2014).	Líderes devem cuidar das pessoas, não as controlar excessivamente (Dekker, 2015).	Liderança ativa no campo (learning teams, leadership walkarounds) (Conklin, 2019).

Nota. Elaborada pelos autores com base em Hollnagel (2008, 2014), Hollnagel et al. (2006), Dekker (2014, 2015) e Conklin (2012, 2019).

A integração dessas perspectivas tem sido descrita como a emergência das "*New Views*" da segurança, parte do conjunto que este compêndio reúne sob a designação de Nova Segurança (Seção 1.2.5) – movimento que busca a transição de uma visão reativa, baseada em falhas (*Safety-I*), para uma abordagem proativa, orientada à compreensão das condições que sustentam o desempenho bem-sucedido (*Safety-II*). Nessa perspectiva, a segurança passa a ser compreendida como propriedade emergente dos sistemas sociotécnicos, construída continuamente por decisões organizacionais, práticas operacionais e capacidades humanas de adaptação.

Contribuições brasileiras

A produção brasileira em Fatores Humanos e Engenharia de Resiliência tem contribuído de modo crescente e reconhecido internacionalmente, tanto na reflexão crítica quanto na agenda construtiva do campo. No eixo crítico, Bergström, van Winsen e Henriqson (2015) – trabalho de coautoria brasileira entre os mais citados sobre o tema – expuseram o risco de a resiliência ser construída como traço do indivíduo, deslocando para a linha de frente a responsabilidade por riscos sistêmicos (*accountability downward*), crítica que fundamenta a armadilha redu-

cionista discutida na Seção 2.4.6. No eixo construtivo, a coletânea *Resilience in a Digital Age* (Matos, Selig & Henriqson, 2022) reúne contribuições que reposicionam a resiliência como propriedade organizacional centrada nas pessoas – "somente colocando as pessoas no centro da transformação é possível aspirar organizações e uma sociedade resilientes". No eixo metodológico, destacam-se a revisão sistemática da produção científica sobre o RAG (Gonçalves et al., 2022) e o framework de avaliação da resiliência a partir da observação do trabalho cotidiano proposto por Trancoso, Patriarca e Henriqson (2024).

Entre os pesquisadores brasileiros de referência destacam-se, em diferentes domínios de aplicação: **Eder Henriqson** (PUCRS – aviação e óleo e gás), em reflexão crítica sobre o campo e aplicação da Engenharia de Resiliência em operações críticas; **Josué França** (Petrobras – óleo e gás), na aplicação do FRAM; **Tarcísio Saurin** (UFRGS – saúde e construção civil), em FRAM, folgas (slacks) e *Design for Resilient Performance*; **Carlos Formoso** (UFRGS – construção civil), na gestão participativa da segurança; **Priscila Wachs** (PUCRS – saúde e óleo e gás); **Paulo Victor de Carvalho** (UFRJ – saúde e nuclear); e **Moacyr Cardoso** (ITA – aviação), em FRAM. No plano metodológico e operacional nacional, a PetroHRA (aprovada pela ANP) adapta a análise de confiabilidade humana ao contexto brasileiro de óleo e gás, e os *Learning and Improvement Teams* (LIT) materializam princípios da Engenharia de Resiliência e do HOP em campo.

2.4.9 Implicações para a Indústria de Energia

A indústria de energia opera em contextos caracterizados por elevada complexidade, forte interdependência sociotécnica e alta variabilidade operacional. Nesses cenários, abordagens tradicionais de segurança – centradas na eliminação de falhas e no cumprimento estrito de procedimentos – mostram-se insuficientes para lidar com condições dinâmicas e imprevisíveis. A Engenharia de Resiliência oferece perspectiva particularmente relevante para o setor ao enfatizar a capacidade adaptativa dos sistemas, o papel do trabalho real e o aprendizado contínuo a partir das operações normais.

Gestão da variabilidade como propriedade central

Uma das principais contribuições da Engenharia de Resiliência para a indústria de energia é o reconhecimento de que a variabilidade operacional é normal e inerente ao funcionamento de sistemas complexos. As adaptações cotidianas não devem ser interpretadas automaticamente como desvios ou violações, mas como expressões legítimas da capacidade adaptativa do sistema. Na indústria de energia, fatores como condições ambientais, interfaces entre equipes, restrições técnicas e demandas operacionais em constante mudança tornam impossível a execução do trabalho exatamente como prescrito. A gestão eficaz da variabilidade torna-se, assim, elemento central da segurança, substituindo a busca irrealista por operação totalmente padronizada. A organização deve apoiar decisões locais bem fundamentadas, criando condições para que adaptações necessárias ocorram de forma segura, em vez de penalizá-las.

Aprendizado a partir das operações normais

Tradicionalmente, o aprendizado organizacional em segurança ocorre de forma reativa, após acidentes ou incidentes significativos. A Engenharia de Resiliência amplia esse horizonte ao defender que as organizações aprendam também com aquilo que funciona bem. O estudo de operações normais e bem-sucedidas permite identificar práticas eficazes, mecanismos de adaptação e fatores que sustentam o desempenho seguro no dia a dia (Hollnagel, 2014). Na indústria de energia, esse enfoque contribui para uma compreensão mais realista do funcionamento do sistema e para a melhoria contínua da segurança operacional, como ilustram estudos em operações de midstream no Brasil (Marques et al., 2025). Esse deslocamento, de aprender apenas com o que falha para aprender também com o trabalho que dá certo, é aprofundado na **Seção 3.2 (Aprendizagem com Eventos e Investigação de Acidentes)**, que trata a aprendizagem organizacional de forma articulada entre eventos adversos e operações normais.

Múltiplas interfaces operacionais

As operações de óleo e gás envolvem múltiplas interfaces: pessoas, tecnologia, procedimentos, clima, logística, requisitos regulatórios e pressões por produção. A Engenharia de Resiliência reconhece que a variabilidade do trabalho é inevitável e necessária, e que a segurança emerge da capacidade das equipes de se adaptar em tempo real, e não apenas do cumprimento de procedimentos. Essa perspectiva dialoga diretamente com situações como operações offshore, manobras críticas, emissão e execução de Permissões de Trabalho (PT) e Análises Preliminares de Risco (APR), resposta a emergências, operações em Posicionamento Dinâmico (DP), operações marítimas e atividades de manutenção.

Complemento ao arcabouço regulatório

O setor de energia é regulado por um conjunto extenso e exigente de normas – entre as quais o *International Safety Management Code (ISM)*, as normas ISO de gestão da segurança, as Normas da Autoridade Marítima (NORMAM) emitidas pela Marinha do Brasil, as Resoluções da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP) e os padrões internos de operadoras como a Petrobras, além das exigências contratuais de clientes internacionais. A Engenharia de Resiliência complementa esse modelo regulatório ao: (a) avançar além do "cumprir procedimento"; (b) valorizar o trabalho real, as adaptações locais e a experiência operacional; e (c) compreender por que as operações funcionam bem na maior parte do tempo, mesmo sob pressão. Esse complemento dialoga diretamente com a discussão internacional sobre as limitações da abordagem prescritiva pós-Macondo (2010), na qual a investigação revelou múltiplos fatores sistêmicos para além da chamada "causa raiz" individual (Bergström & Dekker, 2019).

Os quatro potenciais aplicados ao setor

Desenvolver os quatro potenciais – responder, monitorar, antecipar e aprender – exige revisar as práticas e rotinas da organização para que os expressem de forma integrada, e desenvolver a fluência das lideranças no tema, de modo a assegurar

coerência entre o que se fala e pratica. Esse desenvolvimento corresponde ao Movimento V do framework integrador apresentado na Parte IV (Seção 4.2.5).

Síntese: contribuições e cautelas

Contribuições da Engenharia de Resiliência para a indústria de energia

- **Gestão da variabilidade:** reconhecer que a variabilidade é normal e necessária, focando em gerenciá-la em vez de eliminá-la.
- **Fortalecimento da capacidade adaptativa:** desenvolver os quatro potenciais organizacionais (responder, monitorar, antecipar e aprender).
- **Apoio ao trabalho-como-realizado:** reconhecer a lacuna entre procedimentos e prática, apoiando adaptações necessárias em vez de penalizá-las.
- **Aprendizado com operações normais:** não esperar acidentes para aprender; estudar como operações bem-sucedidas funcionam.
- **Aplicação do FRAM:** modelar operações complexas e identificar potenciais ressonâncias funcionais. Primeiro uso do termo por Woods (2003), após o acidente do Columbia.

Cautelas para a aplicação

- Evitar as três armadilhas – reducionista, moral e normativa – descritas por Bergström e Dekker (2019).
- Reconhecer sobreposições com a teoria HRO e integrar perspectivas (Hopkins, 2014; Haavik et al., 2019).
- Investir na tradução teoria-prática com linguagem acessível, tornando os conceitos operacionalizáveis sem perda de rigor.
- Atentar para o risco de reapropriação dos conceitos de resiliência como transferência de responsabilidade ao operador – o argumento de que "o trabalhador não foi resiliente o suficiente" configura *accountability downward* disfarçado de empoderamento (Bergström, van Winsen e Henriqson, 2015). A capacidade adaptativa deve ser habilitada pela organização, não delegada ao indivíduo.

2.4.10 Quadro-Resumo: Engenharia de Resiliência

Dimensão	Engenharia de Resiliência (RE)
Período de Surgimento	Söderköping, Suécia (2004); Hollnagel, Woods e Leveson (2006). Raízes na comunidade Risø dos anos 1980.
Principais Autores	Erik Hollnagel (quatro potenciais, FRAM, ETTO); David D. Woods (extensibilidade graciosa, adaptabilidade sustentada); Nancy Leveson (engenharia de sistemas, STAMP).
Fundamento Teórico	Ciência da complexidade; teoria de sistemas adaptativos; engenharia de sistemas cognitivos; comunidade Risø
Pressuposto Central	Segurança é capacidade de ter sucesso sob condições variadas; variabilidade de desempenho é normal e necessária, não aberração.
Concepção de Risco	Risco como variabilidade do desempenho – Resultado da variabilidade normal de desempenho – emerge quando a variabilidade excede a capacidade adaptativa; o mesmo processo produz sucesso e falha.
Visão da Contribuição Humana	Humanos como fonte de adaptação e resiliência; a flexibilidade humana compensa limitações de design; expertise distribuída.
Estratégias de Controle	Compreender o trabalho real; gerenciar a variabilidade em vez de eliminá-la; desenvolver as quatro capacidades (responder, monitorar, antecipar, aprender).
Modelo de Causalidade	Acidentes emergem da ressonância funcional – quando variabilidades se combinam de formas inesperadas, excedendo a capacidade adaptativa do sistema.
Forças	Visão proativa; reconhece a realidade operacional (WAD/WAI); ferramentas práticas (FRAM, RAG); integração de múltiplas perspectivas; aprendizado a partir do trabalho que dá certo.

Dimensão	Engenharia de Resiliência (RE)
Limitações/Críticas/Cautelas	Dificuldade de medição (o RAG é instantâneo qualitativo, não métrica objetiva); validação empírica em desenvolvimento; desafios de tradução teoria-prática; sobreposição com HRO; armadilhas reducionista, moral e normativa (Bergström & Dekker, 2019).

Nota. Elaborada pelos autores com base em Hollnagel et al. (2006), Hollnagel (2008, 2009, 2011, 2012, 2014), Woods (2015), Bergström e Dekker (2019), Patriarca et al. (2021) e Resilience Engineering Association (2024), (Bergström & Dekker, 2019); não substitui a confiabilidade.



Referências da Seção 2.4

Bergström, J., & Dekker, S. W. A. (2019). The 2010s and onward: Resilience engineering. In S. W. A. Dekker, *Foundations of safety science: A century of understanding accidents and disasters* (pp. 391–426). CRC Press. https://doi.org/10.4324/9781351059794

Bergström, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety, 141*, 131–141. https://doi.org/10.1016/j.ress.2015.03.008

Columbia Accident Investigation Board. (2003). *Report of the Columbia Accident Investigation Board*, Volume 1. NASA

Conklin, T. (2012). *Pre-accident investigations: An introduction to organizational safety*. Ashgate.

Conklin, T. (2019). *The 5 principles of human performance: A contemporary update of the building blocks of Human Performance for the new view of safety*. PreAccident Media.

Dekker, S. W. A. (2014). *The field guide to understanding 'human error'* (3rd ed.). Ashgate.

Dekker, S. W. A. (2015). *Safety differently: Human factors for a new era* (2nd ed.). CRC Press.

Dekker, S. W. A. (2019). *Foundations of safety science: A century of understanding accidents and disasters*. CRC Press. https://doi.org/10.4324/9781351059794

Gonçalves, B., Wachs, P., Freitas, J. H., Pulz, M., & Henriqson, E. (2022). Resilience Assessment Grid: mapeando o cenário da produção científica. *In Anais do XLII Encontro Nacional de Engenharia de Produção (ENEGEP)*. ABEPRO. https://www.abepro.org.br/biblioteca/TN_ST_389_1928_43585.pdf

Haavik, T. K., Antonsen, S., Rosness, R., & Hale, A. (2019). HRO and RE: A pragmatic perspective. *Safety Science, 117*, 479–489. https://doi.org/10.1016/j.ssci.2016.08.010

Hale, A., & Heijer, T. (2006). Defining resilience. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 35–40). Ashgate.

Hollnagel, E. (2006). Resilience — The challenge of the unstable. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 9–17). Ashgate.

Hollnagel, E. (2008). Preface. In E. Hollnagel, C. P. Nemeth, & S. Dekker (Eds.), *Resilience engineering perspectives, Volume 1: Remaining sensitive to the possibility of failure* (pp. xi–xiv). Ashgate.

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

Hollnagel, E., Tveiten, C. K., & Albrechtsen, E. (2010). *Resilience engineering and integrated operations in the petroleum industry* (SINTEF Report A16331). SINTEF.

Hollnagel, E. (2011). RAG — The resilience analysis grid. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice: A guidebook* (pp. 275–296). Ashgate.

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method — Modelling complex socio-technical systems*. Ashgate.

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

Hollnagel, E. (2018). Safety-II in practice: *Developing the resilience potentials. Routledge*

Hollnagel, E. (2025). From safety to safely: Principles and practice of systemic potentials management. Routledge.

Hollnagel, E. (2026). Decremental and incremental safety cultures: Safety-I and Safety-II revisited. CRC Press.

Hollnagel, E., Nemeth, C. P., & Dekker, S. (Eds.). (2009). *Resilience engineering perspectives, Volume 2: Preparation and restoration*. Ashgate.

Hollnagel, E., & Slater, D. (2026). The incremental safety manifesto. https://incrementalsafety.com/

Hollnagel, E., Wears, R. L., & Braithwaite, J. (2015). *From Safety-I to Safety-II: A white paper*. The Resilient Health Care Net; University of Southern Denmark; University of Florida; Macquarie University.

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

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.

Hopkins, A. (2014). Issues in safety science. *Safety Science, 67*, 6–14. https://doi.org/10.1016/j.ssci.2013.01.007

La Porte, T. R., & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenges of "high-reliability organizations". *Journal of Public Administration Research and Theory, 1*(1), 19–48.

Ljungberg, D., & Lundh, V. (2013). *Resilience engineering within ATM: Development, adaption and application of the Resilience Analysis Grid* (RAG).

Marques, L., Fogaça, L., Henriqson, É., & Amário, M. (2025). *Learning from normal work in complex sociotechnical system: Case in midstream operations. Process Safety Progress.* https://doi.org/10.1002/prs.70022

Matos, F., Selig, P. M., & Henriqson, E. (Eds.). (2022). *Resilience in a digital age: Global challenges in organisations and society*. Springer. https://doi.org/10.1007/978-3-030-85954-1

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2021). Resilience engineering for sociotechnical safety management. In G. Salvendy & W. Karwowski (Eds.), *Handbook of human factors and ergonomics* (5th ed., pp. 475–494). Wiley. https://doi.org/10.1002/9781119636113.ch18

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Resilience Engineering Association. (2024). *RE 20 years: Notes from the Porto meeting*. Zenodo. https://doi.org/10.5281/zenodo.14507214

Trancoso, R., Patriarca, R., & Henriqson, É. (2024). *Assessing resilience in everyday work through observations: An assessment framework for complex sociotechnical systems.* Safety Science, 173, 106461.

Westrum, R. (2006). A typology of resilience situations. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 55–65). Ashgate.

Woods, D. D. (2003). *Creating foresight: How resilience engineering can transform NASA's approach to risky decision making* [Depoimento ao Committee on Commerce, Science and Transportation do Senado dos EUA]. Washington, D.C.

Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts*

(pp. 21–34). Ashgate.

Woods, D. D. (2009). Escaping failures of foresight. *Safety Science, 47*(4), 498–501. https://doi.org/10.1016/j.ssci.2008.07.030

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety, 141*, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

Woods, D. D. (2018). The theory of graceful extensibility: Basic rules that govern adaptive systems. *Environment Systems and Decisions*, 38, 433–457.

Woods, D. D., & Cook, R. I. (2002). Nine steps to move forward from error. *Cognition, Technology and Work, 4*(2), 137–144.

2.5 Perspectivas de Dependência de Trajetória

Autores: Marcelo Cury e Cristina Ribeiro

Revisão e Figuras: Rafael Ceni de Almeida

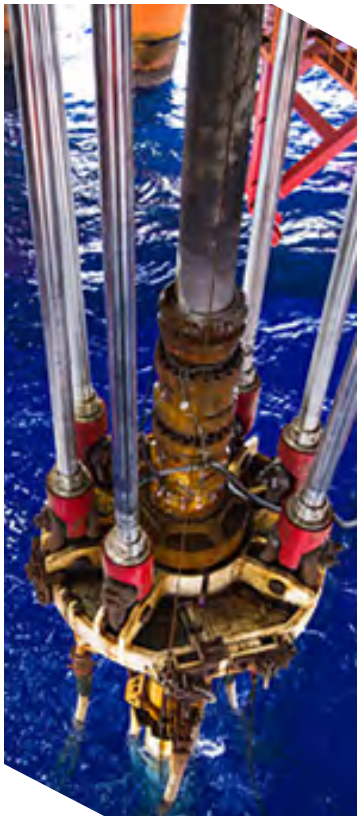
2.5.1 Introdução e Contexto Histórico

As perspectivas de dependência de trajetória representam uma família de teorias sociológicas que compartilham uma premissa fundamental: **os acidentes têm história.** Estas teorias emergiram de estudos detalhados de desastres organizacionais e revelam como condições para falha se desenvolvem ao longo do tempo por meio de processos incrementais que parecem racionais no momento em que ocorrem. Ao deslocar o foco da causalidade imediata para os processos históricos e organizacionais, essas abordagens passaram a analisar os acidentes como o resultado de trajetórias construídas ao longo do tempo, marcadas por decisões, interpretações e adaptações sucessivas.

O conceito de dependência de trajetória, com raízes na economia e na ciência política, foi incorporado à ciência da segurança para explicar como escolhas organizacionais passadas condicionam possibilidades futuras, restringindo alternativas e reforçando padrões de ação. Assim, os sistemas sociotécnicos não evoluem de forma neutra, mas seguem caminhos moldados por experiências anteriores, sucessos acumulados, pressões organizacionais e estruturas institucionais que tendem a reproduzir decisões previamente adotadas

O trabalho pioneiro foi *Man-Made Disasters* de **Barry Turner** (1978), considerado a primeira teoria a argumentar sistematicamente que acidentes são fenômenos sociais e organizacionais, não meramente técnicos. Turner é frequentemente reconhecido como um "pioneiro subestimado" da ciência da segurança (Bills, 2023), cujo trabalho precedeu e fundamentou os desenvolvimentos posteriores de Reason, Perrow e Vaughan. Turner demonstrou, a partir da análise sistemática de múltiplos acidentes, que desastres são precedidos por um *período de incu-*

bação, fase em que sinais de risco são gradualmente ignorados, reinterpretados ou não reconhecidos pelas organizações, permitindo a acumulação de condições latentes que, eventualmente, levam à falha.



Desenvolvimentos subsequentes ampliaram esta perspectiva temporal. **Starbuck e Milliken** (1988) analisaram o desastre do Challenger por meio do processo de *fine--tuning*, identificando como ajustes incrementais baseados em sucessos anteriores erodem progressivamente as margens de segurança. **Diane Vaughan** (1996), também estudando o Challenger, desenvolveu o conceito de *"normalização do desvio"*, descrevendo como desvios das especificações originais se tornam gradualmente aceitos como normais. **Scott Snook** (2000), analisando o incidente de fogo amigo sobre o Iraque, introduziu o conceito de *"deriva prática"*, destacando o afastamento gradual entre regras formais e práticas reais de trabalho. A esses marcos soma-se a síntese integradora de **Dekker** (2011) em "*Drift into Failure*", que articula as contribuições de Turner, Vaughan e Snook ao modelo de migração aos limites de Rasmussen (1997) e é apresentada, como conceito fundamental da tradição, na Seção 2.5.3.

2.5.2 Pressupostos Críticos

As perspectivas de dependência de trajetória compartilham pressupostos distintivos:

1. **Temporalidade da causalidade:** Acidentes não são eventos pontuais, mas o desfecho de processos que se desenvolvem ao longo de meses ou anos. Turner (1978, p. 88) documentou períodos de incubação variando de semanas a décadas, nos quais condições latentes se acumulam de forma imperceptível aos atores organizacionais.
2. **Racionalidade local:** Decisões que contribuem para acidentes fazem sentido no contexto em que são tomadas, ou as pessoas não as teriam tomado. Não existem "decisões monumentalmente ruins"; há apenas

pequenos passos incrementais que parecem razoáveis dado o conhecimento disponível no momento.

3. **Incrementalismo:** A deriva para falha ocorre por meio de pequenas mudanças, não de desvios dramáticos. Conforme Starbuck e Milliken (1988, p. 323): "*Fine-tuning* raramente eleva a probabilidade de sucesso, e frequentemente torna o sucesso menos certo." Cada pequeno passo que se revela bem-sucedido sem comprometer a segurança torna-se a base para o próximo afastamento incremental da norma estabelecida.
4. **Sucesso como precursor de falha:** Sucessos acumulados podem engendrar confiança excessiva, redução da vigilância e normalização de desvios, levando à aceitação progressiva de níveis mais elevados de risco sem que isso seja percebido como deterioração das condições de segurança.

Esses quatro pressupostos são precisamente aqueles em torno dos quais Dekker (2011) organiza "***Drift into Failure"*** (Deriva para Falha): sua leitura de sistemas complexos toma a temporalidade, a racionalidade local, o incrementalismo e o sucesso como precursor de falha como eixos de uma mesma dinâmica de deriva (ver Seção 2.5.3).

2.5.3 Conceitos Fundamentais

Período de Incubação (Turner)

Barry Turner (1978) propôs que desastres são precedidos por um "período de incubação" durante o qual sinais de perigo se acumulam sem serem reconhecidos, interpretados e tratados pelas organizações . Conforme Turner e Pidgeon (1997, p. 72), há uma "acumulação ao longo de um período de tempo de vários eventos que estão em desacordo com a imagem do mundo e seus perigos representada pelas normas e crenças existentes." O modelo compreende seis estágios (Turner & Pidgeon, 1997, pp. 71-72), sintetizados na Figura 2.5.1.





Figura 2.5.1: Modelo dos seis estágios dos *Man-Made Disasters* (Turner). *O Estágio 2 (período de incubação) é o mecanismo distintivo da teoria – fase em que eventos discrepantes das crenças e normas vigentes se acumulam de forma imperceptível. Adaptado de Turner & Pidgeon (1997, pp. 71-72) e Rosness et al. (2010, p. 70).*

Cada estágio é descrito a seguir:

1. **Ponto de partida nocionalmente normal:** situação inicial em que crenças, normas e práticas organizacionais são consideradas adequadas e suficientes para garantir a segurança, baseadas em experiências passadas de sucesso.
2. **Período de incubação:** fase em que sinais de risco, discrepâncias e eventos anômalos se acumulam, sendo ignorados, mal interpretados ou racionalizados, permitindo o desenvolvimento de condições latentes para o desastre.
3. **Evento precipitante**: gatilho que revela a estrutura subjacente de falhas acumuladas, transformando uma situação aparentemente estável em uma condição crítica.
4. **Início (onset):** manifestação do desastre propriamente dito, quando as condições latentes se materializam em um evento adverso.
5. **Resgate e tratamento:** fase de resposta imediata ao evento, envolvendo ações de contenção, mitigação de danos e assistência às vítimas.
6. **Ajuste cultural completo:** reorganização de crenças, normas e práticas organizacionais à luz do evento ocorrido, incorporando lições aprendidas e promovendo mudanças institucionais.

Turner identificou fatores que caracterizam o período de incubação: **rigidez de crenças**, que dificulta a revisão de pressupostos estabelecidos; **fenômeno do**

engodo, no qual a atenção é desviada para problemas secundários; **relutância em considerar cenários críticos**, levando à minimização de riscos emergentes; e **barreiras comunicacionais**, que impedem a circulação eficaz de informações relevantes entre níveis e áreas organizacionais.

Fine-Tuning (Starbuck & Milliken)

Starbuck e Milliken (1988) descreveram o *fine-tuning* como um processo pelo qual engenheiros e gestores perseguem objetivos parcialmente inconsistentes, desempenho, eficiência e segurança, ao mesmo tempo em que aprendem com suas experiências. O ajuste fino reduz progressivamente as probabilidades de sucesso e continua até que ocorra uma falha grave.

O mecanismo central do *fine-tuning* é a retroalimentação positiva gerada pelo sucesso: cada operação bem-sucedida é interpretada como evidência de que o sistema é confiável, justificando novos ajustes que removem redundâncias, reduzem custos ou ampliam a capacidade produtiva. A experiência, que deveria aumentar a cautela, opera paradoxalmente na direção oposta, produz familiaridade e, com ela, complacência. As margens de segurança são consumidas de forma incremental, sem que nenhum passo isolado pareça perigoso.

O processo de *fine-tuning* pode ser compreendido como um mecanismo operacional que contribui para a incubação de acidentes descrita por Turner e para a normalização do desvio proposta por Vaughan. Ao promover ajustes incrementais que reduzem margens de segurança com base em sucessos anteriores, o *fine-tuning* atua como elo entre a acumulação de condições latentes e a aceitação progressiva de desvios como parte da normalidade organizacional. O caso Challenger ilustra o fenômeno: ao longo de 24 lançamentos bem-sucedidos, a NASA e a Thiokol realizaram ajustes sucessivos nas avaliações de risco dos O-rings, cada um localmente justificável, até que o sistema passou a operar em condições que jamais teriam sido aceitas no primeiro lançamento.



Normalização do Desvio (Vaughan)

Diane Vaughan (1996) identificou um processo pelo qual desvios das especificações técnicas tornam-se gradualmente aceitos como normais. O padrão envolve quatro movimentos: (1) um sinal de perigo potencial emerge; (2) engenheiros reconhecem o desvio, mas o reinterpretam à luz de experiências anteriores bem-sucedidas; (3) a aceitação gerencial do desvio como risco operacional aceitável, especialmente quando não há falhas catastróficas associadas; e (4) a incorporação desse novo patamar de desempenho como parte da normalidade organizacional, redefinindo, na prática, o limite do que é considerado seguro.

Nesse contexto, o sucesso repetido apesar da presença do desvio exerce um papel decisivo: reforça a crença de que o sistema continua confiável. Cada operação bem-sucedida reclassifica o desvio, antes visto como sinal de alerta, como evidência empírica de que o risco é controlável, ainda que as condições originais de projeto estejam sendo gradualmente violadas. O que inicialmente representava uma exceção torna-se rotina, e a margem de segurança vai sendo silenciosamente erodida (veja Figura 2.5.2).

A normalização do desvio é sustentada por aquilo que Vaughan denomina *"segredo estrutural"* (*structural secrecy*), a forma como a própria estrutura organizacional fragmenta a informação, distribui responsabilidades e limita a compreensão sistêmica do risco. O conhecimento crítico sobre as falhas potenciais existe dentro da organização, mas encontra-se disperso entre departamentos, níveis hierárquicos e especialidades técnicas, de modo que nenhum ator individual detém uma visão completa das implicações acumuladas dos desvios. Conforme Pidgeon e O'Leary (2000, p. 28) sintetizaram, a cultura da NASA "*provided a way of seeing that was simultaneously a way of not seeing*", as suposições institucionalizadas iluminam alguns perigos enquanto desviam a atenção de outros.

Como consequência, decisões que aumentam o risco sistêmico são tomadas de maneira localmente racional, coerente com os objetivos, incentivos e informações disponíveis a cada nível. Quando a falha catastrófica finalmente ocorre, ela tende a ser interpretada como inesperada, ainda que, retrospectivamente, revele-se o resultado previsível de um longo processo de aceitação incremental do desvio.

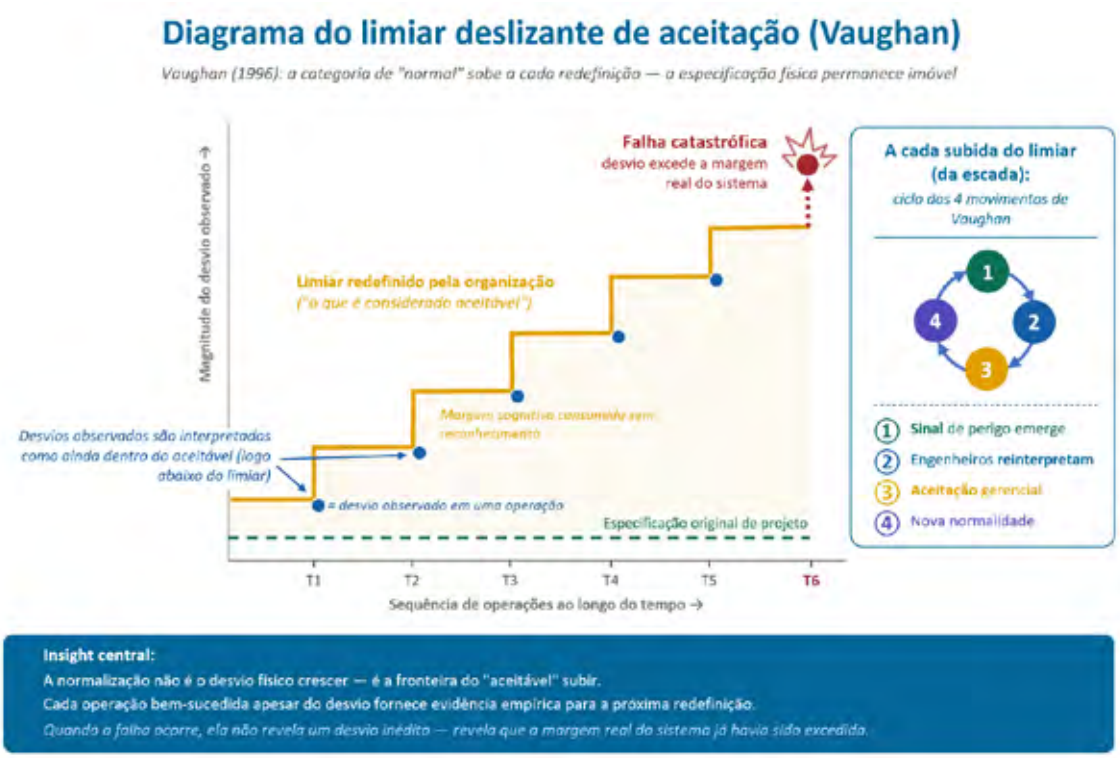


Figura 2.5.2: Normalização do desvio: limiar deslizante de aceitação e ciclo dos quatro movimentos (Vaughan, 1996). A figura integra dois aspectos do mesmo processo. Fonte: *elaboração própria a partir de Vaughan (1996, Caps. 3 e 8).*

Nota: À esquerda, a linha amarela em escada representa o "limiar do aceitável" definido organizacionalmente, redefinido para cima a cada operação bem-sucedida (T1...T6); a linha tracejada verde, abaixo, representa a especificação original de projeto, que permanece imóvel ao longo do tempo. Os pontos azuis marcam desvios observados em cada operação, sempre interpretados como estando "logo abaixo" do limiar então vigente – proximidade que torna a redefinição subsequente plausível para os atores envolvidos. À direita, o painel desdobra o ciclo dos quatro movimentos pelos quais cada subida do degrau ocorre: (1) um sinal de perigo emerge; (2) engenheiros reinterpretam o desvio à luz de experiências bem-sucedidas anteriores; (3) aceitação gerencial do novo patamar como risco operacional aceitável; (4) incorporação como nova normalidade organizacional. O insight central – destacado no rodapé da figura – é que ***a normalização não consiste no desvio físico crescer, mas no limiar do aceitável subir****: a margem real do sistema permanece a mesma, enquanto a margem cognitiva é silenciosamente consumida. O endpoint catastrófico em T6 corresponde ao desfecho específico do caso Challenger, em que o limiar redefinido finalmente excedeu a margem real do sistema; não representa uma inevitabilidade universal da normalização – sistemas podem operar normalizados por longos períodos antes que essa convergência ocorra, ou sem que ela jamais ocorra de forma catastrófica.*

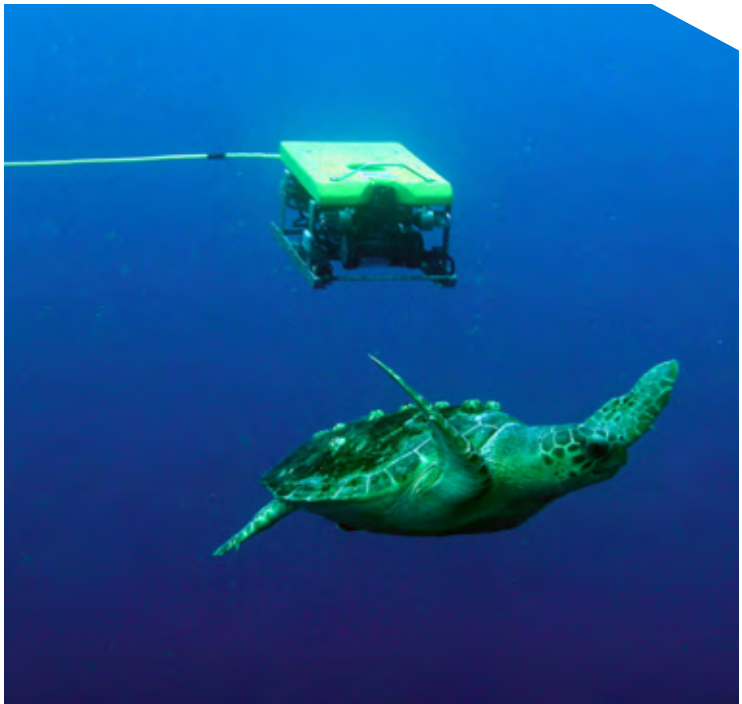
Deriva Prática (Snook)

Scott Snook (2000, p. 186) desenvolveu o conceito de *"deriva prática"* (*practical drift*) para descrever como práticas localmente eficientes, adquiridas por meio da

experiência e mantidas por repetição, substituem gradualmente procedimentos formais. Trata-se de "um desacoplamento incremental da prática em relação aos procedimentos escritos" (Vaughan, 1999, p. 273).

Segundo Snook, existe uma lacuna inevitável entre o "trabalho como imaginado" (*work as imagined*), incorporado em regras, planos e procedimentos, e o "trabalho como realizado" (*work as done*). Para funcionar na prática, os operadores precisam improvisar, adaptar e priorizar, tomando decisões que fazem sentido em seu contexto imediato. Esses ajustes, embora eficazes localmente, introduzem desvios cumulativos em relação ao modelo formal de operação.

A deriva prática não acontece como violação consciente ou negligência deliberada. Pelo contrário, ela se desenvolve porque os desvios *funcionam*: resolvem problemas, aumentam a eficiência e evitam falhas imediatas. O sucesso operacional reforça essas práticas adaptativas, transformando-as em rotina. Com o tempo, o sistema passa a operar em um estado significativamente diferente daquele previsto pelos projetistas, sem que isso seja explicitamente reconhecido como perda de segurança. Snook (2000, p. 186) representou esse processo como uma trajetória de quatro estados sistêmicos: o sistema parte de um projeto formal acoplado por regras (Designed), opera na prática como subunidades desacopladas (*Engineered*), deriva para um estado em que a prática local substitui o procedimento (*Applied*) e, quando subitamente reacoplado por uma demanda externa, falha catastroficamente (*Failed*).



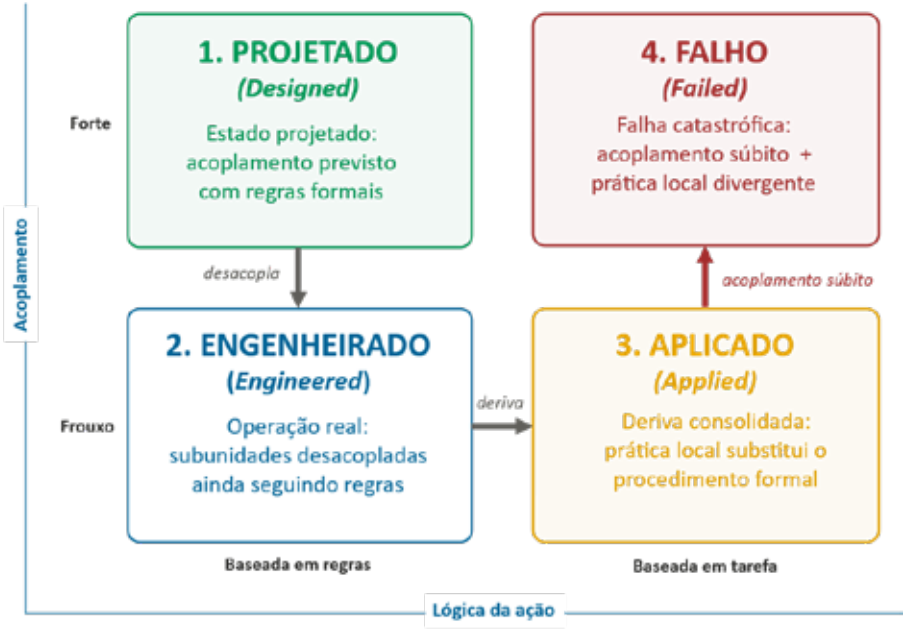


Figura 2.5.3: Os quatro estados sistêmicos da deriva prática de Snook. *O sistema parte do estado projetado (Designed: acoplamento previsto + regras formais), opera como Engineered (subunidades desacopladas, ainda seguindo regras), deriva para Applied (prática local substitui o procedimento) e, ao ser reacoplado subitamente por uma demanda imprevista, alcança Failed. Os números indicam a trajetória teórica da deriva prática rumo à falha catastrófica, não uma cronologia operacional. Adaptado de Snook (2000, p. 186, Fig. 6.5) e Rosness et al. (2010, p. 90, Fig. 13).*

A distinção central entre deriva prática e normalização do desvio é analiticamente significativa: enquanto a normalização do desvio é progressivamente incorporada nas políticas formais da organização, podendo haver documentação, deliberação técnica e aprovação gerencial ao longo do tempo, a deriva prática permanece não documentada e invisível para os níveis hierárquicos superiores, emergindo como *workarounds* locais que preenchem lacunas onde regras e procedimentos não alcançam a complexidade do trabalho real (Dekker, 2019, pp. 258-259).

No estudo do abate acidental de dois helicópteros Black Hawk pelo Exército dos Estados Unidos, caso central de *Friendly Fire* (Snook, 2000), o desastre não foi resultado de erro individual ou quebra explícita de regras, mas da convergência de múltiplas derivas práticas em diferentes partes do sistema: planejamento, vigilância aérea, identificação de alvos e comando. Cada unidade operou de modo coerente com suas metas locais, mas o sistema como um todo perdeu a capacidade de coordenar-se de forma segura. A noção de deriva prática desloca, assim, o foco analítico da pergunta "quem errou?" para "como o sistema passou a operar desse modo".

Os quatro mecanismos descritos incubação, *fine-tuning*, normalização do desvio e deriva prática encontram síntese integradora na formulação de Dekker (2011), que os articula em uma única leitura de sistemas complexos.

Deriva para Falha (Dekker)

A síntese proposta por Dekker (2011) em ***Drift into Failure*** (Deriva para Falha ou Deriva em direção ao Fracasso) ancora-se em uma leitura pós-newtoniana de sistemas complexos. Dekker integrou os frameworks de Turner, Vaughan e Snook com o modelo de migração para fronteiras de segurança de Rasmussen (1997), identificando cinco características recorrentes, operando em paralelo e não sequencialmente, pelas quais sistemas sociotécnicos competentes se afastam gradualmente de seus limites seguros: **escassez e competição, decrementalismo, sensibilidade às condições iniciais, tecnologia indócil e contribuição da estrutura protetiva** (ver Figura 2.5.4). Esta síntese consolidou a tradição como um corpo teórico coerente, superando a fragmentação entre obras publicadas em momentos distintos e com diferentes objetos empíricos.

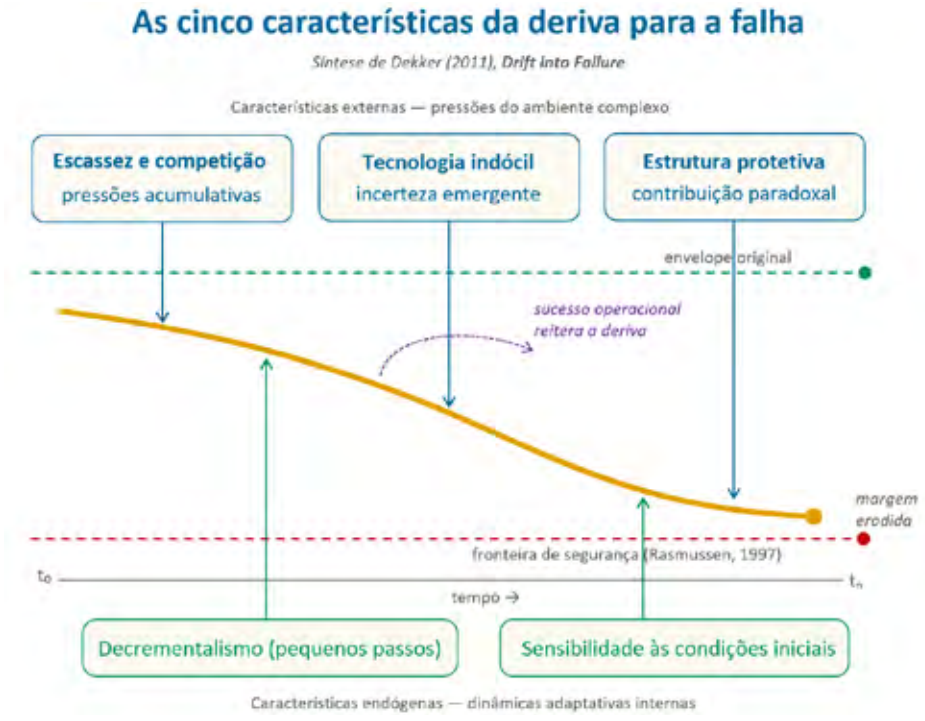


Figura 2.5.4: As cinco características da deriva para a falha (síntese de Dekker, 2011). **Fonte:** *elaboração própria a partir de Dekker (2011, Caps. 3 e 6).*

Nota: As três características externas – escassez e competição, tecnologia indócil e estrutura protetiva – operam como pressões do ambiente complexo em que o sistema está inserido. As duas características endógenas – decrementalismo (pequenos passos) e sensibilidade às condições iniciais – descrevem as dinâmicas adaptativas internas que se acumulam ao longo do tempo. As cinco operam em paralelo, não sequencialmente: nenhum estágio precede outro. A trajetória do sistema migra gradualmente do envelope original (linha tracejada superior) em direção à fronteira de segurança (linha tracejada inferior; cf. Rasmussen, 1997), erodindo margens sem cruzar inequivocamente para a falha – a deriva produz vulnerabilidade aumentada, não desfecho determinístico. O sucesso operacional reiterado retroalimenta positivamente o processo: cada operação bem-sucedida reclassifica desvios como evidência de robustez, reforçando os ajustes que erodem margens. Fonte: elaboração própria a partir de Dekker (2011, Caps. 3 e 6).

Do ponto de vista metodológico, o desafio de detectar proativamente a deriva antes que resulte em falha permanece em aberto (Dekker, 2019). Respostas emergentes na literatura incluem metodologias de análise sistemática do trabalho como realizado versus como imaginado, auditorias de práticas informais e revisões de eventos com atenção explícita a padrões de aceitação incremental. A questão não é primariamente técnica, mas organizacional: requer estruturas que permitam à liderança ver o que os sistemas de reporte convencionais são estruturalmente incapazes de capturar.

2.5.4 Base Empírica

As perspectivas de dependência de trajetória foram construídas a partir de estudos empíricos aprofundados de desastres reais, envolvendo análises históricas, etnográficas e documentais.

Turner (1978) analisou sistematicamente 84 relatórios de inquéritos públicos britânicos, compreendendo 19 relatórios sobre acidentes em mineração (incluindo Aberfan e a mina Cambrian Colliery), 33 sobre explosões de caldeiras e 32 sobre naufrágios marítimos, além de casos miscelâneos como o incêndio de Summerland e a explosão química de Flixborough (Bills, 2023; Rosness et al., 2010). Dentre esse conjunto, Turner estudou três acidentes em profundidade para elaborar sua teoria: o colapso da pilha de rejeitos de mineração em Aberfan, País de Gales (1966, 144 mortos - a maioria crianças); a colisão em cruzamento ferroviário em Hixon (1968); e o incêndio no complexo de lazer Summerland na Ilha de Man (1973, 50 mortos). A partir dos 13 relatórios de inquéritos que constituíram seu corpus central de análise - registrando 351 fatalidades -, Turner identificou padrões recorrentes de falhas informacionais e organizacionais, posteriormente testados nos demais relatórios do conjunto mais amplo (Bills, 2023).

Starbuck e Milliken (1988) examinaram o desastre do ônibus espacial Challenger por meio de análise documental e entrevistas com engenheiros e gestores da NASA e da Thiokol. Demonstraram como decisões de ajuste incremental foram adotadas ao longo do tempo em resposta a pressões de desempenho e interpretações seletivas da experiência, reduzindo progressivamente as margens de segurança sem que isso fosse percebido como aumento de risco.

Vaughan (1996) conduziu estudo etnográfico-histórico de longa duração sobre o programa do ônibus espacial, baseado na análise de milhares de documentos internos, relatórios técnicos, comunicações organizacionais e mais de uma centena de entrevistas. Seu trabalho evidenciou o processo de normalização do desvio e o conceito de "segredo estrutural", demonstrando como a fragmentação organizacional limita a percepção sistêmica do risco acumulado ao longo de nove anos de operação com os O-rings do Challenger. O acidente do ônibus espacial Columbia (2003) foi posteriormente analisado pelo Columbia Accident Investigation Board (CAIB) utilizando explicitamente o framework de normalização do desvio de Vaughan, identificando padrões análogos, desta vez em relação aos danos causados por detritos de espuma na asa, dezessete anos após o Challenger (CAIB, 2003; Woods, 2006).



Snook (2000) investigou o abate acidental de dois helicópteros Black Hawk pelo Exército dos Estados Unidos por meio de análise detalhada de documentos, comunicações e mais de 250 entrevistas. Seu estudo demonstrou como adaptações locais, desenvolvidas para lidar com demandas operacionais reais, produziram múltiplas derivas práticas que, ao se acumularem, resultaram na perda de alinhamento sistêmico e na falha catastrófica.

Dekker (2011) sintetizou esses e outros estudos de caso em diferentes setores de alto risco, aviação, saúde, energia e defesa, para desenvolver o conceito de *drift into failure*. Sua abordagem baseia-se em extensa revisão empírica e análise comparativa de sistemas sociotécnicos complexos, identificando mecanismos recorrentes pelos quais adaptações locais, pressões organizacionais e decisões racionalmente justificáveis levam à erosão gradual das margens de segurança.

Em conjunto, esses estudos fornecem uma base empírica robusta e convergente, evidenciando que acidentes organizacionais emergem de processos históricos e sociais que se desenvolvem no funcionamento normal dos sistemas, e não de falhas isoladas ou decisões excepcionalmente inadequadas.

2.5.5 Modelo de Causalidade de Acidentes

Estas perspectivas oferecem modelos complementares que enfatizam processos graduais:

- **Incubação (Turner)**: Sinais de perigo acumulam-se não percebidos devido a rigidez de crenças, barreiras comunicacionais e relutância em temer o pior. Durante a fase de incubação, anomalias técnicas, quase-acidentes e advertências convivem com crenças organizacionais consolidadas, permitindo que condições latentes se acumulem até que um evento precipitante revele a fragilidade do sistema.
- **Fine-tuning (Starbuck & Milliken):** Mudanças incrementais são introduzidas em resposta a experiências anteriores, à medida que gestores e especialistas ajustam operações para otimizar desempenho, custos ou eficiência. A organização aprende seletivamente com sucessos passados, reinterpretando riscos como aceitáveis, o que reduz progressivamente as margens reais de segurança.
- **Normalização do desvio (Vaughan):** Aceitação gradual de padrões de desempenho que divergem das especificações originais, à medida que desvios não produzem consequências imediatas negativas. Com o tempo, o que inicialmente era visto como anormal passa a ser redefinido como normal, sustentado por sucessos repetidos, pressões organizacionais e pelo "segredo estrutural" que impede a percepção sistêmica do risco acumulado.
- **Deriva prática (Snook):** Adaptações locais e pragmaticamente racionais no trabalho cotidiano afastam o "trabalho como realizado" do "trabalho como imaginado", sem que isso seja percebido como violação consciente. Essas adaptações funcionam no curto prazo, são reforçadas pelo sucesso operacional e, de forma cumulativa, deslocam o sistema para além de seus limites seguros.

Turner e Pidgeon (1997, pp. 180-181) propuseram que a distinção de Reason entre falhas ativas e latentes "pode ser vista como uma divisão do período de incubação do desastre em duas fases ligadas, mas conceitualmente diferentes", sugerindo complementaridade entre estas perspectivas e o modelo de Reason, não uma relação de antagonismo. Falhas latentes e ativas não são categorias separadas, mas diferentes expressões temporais do mesmo fenômeno socio-técnico: as falhas latentes são produzidas, mantidas e reforçadas por processos organizacionais contínuos; as falhas ativas representam o momento final em que um sistema já fragilizado se torna incapaz de absorver variações adicionais.

Um insight central de Dekker (2011) é que a deriva para falha é incremental, cada passo é uma pequena partida da norma anterior que não parece digna de nota ou relato. É exatamente esse incrementalismo que torna a distinção entre o normal e o anormal tão difícil para quem está dentro do sistema: «se a diferença entre o que ‹deveria ser feito› e o que é feito com sucesso hoje é mínima, então esse leve afastamento da norma não merece ser comentado ou reportado» (Dekker, 2019, p. 257) – especialmente se gera ganho produtivo.

2.5.6 Forças e Limitações

Forças

- **Framework explanatório poderoso:** Explica como organizações "esquecem de ter medo" por meio de processos aparentemente racionais e como condições para acidentes se desenvolvem no funcionamento normal, não em disfunções excepcionais.
- **Fundação empírica rica:** Baseada em estudos de caso detalhados com reconstrução minuciosa de contextos organizacionais reais – não em modelos abstratos ou experimentos controlados.
- **Dimensão temporal:** Adiciona perspectiva histórica frequentemente ausente em teorias focadas em eventos proximais, tornando visível o processo de construção do risco ao longo do tempo.
- **Insight sociológico:** Explica comportamento organizacional sob pressão de formas que ressoam com a experiência prática, sem recorrer a pressupostos de incompetência, má-fé ou irracionalidade dos atores.

Limitações

- **Dificuldade de previsão:** Oferecem capacidade preditiva limitada sobre quando acidentes ocorrerão; é difícil determinar prospectivamente quando a incubação levará a um acidente e qual será o evento precipitante.
- **Orientação prescritiva limitada:** Oferecem mais explicação do que prescrição clara para prevenção; os mecanismos que tornam a deriva visível retrospectivamente são precisamente os que a tornam invisível no momento em que ocorre.
- **Viés retrospectivo:** Padrões são mais facilmente identificáveis após acidentes; detectar incubação em tempo real permanece um desafio metodológico e organizacional em aberto.

2.5.7 Debates e Controvérsias

Uma questão recorrente é a relação entre a normalização do desvio e a deriva prática. Embora ambas descrevam processos de afastamento gradual de padrões, diferem em aspecto crucial: na normalização, o desvio pode ser formalmente reconhecido pela organização e reclassificado como risco operacional aceitável, podendo haver documentação, deliberação técnica e aprovação gerencial ao longo do tempo; na deriva prática, as adaptações não chegam a ser formalizadas ou percebidas pelos níveis hierárquicos superiores, ocorrendo exclusivamente como ajustes locais, fora da estrutura formal de documentos, preenchendo lacunas onde procedimentos não alcançam a complexidade do trabalho real (Dekker, 2019, pp. 258-259).

Outro debate central envolve a possibilidade de detecção desses processos por meio dos mecanismos organizacionais convencionais. Dekker (2019, pp. 259-260) demonstra que sistemas de reporte de incidentes são estruturalmente incapazes de capturar a deriva e a normalização, não porque as pessoas temam reportar, mas porque as adaptações que constituem esses processos não são reconhecidas como incidentes por quem as vive. São, precisamente, *workarounds* (soluções alternativas), limitações, ajustes ou adaptações percebidas como parte normal do trabalho cotidiano: não se qualificam como ocorrências reportáveis e, portanto, simplesmente não chegam ao sistema. A normalização que acompanha a

deriva dissolve a própria categoria de "incidente" antes que qualquer reporte seja possível. Isso levanta uma implicação importante para a indústria: a ausência de registros no sistema de reporte não é evidência de ausência de deriva, pode ser, ao contrário, evidência de que a deriva já se consolidou.

2.5.8 Desenvolvimentos Recentes

Nas últimas décadas, a tradição da dependência de trajetória consolidou-se teoricamente, recebeu validação empírica independente e expandiu-se para novos setores. A consolidação teórica mais significativa foi a síntese de Dekker (2011) em "***Drift into Failure"*** (Deriva para Falha), apresentada na Seção 2.5.3 (Conceitos Fundamentais), à qual se somam validações empíricas, releituras genealógicas e a difusão dos conceitos para além da aviação.



Um desenvolvimento empírico de grande relevância foi a aplicação explícita do framework de normalização do desvio de Vaughan ao desastre do ônibus espacial Columbia (2003) pelo Columbia Accident Investigation Board (CAIB, 2003). O relatório identificou padrões de aceitação incremental de risco, em relação aos danos causados por detritos de espuma na asa, estruturalmente análogos aos observados no Challenger dezessete anos antes. Esta replicação em contexto independente, conduzida por investigadores que não eram os autores originais da teoria, conferiu ao conceito de normalização do desvio uma validade empírica particularmente robusta.

Uma contribuição recente relevante é a reavaliação do legado de Barry Turner por Bills (2023), que documenta o impacto desproporcional de *Man-Made Disasters* (1978) sobre a ciência da segurança contemporânea e a relativa invisibilidade de Turner em relação aos autores que ele influenciou diretamente, especialmente Reason, Perrow e Vaughan. Este trabalho contribui para consolidar a genealogia teórica da família de dependência de trajetória e para reconhecer sua precedência em relação a desenvolvimentos posteriores que frequentemente citam apenas as sínteses mais recentes.

A tradição expandiu-se também para além da aviação e da indústria de processos. No setor de óleo e gás, a explosão do Deepwater Horizon (2010) mobilizou extensamente os frameworks desta tradição, especialmente a incubação de Turner e a normalização de Vaughan, para explicar como anos de operação aparentemente bem-sucedida precederam a falha catastrófica. Na área da saúde, pesquisadores aplicaram o conceito de normalização do desvio a contextos clínicos, demonstrando como práticas assistenciais se afastam progressivamente de protocolos sem que isso seja percebido como declínio de segurança. A generalidade dos mecanismos identificados por Turner, Vaughan e Snook tem-se revelado, assim, uma das principais forças da tradição.

2.5.9 Implicações para a Indústria de Energia

As perspectivas de dependência de trajetória são particularmente relevantes para a indústria de óleo e gás, onde pressões comerciais intensas, complexidade organizacional, longos períodos sem acidentes e crenças consolidadas e pouco questionadas criam condições propícias para normalização e deriva.

- **Vigilância contra normalização:** Manter ceticismo ativo sobre condições que se tornaram "normais" mas divergem de especificações originais, especialmente após longos períodos de operação sem incidentes graves.
- **Atenção à lacuna do trabalho-prescrito/real:** Monitorar ativamente a divergência entre procedimentos formais e práticas reais, com o intuito de aprender com o trabalho real e verificar a aplicabilidade e a necessidade de revisão dos procedimentos formais.
- **Gestão de pressões de produção:** Reconhecer como pressões de eficiência e competitividade encontram caminho para decisões operacionais por meio de ajustes incrementais, cada um localmente justificável, mas cujo efeito cumulativo é a erosão das margens de segurança.
- **Cultura de inquietude crônica:** Manter "medo saudável" mesmo após longos períodos de operação bem-sucedida, reconhecendo que o sucesso acumulado é o mecanismo que gera complacência.
- **Cultura de segurança psicológica:** Propiciar um ambiente seguro para apontamentos e sugestões de melhoria dos processos atuais, sem pos-

sibilidade de retaliação – condição necessária para que sinais fracos cheguem à liderança antes de se tornarem eventos.

- **Aprendizagem de quase-acidentes:** Tratar quase-acidentes como janelas para condições incubadas, não como evidência de sucesso ou "sorte". O quase-acidente revela que o sistema já opera próximo de seus limites.
- **Consciência sobre o viés do histórico de sucesso na tomada de decisão:** Reconhecer como a acumulação de sucessos anteriores influencia a percepção de risco, tornando o próximo passo incremental sempre justificável, é condição para que decisores resistam à lógica do *fine-tuning* e mantenham ou ampliem as margens de segurança, em vez de consumi-las gradualmente.

2.5.10 Quadro-Resumo: Perspectivas de Dependência de Trajetória

Essas perspectivas convergem ao demonstrar que, em sistemas sociotécnicos complexos, o acidente não representa uma ruptura da normalidade, mas a consequência lógica de uma trajetória organizacional construída ao longo do tempo.

Dimensão	Perspectivas de Dependência de Trajetória
Período de Surgimento	1978 (Turner) a 2000s (sínteses contemporâneas).
Principais Autores	Barry Turner, Diane Vaughan, Scott Snook, William Starbuck, Frances Milliken, Sidney Dekker.
Fundamento Teórico	Sociologia organizacional, estudos etnográficos de desastres. Ênfase em processos temporais e históricos.
Pressuposto Central	Acidentes têm história; emergem de decisões incrementais que parecem racionais no momento, mas acumulam vulnerabilidades ao longo do tempo.
Concepção de Risco	Risco como aceitação gradual – desvios são incrementalmente normalizados; sucesso passado engendra confiança que contribui para deriva futura.

Dimensão	Perspectivas de Dependência de Trajetória
Visão da Contribuição Humana	Decisões fazem sentido no contexto; não há "decisões monumentalmente ruins" – apenas pequenos passos incrementais localmente racionais.
Estratégias de Controle	Vigilância contra normalização; atenção à lacuna prescrito/real; cultura de inquietude crônica; aprendizagem de quase-acidentes
Modelo de Causalidade	Quatro lentes teóricas complementares: Incubação (Turner), Fine-tuning (Starbuck & Milliken), Normalização do desvio (Vaughan) e Deriva prática (Snook) – cada uma iluminando um aspecto distinto do mesmo processo de erosão gradual da segurança, integradas por Dekker (2011) na leitura de sistemas complexos.
Forças	Framework explanatório poderoso; fundação empírica rica; dimensão temporal; insight sociológico profundo.
Limitações	Dificuldade de previsão; orientação prescritiva limitada; viés retrospectivo; paradoxo do sucesso.



Referências da Seção 2.5

Bills, K. (2023). Barry Turner: The under-acknowledged safety pioneer. Safety, 9(4), 68. https://doi.org/10.3390/safety9040068.

Columbia Accident Investigation Board. (2003). Report of the Columbia Accident Investigation Board (Vol. 1). NASA.

Dekker, S. W. A. (2011). Drift into failure: From hunting broken components to understanding complex systems. Ashgate.

Dekker, S. W. A. (2019). *Foundations of safety science: A century of understanding accidents and disasters*. Routledge/CRC Press

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. Safety Science, 34(1-3), 15–30. https://doi.org/10.1016/S0925-7535(00)00004-7

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2-3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Snook, S. A. (2000). Friendly fire: The accidental shootdown of U.S. Black Hawks over Northern Iraq. Princeton University Press.

Starbuck, W. H., & Milliken, F. J. (1988). Challenger: Fine-tuning the odds until something breaks. Journal of Management Studies, 25(4), 319–340. https://doi.org/10.1111/j.1467-6486.1988.tb00040.x.

Tinmannsvik, R. K., & Wærø, I. (2010). Organisational accidents and resilient organisations: Six perspectives (Rev. 2, Relatório SINTEF A17034). SINTEF.
Turner, B. A. (1978). Man-made disasters. Wykeham Publications.

Turner, B. A., & Pidgeon, N. F. (1997). Man-made disasters (2ª ed.). Butterworth-Heinemann.

Vaughan, D. (1996). The Challenger launch decision: Risky technology, culture, and deviance at NASA. University of Chicago Press.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. Annual Review of Sociology, 25(1), 271–305. https://doi.org/10.1146/annurev.soc.25.1.271.

Woods, D. D. (2006). Essential characteristics of resilience for organizations. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), Resilience engineering:

Concepts and precepts. Ashgate.




Sea Tel
BRAVA



Parte III

Ecossistema de fatores humanos e abordagens complementares

Autor: Josué E. Maia França



Conforme apresentado na Parte I, Fatores Humanos constitui um **campo da ciência interdisciplinar** que integra conhecimentos de múltiplas áreas para compreender e otimizar o desempenho dos sistemas sociotécnicos. Esta natureza interdisciplinar – que dialoga com psicologia, engenharia, sociologia, ciências cognitivas e organizacionais, entre outras – impõe tanto um desafio quanto uma oportunidade: a superação de abordagens fragmentadas e departamentalizadas em favor de uma visão holística e integrada.

O conceito de **Ecossistema de Fatores Humanos** (França, 2024) oferece uma metáfora integradora para esta visão. Assim como em um ecossistema biológico, onde organismos diversos coexistem, interagem e se adaptam continuamente ao ambiente, as disciplinas e as abordagens que compõem o campo são dinâmicas, interdependentes e em constante adaptação à realidade dos sistemas sociotécnicos. Cada disciplina ou abordagem é um bioma, com suas espécies, seu solo e sua história, que se conecta aos demais por meio de raízes conceituais e práticas. Na metáfora proposta, "eco" representa as características distintivas de cada disciplina; "system" representa suas convergências e sobreposições.

As **perspectivas teóricas fundamentais** apresentadas na Parte II – NAT, HRO, Rasmusseniana, Engenharia de Resiliência e Dependência de Trajetória – constituem componentes essenciais deste ecossistema, cada qual com seus pressupostos, modelos explicativos e ferramentas analíticas próprias. As **abordagens complementares** apresentadas nesta Parte III ampliam o repertório disponível, frequentemente integrando insights de múltiplas perspectivas teóricas e dialogando com outras disciplinas do ecossistema. Juntas, oferecem às organizações

um conjunto diverso de lentes interpretativas e ferramentas práticas para sua **jornada de aprendizagem em Fatores Humanos**.

É importante ressaltar que a distinção entre "perspectivas teóricas fundamentais» (Parte II) e «abordagens complementares" (Parte III) não implica uma dicotomia entre teoria e prática. Todas as abordagens aqui apresentadas possuem fundamentação teórica e implicações práticas; a diferença reside primariamente em seu escopo e propósito: enquanto as perspectivas da Parte II oferecem frameworks explanatórios abrangentes sobre a natureza dos acidentes e da segurança, as abordagens da Parte III frequentemente integram insights de múltiplas perspectivas em metodologias e práticas mais diretamente aplicáveis a contextos específicos.

Conforme Le Coze (2024), a gestão de segurança requer pragmatismo, não dogmatismo. O problema surge quando diferentes abordagens são tratadas como ilhas, como se competissem entre si por relevância ou autoridade. Não se trata de diluir saberes distintos em um caldo genérico, mas de reconhecer **zonas de contato** – pontos de convergência e potenciais de sinergia entre áreas que, apesar de suas especificidades metodológicas, podem ser articuladas de forma complementar. Como em uma floresta mista, a diversidade pode gerar resiliência, adaptação e inovação.

As seções seguintes detalham o conceito de Ecossistema de Fatores Humanos e apresentam as abordagens complementares selecionadas pelo GT Fatores Humanos da ABESPetro, consideradas prioritárias para a indústria de energia brasileira, tanto por sua relevância conceitual quanto por sua aplicabilidade no contexto regulatório: Aprendizagem com Eventos e Investigação de Acidentes, Cultura Justa e Accountability, HRA e HFE, entre outras.

3.1 Ecossistema de Fatores Humanos

Autor: Josué E. Maia França

3.1.1 Caracterização e Disciplinas do Ecossistema

As disciplinas que compõem o Ecossistema de Fatores Humanos são **amorfas, dinâmicas e em constante adaptação** à realidade dos sistemas sociotécnicos. Conforme Dekker (2019), sistemas complexos operando sob pressão competitiva devem atender simultaneamente a múltiplos objetivos conflitantes, sempre com recursos limitados. São as pessoas, em todos os níveis da organização, que reconciliam estas demandas conflitantes e mantêm unidos sistemas inerentemente imperfeitos. A segurança não é propriedade estática, mas sim criação dinâmica e contínua por meio da prática.

Entre as principais disciplinas e abordagens que compõem este ecossistema, destacam-se (França, 2024): Novas Visões de Segurança (Safety-II, Safety Differently, HOP), Confiabilidade Humana (HRA – Human Reliability Analysis), Engenharia de Fatores Humanos (HFE – Human Factors Engineering), Segurança de Processo, Análise de Risco, Ergonomia, Análise de Acidentes e Sistemas de Gestão.

A representação visual do ecossistema (Figura 3.1.1) evidencia uma característica importante: a lacuna nos sistemas de gestão. Esta lacuna reflete a necessidade constante de adaptar e evoluir os sistemas de gestão às demandas reais dos locais de trabalho – evidenciada pela distinção entre Trabalho como Imaginado (WAI) e Trabalho como Realizado (WAD). Nenhum sistema de gestão, por mais sofisticado que seja, consegue capturar completamente a complexidade e a variabilidade do trabalho real; a lacuna representa esta incompletude inerente e a necessidade de aprendizagem e adaptação contínuas.

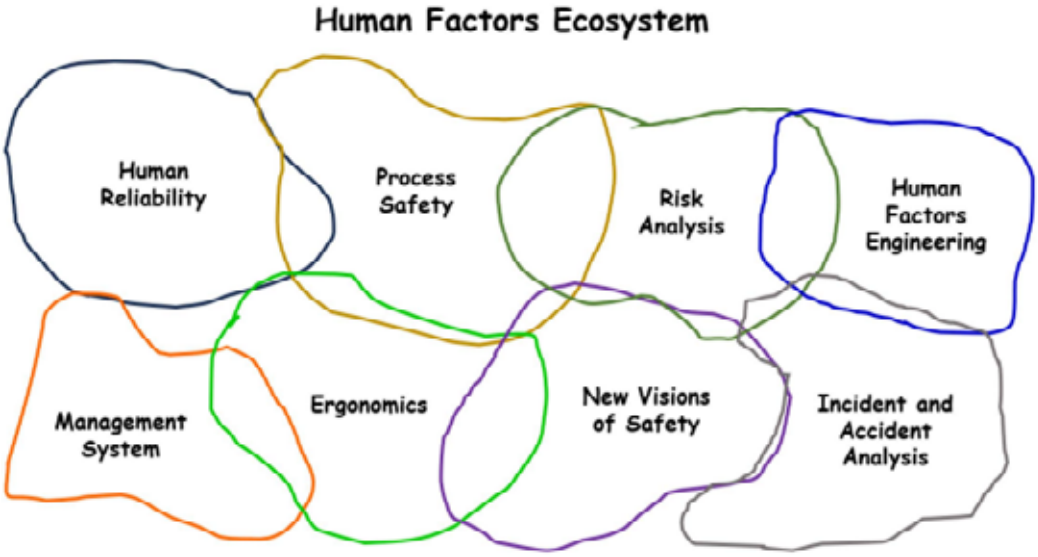


Figura 3.1.1: Representação visual do conceito de Ecossistema de Fatores Humanos. **Fonte:** França (2024).

O valor do conceito de ecossistema reside precisamente na identificação de **convergências e complementaridades** entre disciplinas que, tradicionalmente, são tratadas de forma segregada nas organizações. Por exemplo, a compreensão do erro humano conecta HRA, Ergonomia Cognitiva e as Novas Visões de Segurança; a análise de acidentes dialoga com todas as perspectivas teóricas da Parte II; e a Engenharia de Fatores Humanos integra princípios de Ergonomia, Análise de Risco e Segurança de Processo.



Referências da Seção 3.1

Dekker, S.W.A (2019). Foundations of Safety Science: A Century of Understanding Accidents and Disasters. CRC Press. https://doi.org/10.4324/9781351059794

França, J. E. M. (2024). Human factors ecosystem – How human performance and process safety builds the energy transition and a low-carbon future for O&G industry (SPE-220793-MS). Society of Petroleum Engineers. https://doi.org/10.2118/220793-MS

Le Coze, J. C. (2024). Evolution of safety [Apresentação]. Rio de Janeiro.

3.2 Aprendizagem com Eventos e Investigação de Acidentes

Autor: Rafael Ceni de Almeida

Revisão: Caroline Bastos Capaverde

3.2.1 Dois modos de aprender: o Reativo e o Proativo

A capacidade de uma organização aprender representa um dos pilares fundamentais da segurança e da eficiência operacional em sistemas complexos. Essa aprendizagem pode ocorrer de duas formas fundamentalmente distintas: **reativamente**, após eventos indesejados, ou **proativamente**, por meio do estudo de como o trabalho cotidiano cria sucesso e segurança. As duas formas diferem no que observam e em que direção olham: a aprendizagem reativa examina as falhas depois que ocorrem, voltando-se ao passado; a proativa observa o trabalho normal enquanto ele acontece, voltando-se ao futuro, para antecipar como o risco se transforma.

Esta seção sustenta uma tese. **Aprender com eventos não se reduz a extrair causas de falhas passadas.** Como o erro humano é sintoma – e não causa – de vulnerabilidades sistêmicas mais profundas (Woods et al., 2010; Dekker, 2014a), a aprendizagem reativa é necessária, porém limitada e sistematicamente enviesada. O progresso em segurança depende de deslocar o centro de gravidade da aprendizagem retrospectiva – *por que algo deu errado* – para a aprendizagem situada e proativa – *como a prática cria segurança no trabalho cotidiano*. Em síntese: **segurança não é algo que um sistema tem, mas algo que um sistema faz.**

Esse deslocamento apoia-se em duas tradições epistemológicas complementares da aprendizagem organizacional (Antonello & Godoy, 2010). A **tradição cognitivo-reflexiva** (Argyris & Schön, 1978), dominante por décadas, conceitua o conhecimento como posse cognitiva: algo a ser extraído, codificado, armazenado e transferido entre níveis organizacionais – aprender é adquirir, distribuir e institu-

cionalizar ***conhecimento-como-conteúdo***. Nessa tradição, distingue-se a aprendizagem de ***single-loop***, na qual a organização detecta e corrige desvios sem questionar as premissas e os valores que governam sua ação, da aprendizagem de ***double-loop***, na qual as próprias premissas, normas e objetivos que orientam o comportamento são revistos e modificados (Argyris & Schön, 1978).

A **abordagem baseada na prática** (*practice-based approach*), desenvolvida por Gherardi (2006, 2012) e Gherardi e Nicolini (2000a, 2002a), propõe uma reorientação ontológica: o conhecimento é o *knowing-in-practice*[1] – uma realização coletiva, situada e inseparável das práticas concretas de trabalho –, e não uma posse individual. Aprender, nessa perspectiva, é transformar continuamente a maneira como uma comunidade de praticantes faz as coisas em conjunto – mais do que adquirir informação (Gherardi & Nicolini, 2000a). Este capítulo integra contribuições das duas tradições.

Esse reenquadramento começa por reconhecer o estatuto do erro humano. Organizações de menor confiabilidade tendem a reagir às falhas com a busca por culpados, enquanto organizações mais resilientes utilizam tanto os eventos adversos quanto as operações bem-sucedidas como oportunidades de aprendizado sistêmico; seguem investindo na antecipação do potencial mutável de falha, em vez de tomar o sucesso passado como razão para a confiança (Woods et al., 2010). Se os erros são uma forma de informação sobre o funcionamento do sistema, então constituem base para aprendizagem, ainda que sejam apenas parte da história.

> *"Se rotulamos eventos como 'erro humano' e paramos aí, o que aprendemos? A resposta é: muito pouco. O rótulo 'erro humano' é um julgamento feito em retrospectiva"* (Woods et al., 2010).

A seção desenvolve essa tese em três movimentos. O **primeiro** examina a aprendizagem reativa – sua necessidade, mas também as barreiras emocionais e organizacionais, os vieses cognitivos e os mecanismos de distanciamento que a limitam – e

1 Mantém-se o termo *knowing-in-practice* no original. Em inglês, conhecer é um substantivo verbal que marca a natureza processual, situada e contínua do conhecer-na-prática. Ao longo do texto, quando traduzido, adota-se o infinitivo substantivado ("o conhecer"/"o saber"), que preserva esse caráter verbal. Reserva-se "conhecimento" (*knowledge*) para a concepção de conhecimento como posse ou conteúdo, característica da tradição cognitivo-reflexiva (Gherardi, 2006; Antonello & Godoy, 2010).

culmina na evolução dos modelos de investigação, do linear ao sistêmico. O **segundo** apresenta a virada proativa: o estudo do trabalho normal (Safety-II), a Engenharia de Resiliência e sua operacionalização por meio de um repertório de métodos, entre os quais as Equipes de Aprendizagem e Melhoria. O **terceiro** trata das condições organizacionais que habilitam ambos os modos e sintetiza, em dez passos, o que a pesquisa ensina sobre como sistemas complexos falham e aprendem.

APRENDER COM A FALHA: A APRENDIZAGEM REATIVA E SEUS LIMITES

3.2.2 Aprendizagem Reativa: Barreiras ao Aprender com Falhas

A aprendizagem reativa é a forma mais reconhecível de aprendizado organizacional: parte de um evento indesejado já ocorrido e busca compreendê-lo para evitar sua repetição. É indispensável – nenhuma organização madura prescinde de investigar seus acidentes –, mas opera sob condições que a tornam frágil. Antes de examinar seus métodos, é preciso reconhecer as barreiras que se interpõem entre o evento e aquilo que dele efetivamente se aprende.

Quando uma organização experimenta um incidente, existem consequências reais, tangíveis e por vezes trágicas que criam barreiras significativas ao processo de aprendizagem. Woods et al. (2010) identificam diversas barreiras:

- As consequências negativas são emocionais e perturbadoras para todos os envolvidos;
- A falha gera pressão de diferentes stakeholders para resolver a situação rapidamente;
- Uma causa clara e compreensível ajuda os stakeholders a seguir em frente após uma tragédia;
- Gerenciamento de responsabilidade financeira para amenizar as consequências e perdas;
- Desejo de retribuição por parte de alguns stakeholders e processos de defesa contra ações punitivas;
- Confrontar dissonâncias e mudar conceitos e formas de agir é doloroso e custoso em sentidos não econômicos.

Essas barreiras são tão complexas e sutis quanto as circunstâncias que cercam a própria falha. Como acidentes sempre envolvem múltiplos contribuintes, a decisão de focar em um ou outro do conjunto, e portanto, o que será aprendido, é amplamente determinada socialmente. Quando essa determinação social é capturada pela lógica da identificação de culpados, cristaliza-se em mecanismo organizacional o fenômeno que a Seção 3.3.8 desenvolve como captura punitiva do sistema de *accountability* (Catino, 2008; Parris, 2025).

Histórias Primárias versus Histórias Secundárias

As histórias primárias (*first stories*), enviesadas pelo conhecimento do resultado, são relatos simplificados que atribuem a causa a fatores proximais, geralmente o "erro humano". Aparecem na imprensa e dirigem reações públicas, legais e regulatórias. Em contraste, as histórias secundárias (*second stories*) revelam os múltiplos contribuintes que criam as condições para os erros, permitindo ver como o sistema se move em direção a acidentes, movimento que, em geral, é bloqueado. É por meio dessas percepções mais profundas que a aprendizagem ocorre e o processo de melhoria começa (Woods et al., 2010).

Tabela 3.2.1: Contraste entre Histórias Primárias e Secundárias

Histórias Primárias	Histórias Secundárias
Erro humano é visto como causa da falha.	Erro humano é visto como efeito de vulnerabilidades sistêmicas mais profundas.
Dizer o que as pessoas deveriam ter feito é satisfatório para descrever a falha.	Dizer o que deveriam ter feito não explica por que fazia sentido fazerem o que fizeram.
Pedir às pessoas que sejam mais cuidadosas fará o problema desaparecer.	Buscar continuamente as próprias vulnerabilidades fará a segurança melhorar.

Fonte: *Adaptado de Woods et al. (2010)*

3.2.3 Vieses Cognitivos na Investigação de Acidentes

A aprendizagem reativa não é limitada apenas por barreiras emocionais e organizacionais: é também distorcida por vieses cognitivos sistemáticos, que operam silenciosamente sobre quem investiga. Três deles são particularmente relevantes na análise de acidentes.

Viés de Retrospectiva (Hindsight Bias)

Saber como a história terminou muda a forma como enxergamos o seu começo. Esse é o viés de retrospectiva: uma vez conhecido o resultado, não conseguimos mais desconhecê-lo (Dekker, 2014a). Dekker propõe uma imagem útil, a do túnel. Quem vivia a situação estava dentro do túnel, olhando para a frente, cercado de incerteza, sem saber como as coisas terminariam. O investigador, depois do evento, observa o túnel de fora e de cima, já conhecendo a saída. Dessa posição privilegiada, três distorções se instalam quase automaticamente: o que era uma situação confusa e ambígua passa a parecer uma sequência simples e linear; sinais que, no momento, eram apenas ruído entre muitos outros passam a parecer avisos óbvios que "deveriam ter sido vistos"; e pequenas adaptações que faziam sentido na hora passam a parecer violações evidentes. O resultado é um julgamento sobre o que as pessoas deveriam ter feito, que pouco explica o que de fato aconteceu. Uma técnica para atenuar o viés é pedir que os avaliadores expliquem como cada desfecho possível poderia ter ocorrido – uma postura de "advogado do diabo" (Woods et al., 2010). Mais fundamentalmente, a tarefa do investigador é reconstruir a visão de dentro do túnel (Dekker, 2014a).

Raciocínio Contrafactual

O raciocínio contrafactual consiste em comparar o que de fato aconteceu com um mundo hipotético que teria dado certo (Hilton, 1990). Ao explicar um evento, é quase irresistível listar tudo o que as pessoas poderiam ter feito para evitá-lo: "se apenas tivessem checado o alarme", "se apenas tivessem parado a operação". O problema é que esse mundo hipotético não existia para quem estava na situação. Os contrafactuais descrevem bifurcações que só se tornam visíveis depois,

quando já se conhece o resultado; dizem o que as pessoas deixaram de fazer, mas não porque fazia sentido fazer o que fizeram (Dekker, 2014a). Em outras palavras, o raciocínio contrafactual fala da realidade do investigador, que conhece o desfecho, e não da realidade de quem agiu.

Racionalidade Local

O princípio da racionalidade local sustenta que as pessoas fazem o que faz sentido para elas, dado o seu conhecimento, os seus objetivos, o seu foco de atenção e os recursos de que dispõem naquele momento (Dekker, 2014a; Woods et al., 2010). Quase ninguém vai ao trabalho com a intenção de fazer um mau trabalho ou de se acidentar. Por isso, a pergunta do investigador não deveria ser "onde as pessoas erraram?", mas "por que as suas avaliações e ações faziam sentido para elas naquele momento?" (Dekker, 2014a). Reconstruir essa racionalidade local – o mundo como ele se apresentava de dentro do túnel – é o que transforma a investigação de um exercício de atribuição de culpa em uma fonte de aprendizado sistêmico.

> *"A atribuição de erro após o fato é um processo de julgamento social e psicológico, não uma conclusão objetiva" (Woods et al., 2010).*

3.2.4 Distanciamento através de diferenças

Um fenômeno comum que limita a aprendizagem organizacional é o "distanciamento por diferenças". Organizações frequentemente descartam eventos porque, na superfície, parecem diferentes de sua própria operação. Em algum nível de análise, todos os eventos são únicos; em outros níveis, revelam padrões comuns (Woods et al., 2010).

Cada evento, por mais dissimilar de outros na superfície, contém informação sobre padrões gerais subjacentes que ajudam a antecipar riscos potenciais antes que a falha ou o dano ocorram. Focar nos padrões comuns, e não nas diferenças superficiais, exige deslocar a análise de características superficiais para padrões mais profundos e dimensões mais abstratas.

"Outros, no futuro, podem facilmente olhar para conclusões de investigações e negar sua relevância para a própria situação, enfatizando diferenças. É por isso que evitar o viés de retrospectiva é tão importante: quando começamos com 'Como eles puderam perder o que agora é óbvio?', estamos habilitando racionalizações futuras de distanciamento por diferenças" (Woods et al., 2010).

3.2.5 Modelos e Ferramentas de Investigação: do Linear ao Sistêmico

Modelos Lineares e de Falhas Latentes

O modelo de sequência de eventos ou "**dominó**" (Heinrich, 1931) representa acidentes como cadeia linear de causas discretas, em que a remoção de qualquer elo interrompe a sequência – daí a noção de "causa raiz". O modelo de falhas latentes ou "**queijo suíço**" (Reason, 1990) avança ao distribuir a causalidade entre múltiplas camadas defensivas: desastres resultam da concatenação de pequenas falhas – cada uma importante, mas insuficiente isoladamente – quando "buracos" nas defesas se alinham.

Ambos, contudo, permanecem essencialmente **lineares e decompositivos**, e por isso encontram três limites em sistemas sociotécnicos complexos: os resultados emergem de **interações não lineares** entre componentes, e não da soma de suas falhas (Hollnagel, 2014; Leveson, 2004); as próprias barreiras são dinâmicas – adaptações cotidianas e pressões de produção erodem-nas gradualmente, num processo de **deriva prática** (Dekker, 2011; Snook, 2000); e a noção retrospectiva de "causa raiz" frequentemente obscurece a **racionalidade local** que tornou as ações inteligíveis no momento em que foram tomadas (Woods et al., 2010).



No nível das técnicas, essa lógica linear materializa-se em ferramentas amplamente usadas no setor: a **análise de causa raiz (RCA)** e suas árvores causais, o **diagrama de Ishikawa** (a "espinha de peixe") e os **Cinco Porquês**, entre outras (Ishikawa, 1986; Ohno, 1988). Reconhecer seus limites em sistemas complexos não as torna descartáveis: elas têm valor real e permanecem apropriadas onde a relação causa-efeito é estável e pode ser estabelecida por análise – os domínios simples e complicados, na distinção de Snowden e Boone (2007) – e, em particular, na análise de falhas de equipamento e de modos de falha técnicos. O risco está em aplicá-las a sistemas sociotécnicos complexos, nos quais o desfecho emerge de interações não lineares e a busca por uma "causa raiz" única tende a deter-se no operador mais próximo, encerrando a análise justamente onde o aprendizado começaria. A regra prática é ajustar a ferramenta à natureza do sistema: técnicas lineares para problemas ordenados; métodos sistêmicos, como os discutidos a seguir, para a complexidade (ver Seção 1.1.5).

Extremidades Afiada e Cega do Sistema

Sistemas complexos têm uma *extremidade afiada (sharp end)* onde praticantes interagem diretamente com o processo perigoso, e uma *extremidade cega (blunt end)* onde reguladores, administradores e formuladores de política controlam recursos, restrições e incentivos. A história do sucesso e da falha é como a prática da extremidade afiada se adapta para lidar com complexidades, moldada pelos recursos da extremidade cega.

Ferramentas de Investigação

Ferramentas sistêmicas contemporâneas ampliam o repertório analítico em sistemas complexos. Cada uma carrega pressupostos teóricos próprios e responde melhor a certos tipos de pergunta:

- **AcciMap** (Rasmussen, 1997): Mapeia decisões e ações em múltiplos níveis organizacionais, desde governo/reguladores até operadores, identificando como pressões fluem do topo para baixo e como adaptações locais propagam-se para cima.

- **FRAM - Functional Resonance Analysis Method** (Hollnagel, 2012): Analisa como a variabilidade de desempenho de funções interconectadas pode ressoar e produzir resultados inesperados, tanto positivos quanto negativos.
- **STAMP - Systems-Theoretic Accident Model and Processes** (Leveson, 2004): Trata segurança como problema de controle, analisando como restrições de segurança foram violadas e como estruturas de controle falharam em manter comportamento seguro.
- **HFACS - Human Factors Analysis and Classification System** (Shappell & Wiegmann, 2000): Taxonomia baseada no modelo de Reason, organiza fatores contribuintes em níveis hierárquicos desde atos inseguros até influências organizacionais.

Nota: nenhuma dessas ferramentas, contudo, é completa ou neutra: AcciMap e FRAM exigem julgamento expressivo do analista para delimitar níveis e funções, e enfrentam questões reconhecidas de confiabilidade entre investigadores (Underwood & Waterson, 2014); STAMP requer formação em teoria de controle e aplica-se com mais naturalidade em sistemas com forte componente automatizado; HFACS, por herdar a taxonomia de Reason, partilha das limitações dos modelos de falhas latentes – em particular, a tendência a categorizar antes de compreender. A escolha de ferramenta deve ser guiada pela natureza do sistema, pela pergunta investigativa e pela competência analítica disponível – frequentemente combinando mais de uma abordagem.

Vale registrar, ainda, que algumas dessas ferramentas não se limitam à investigação retrospectiva. O **FRAM** foi concebido tanto para analisar eventos quanto, sobretudo, para modelar a variabilidade do trabalho cotidiano e antecipar como o desempenho normal pode ressoar em resultados indesejados – sendo, portanto, também um método de ***análise proativa do trabalho normal*** (Hollnagel, 2012). De modo análogo, o STAMP deu origem a uma técnica prospectiva de análise de perigos (STPA), aplicada já na fase de projeto. AcciMap e HFACS, por sua vez, permanecem predominantemente retrospectivos, ainda que os marcos que os fundamentam – a estrutura de gestão de risco de Rasmussen e as camadas de Reason – informem o raciocínio proativo sobre controles.

ORIENTAÇÃO PRÁTICA: AO INVESTIGAR UM EVENTO, PERGUNTE TAMBÉM O QUE DEU CERTO

Mesmo em um evento adverso, a imensa maioria das ações, defesas e adaptações funcionou – muitas vezes por um longo tempo antes que o evento ocorresse. Investigações orientadas apenas para o que falhou desperdiçam essa informação. Recomenda-se, portanto, que toda análise de evento pergunte, lado a lado: o que normalmente dá certo nesta atividade e o que deu certo mesmo desta vez? Tornar visível o que funcionou (i) reduz o viés de retrospectiva, ao reinserir a incerteza vivida pelos praticantes; (ii) revela as fontes de resiliência que sustentaram a operação e que devem ser preservadas; e (iii) ajuda a enxergar como o sistema derivou lentamente para a falha, quando adaptações antes seguras deixaram de sê-lo.

Hollnagel, 2014; Dekker, 2011; Flight Safety Foundation, 2021

A própria trajetória dessas ferramentas, do encadeamento linear à análise sistêmica, revela um limite intrínseco da aprendizagem reativa: por mais sofisticado que seja o método, ele parte, basicamente, do que deu errado. Compreender por que um acidente ocorreu exige, antes, compreender como, na imensa maioria das vezes, o trabalho dá certo. É a esse deslocamento que o próximo movimento se dedica.

APRENDER COM O TRABALHO NORMAL: A VIRADA PROATIVA

3.2.6 Aprendizagem Proativa: Como a Prática Cria Segurança

Tipicamente, as reações à falha assumem que o sistema é "seguro" (ou foi tornado seguro) de forma inerente e que as falhas manifestas são apenas a marca de um componente não confiável. Mas o que é irredutível é a incerteza sobre o futuro: a mudança está sempre ativa e os recursos são sempre finitos. Como resultado, todos os sistemas confrontam perigos inerentes e trade-offs, e são vulneráveis à falha.

Em contraste com a visão de que os praticantes são a principal fonte de não confiabilidade em um sistema de outro modo bem-sucedido, o exame mais detido de como o sistema funciona diante das demandas cotidianas e excepcionais mostra que pessoas em muitos papéis efetivamente **"criam segurança"** por meio de seus esforços e de sua expertise. As pessoas contribuem ativamente para a segurança, bloqueando trajetórias potenciais de acidente ou recuperando-se delas, quando conseguem desempenhar esses papéis com sucesso.

> *"Para entender episódios de falha, você tem que primeiro entender o sucesso usual – como pessoas em seus vários papéis aprendem e se adaptam para criar segurança em um mundo repleto de perigos, tradeoffs e múltiplos objetivos"* (Woods et al., 2010).

Ironicamente, entender as fontes de falha começa por entender como os praticantes criam sucesso e segurança, como coordenam atividades de maneiras que os ajudam a lidar com os diferentes tipos de complexidade que experienciam. O sucesso não está "embutido" no sistema: é produto de esforço contínuo. As histórias secundárias revelam como a prática é organizada para permitir que os praticantes criem sucesso face às ameaças; indivíduos, equipes e organizações estão cientes dos perigos e adaptam suas práticas e ferramentas para se proteger ou neutralizá-los. São esses esforços que "fazem a segurança".



PERSPECTIVA BASEADA NA PRÁTICA: SEGURANÇA COMO COMPETÊNCIA COLETIVA E INCORPORADA

A abordagem baseada na prática oferece a fundamentação ontológica da virada proativa. Gherardi e Nicolini (2000a, 2002b) sustentam que a segurança em operações de alto risco é uma competência coletiva e incorporada – uma realização social, situada nas práticas das comunidades de trabalho e sustentada no fazer cotidiano –, e não um atributo fixo do sistema nem um conteúdo que se ensina e se transfere (Biermann-Teuscher et al., 2024). Daí a tese de que transferir é transformar: o conhecimento de segurança não circula como um pacote estável a ser distribuído, mas é continuamente redefinido e renegociado nas práticas que o mobilizam (Gherardi & Nicolini, 2000b). Disso decorre que a aprendizagem genuína não se esgota em repositórios de lições aprendidas ou em análises de incidentes: realiza-se nas adaptações situadas, na variabilidade incorporada e na expertise coletiva que os praticantes mobilizam ao criar segurança diante das demandas reais do trabalho.

É nesse plano que opera o knowing-in-practice (Gherardi & Nicolini, 2000a; Gherardi, 2012) – o conhecer que vive no fazer coletivo –, substrato da **Aprendizagem Operacional**. *Para estudá-lo, é preciso observar a prática enquanto ela se desenrola, e não apenas perguntar o que as pessoas "sabem" (Gherardi, 2012, p. 23).*

Gherardi, 2006, 2012; Gherardi & Nicolini, 2000a, 2002a, 2002b; Biermann-Teuscher et al., 2024

Se a segurança é uma competência que vive no fazer cotidiano, então aprender sobre segurança exige observar o trabalho normal – e não apenas as ocasiões em que ele falha. É exatamente esse deslocamento de foco que a distinção entre **Safety-I e Safety-II**, articulada por Hollnagel (2014), torna explícita: ela representa uma mudança paradigmática na forma como pensamos a segurança e a aprendizagem organizacional (Hollnagel, 2014; Dekker, 2014b). As duas perspectivas implicam, inclusive, direções opostas de melhoria: a Safety-I procura *reduzir* o número de resultados inaceitáveis (uma segurança decremental, que tende a zero), ao passo que a Safety-II procura *aumentar* o número de resultados aceitáveis (uma segurança incremental, que tende ao todo) (Hollnagel, 2014, 2018).

Tabela 3.2.2: Contraste entre Safety-I e Safety-II

Aspecto	Safety-I (Segurança Decremental)	Safety-II (Segurança Incremental)
Definição de segurança	Que o menor número possível de coisas dê errado.	Que o maior número possível de coisas dê certo.
Princípio de gestão	Reativo: responder quando algo acontece ou é categorizado como risco inaceitável.	Proativo: antecipar desenvolvimentos e eventos, buscando identificar continuamente riscos potenciais.
Visão do erro humano	Falhas são causadas por erros humanos, falhas técnicas e eventos adversos.	Variabilidade de desempenho é inevitável e representa ajustes necessários às condições.
Foco da aprendizagem	Investigação de acidentes, incidentes e quase-acidentes.	Estudo do trabalho cotidiano e de como o sucesso é criado.
Papel do humano	Risco a ser controlado; fonte de variabilidade indesejada.	Recurso necessário para flexibilidade e resiliência do sistema.

Fonte: *Adaptado de Hollnagel (2014)*

A Figura 3.2.1 sintetiza esse deslocamento. A distribuição do desempenho cotidiano – ampla, contínua, povoada de ajustes – é o que sustenta tanto os sucessos quanto as falhas; e são as condições de frequência e similaridade que determinam onde a aprendizagem é, de fato, possível.



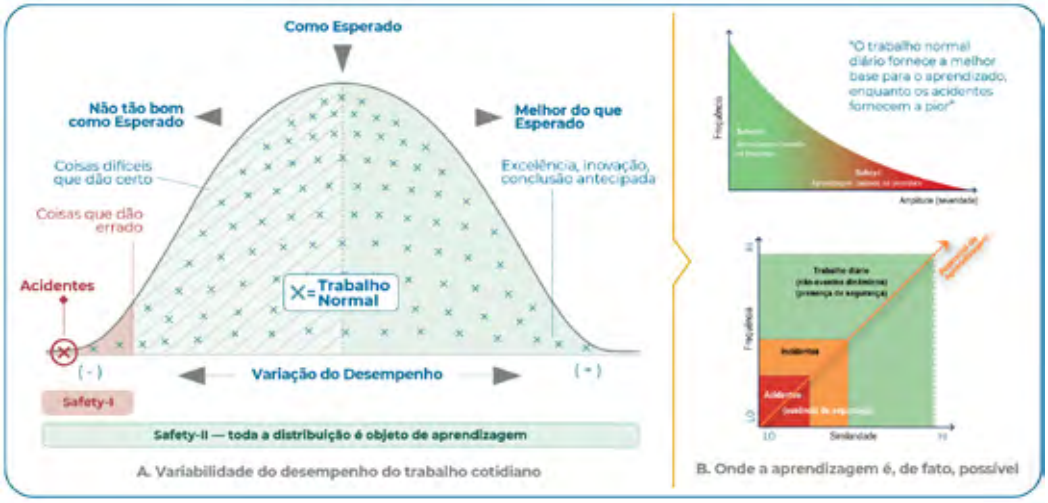


Figura 3.2.1: Aprendizagem com o trabalho normal – da Segurança Tradicional/Decremental (Safety-I) à Segurança Contemporânea/Incremental (Safety-II). (A) Variabilidade do desempenho do trabalho cotidiano; (B) onde a aprendizagem é, de fato, possível. **Fonte:** adaptado de Hollnagel (2014; 2018; 2021) e Flight Safety Foundation (2021).

Nota: O Painel A representa a distribuição da variabilidade do desempenho do trabalho cotidiano (cada X é uma instância do trabalho normal). A maior parte do trabalho situa-se em torno de "como esperado", estendendo-se do "não tão bom como esperado" – incluindo coisas difíceis que, ainda assim, dão certo – ao "melhor do que esperado", que produz excelência, inovação e conclusão antecipada; as "coisas que dão errado", incluindo os acidentes, ocupam apenas uma cauda estreita e marginal. A Safety-I volta-se exclusivamente a essa cauda adversa, enquanto o Safety-II toma toda a distribuição como objeto de aprendizagem. O Painel B detalha por que isso importa. Em frequência × amplitude (severidade), a aprendizagem baseada na frequência (Safety-II) apoia-se numa base muito mais ampla do que a baseada na severidade (Safety-I): o trabalho normal diário oferece a melhor base para aprender, e os acidentes, a pior (Hollnagel, 2018). Em frequência × similaridade, os acidentes – raros, dissimilares e expressão da ausência de segurança – situam-se no canto de baixa frequência e baixa similaridade; os incidentes ocupam uma faixa intermediária; e o trabalho diário – frequente, similar e expressão da presença de segurança ("não-eventos dinâmicos") – concentra-se no canto de alta frequência e alta similaridade. O potencial de aprendizagem cresce ao longo da diagonal, na direção do trabalho cotidiano.

Há uma razão estrutural para que as organizações aprendam tanto com o fracasso e tão pouco com o sucesso. Hollnagel descreve a segurança como um problema de **detecção de sinais**: resultados inesperados – acidentes e incidentes – destacam-se nitidamente acima do "limiar de detecção" da atenção organizacional; são poucos, dissimilares e impossíveis de ignorar. Já os resultados esperados – o trabalho que dá certo o tempo todo – situam-se abaixo desse limiar: são tão frequentes e tão semelhantes que não chamam a atenção e passam despercebidos (Hollnagel, 2018). Aprender com o trabalho normal exige, por isso, um esforço deliberado de *aprender a notar* aquilo que normalmente se ignora.

Tabela 3.2.3: As quatro condições para a aprendizagem

Condição	O que exige	Evento adverso (segurança ausente)	Trabalho cotidiano (segurança presente)
Motivação	Deve haver motivação e necessidade de aprender.	Alta	Baixa
Oportunidade	Deve haver muitos casos com que aprender.	Poucas	Muitas
Similaridade	Os casos devem ser semelhantes entre si.	Baixa	Alta
Confirmação	Deve ser possível confirmar o que foi aprendido.	Difícil	Fácil

Fonte: *adaptado de Hollnagel (2021).*

O quadro revela um paradoxo: o evento adverso reúne a maior motivação para aprender, mas as piores condições para fazê-lo; o trabalho cotidiano, a menor motivação e as melhores condições. A virada proativa consiste, em boa medida, em suprir deliberadamente a motivação que falta para aprender com aquilo que dá certo (Hollnagel, 2021).

Trabalho como Imaginado × Trabalho como Realizado: a dupla face das adaptações

Gestores e projetistas costumam imaginar o trabalho como ordenado e previsível – o **Trabalho como Imaginado (WAI)** –, e é sobre essa imagem que se constroem procedimentos, análises de risco e sistemas de gestão. O trabalho real – o **Trabalho como Realizado (WAD)** – exige, porém, adaptação constante a pressões de tempo, equipamentos variáveis, informação incompleta e situações inesperadas. Essas adaptações são, na maioria das vezes, necessárias, e frequentemente são justamente o que permite ao sistema operar com segurança (Dekker, 2014b).



Seria um equívoco, contudo, ler toda adaptação como benéfica. A mesma variabilidade que cria segurança tem **dupla face**: sob pressão crônica de produção, pequenas adaptações localmente racionais podem acumular-se e deslocar lentamente o sistema em direção aos seus limites – a *deriva para o fracasso* (Dekker, 2011) – até que o que era exceção se torne rotina, num processo de *normalização do desvio* (Vaughan, 1996). E a variabilidade do desempenho, necessária ao funcionamento, também pode ressoar e combinar-se de formas que produzem dano (Hollnagel, 2012). Observar o WAD, portanto, não é celebrar adaptações: é compreendê-las nas **duas direções** – reconhecendo as adaptações benéficas, que merecem ser sustentadas, e, ao mesmo tempo, as adaptações perigosas, os pontos cegos e as armadilhas de erro (situações que tornam o erro mais provável) que precisam ser tratados (IOGP, 2022). É essa leitura equilibrada do hiato entre WAI e WAD que orienta os métodos proativos discutidos adiante.

A esse duplo caráter das adaptações soma-se uma tensão de projeto raramente explicitada. Ao conceber procedimentos, análises de risco e sistemas de gestão, a organização não apenas imagina o trabalho de forma ordenada e previsível, o Trabalho como Imaginado, como também projeta um **Trabalhador como Imaginado (Worker-as-Imagined)**: uma figura suposta, ao mesmo tempo, plenamente aderente, constante e previsível e, quando algo não previsto emerge, criativa e capaz de compensar as próprias limitações do sistema (Hollnagel & Dekker, 2025). Trata-se de um paradoxo – espera-se conformidade na maior parte do tempo, mas criatividade quando necessário –, sendo que esta segunda expectativa quase nunca possui papel formal nas decisões de projeto. Reconhecer essa

contradição evita a leitura simplista do Trabalho como Realizado como mera "não adesão ao procedimento" e recoloca a variabilidade humana como recurso indispensável, sem o qual poucas das soluções convencionais de Fatores Humanos efetivamente funcionariam.

A Engenharia de Resiliência reenquadra o erro humano: em vez de tratá-lo como variável a ser eliminada, considera-o expressão da variabilidade de desempenho que mantém o sistema funcionando. Nessa perspectiva, segurança não é a ausência de eventos adversos, mas a **presença de capacidades** que permitem ao sistema desempenhar o exigido sob condições esperadas e inesperadas – capacidades essas que se traduzem nos quatro potenciais sistêmicos discutidos a seguir (Hollnagel, 2018).

3.2.7 Engenharia de Resiliência: Monitorando a Capacidade Adaptativa

A Engenharia de Resiliência representa uma forma de pensar sobre segurança que se afasta das abordagens convencionais de gestão de risco. Busca formas de melhorar a capacidade das organizações de monitorar e revisar modelos de risco, criar processos que são robustos porém flexíveis, e usar recursos proativamente face a perturbações ou pressões contínuas de produção e econômicas (Hollnagel, Woods & Leveson, 2006).

Segundo a Engenharia de Resiliência, acidentes não representam uma quebra ou mau funcionamento de funções normais do sistema, mas **colapsos nas adaptações necessárias para lidar com a complexidade do mundo real**. O sucesso tem sido atribuído à capacidade de grupos, indivíduos e organizações de antecipar a forma mutável do risco antes que o dano ocorra o fracasso, por sua vez, corresponde à ausência, temporária ou permanente, dessa capacidade (ver Seção 2.4).

Propriedades de Resiliência

Monitorar essa capacidade é necessário porque ela não é um atributo fixo: pode ser construída, sustentada, degradada e perdida ao longo do tempo (Woods, 2018).

Seu estado pode ser lido em propriedades como (Woods et al., 2010; Hollnagel, Woods & Leveson, 2006):

- **Capacidade de amortecimento (buffering capacity):** o tamanho ou os tipos de perturbações que o sistema pode absorver ou às quais pode adaptar-se sem um colapso fundamental no desempenho;
- **Flexibilidade:** a capacidade do sistema de se reestruturar em resposta a mudanças ou pressões externas;
- **Margem:** quão perto o sistema está atualmente operando em relação a um ou outro tipo de limite de desempenho;
- **Tolerância:** se o sistema degrada graciosamente conforme estresse e pressão aumentam, ou colapsa rapidamente quando a pressão excede a capacidade adaptativa – padrão denominado colapso abrupto (brittleness), o oposto da extensibilidade graciosa (Woods, 2018; ver Seção 2.4.3).

Quatro Potenciais Sistêmicos

A Engenharia de Resiliência operacionaliza essa visão por meio dos quatro potenciais sistêmicos (Hollnagel, 2018): a capacidade de Responder ao atual, Monitorar o crítico, Aprender com o factual e Antecipar o potencial. Esses potenciais tornam-se observáveis em dimensões organizacionais concretas (Woods et al., 2010); três delas são especialmente diagnósticas:

- **Preparação/Antecipação:** a organização é proativa em captar evidências de problemas em desenvolvimento, em vez de apenas reagir depois que se tornam significativos?
- **Opacidade/Observabilidade:** a organização monitora limites de segurança e reconhece quão perto está da "borda" em termos de defesas e barreiras degradadas, considerando o desempenho passado, o atual e o potencial futuro (Rigaud & Martin, 2013)?
- **Flexibilidade/Rigidez:** como a organização se adapta a mudanças, perturbações e oportunidades?

Essas três dimensões instanciam, respectivamente, os potenciais de Antecipar, Monitorar e Responder. A quarta capacidade – **Aprender** – é o objeto próprio

desta seção, e sua operacionalização é tratada no repertório de métodos a seguir (3.2.8) e, em detalhe, nas Equipes de Aprendizagem e Melhoria (3.2.9).

Para acompanhar os quatro potenciais ao longo do tempo, o instrumento de referência é a Grade de Análise de Resiliência (RAG; ver Seção 2.4.3). Reaplicada periodicamente e ancorada na observação do trabalho cotidiano, ela revela não apenas lacunas, mas também as práticas, formais e informais, que sustentam cada potencial – o que a aproxima do repertório de métodos de aprendizagem proativa (Trancoso, Patriarca, & Henriqson, 2024).

3.2.8 Operacionalizando a Aprendizagem Proativa: um Repertório de Métodos

Observar o trabalho normal como prática regular exige dispositivos concretos e não há método único. A aprendizagem proativa operacionaliza-se por uma **família de métodos complementares**, que partilham a orientação ao Trabalho como Realizado e ao estudo de como o sucesso é produzido, mas diferem em granularidade, recursos exigidos e tipo de pergunta a que melhor respondem (IOGP, 2022; Flight Safety Foundation, 2021). O ponto de partida é a constatação de Hollnagel (2021) de que o trabalho cotidiano, frequente, similar e verificável, oferece a melhor base para aprender, enquanto os acidentes, raros e dissimilares, oferecem a pior. Daí o princípio prático comum a essas fontes: integrar tais métodos aos processos de gestão já existentes, em vez de construir uma estrutura paralela (IOGP, 2022).

A Tabela 3.2.4 sintetiza um repertório documentado nos setores de óleo e gás (IOGP, 2022) e de aviação (Flight Safety Foundation, 2021), ordenado aproximadamente da menor para a maior intensidade de recursos.

Tabela 3.2.4: Repertório de métodos para aprender com o trabalho normal

Método	O que busca tornar visível	Melhor uso	Referência
Conversas de aprendizagem da liderança	Fatores que dificultam o trabalho e o "trabalho como realizado", a partir da escuta ativa, de perguntas abertas e não acusatórias.	Engajamento cotidiano; integra-se a diálogos diários e a visitas de liderança.	IOGP (2022).
Revisão pós-trabalho estruturada (debriefing)	Surpresas, adaptações e diferenças entre o planejado e o realizado, logo após etapas críticas.	Captura imediata de aprendizado na rotina; pode seguir o ciclo reflexivo de Gibbs (Gibbs, 1988).	IOGP (2022).
Walk Through/ Talk Through (WTTT)	Etapas críticas e armadilhas de erro, em diálogo individual com quem executa a tarefa.	Exame granular de tarefas estabelecidas e sequenciais; de raiz HRA, mas aplicado como diálogo de aprendizagem.	IOGP (2022).
Functional Resonance Analysis Method (FRAM)	Como a variabilidade de funções interconectadas do trabalho normal pode ressoar e combinar-se, produzindo resultados desejados ou indesejados.	Análise prospectiva de atividades acopladas e variáveis; modela o Trabalho como Realizado; exige analista treinado.	Hollnagel (2012).
Equipes de Aprendizagem e Melhoria (LIT)	Restrições, trade-offs e dilemas que atravessam equipes e funções, em sessão coletiva facilitada.	Trabalho realizado por pessoas em interação; dependências entre equipes (desenvolvida em 3.2.9); exige facilitador e/ou supervisor de linha treinado.	IOGP (2022); Flight Safety Foundation (2021); Conklin (2019).
Monitoramento de Operações Normais (NOM) e observação do trabalho cotidiano	A operação como de fato ocorre, por observação "sobre o ombro" complementada por conversa, incluindo boas práticas usualmente invisíveis	Questões sistêmicas difíceis de verbalizar; aproxima especialistas de segurança e linha de frente.	Flight Safety Foundation (2021); de la Flor (2021).

Método	O que busca tornar visível	Melhor uso	Referência
Levantamentos locais de segurança (de auditoria a compreensão)	A realidade do trabalho por trás das respostas "corretas" das auditorias de conformidade.	Diagnóstico de procedimentos e de mudanças; transforma o auditor em investigador do trabalho real.	Flight Safety Foundation (2021).
Uso ampliado de dados operacionais	A distribuição inteira do desempenho cotidiano, e não apenas os eventos de exceção.	Organizações com dados já coletados; alimenta autoaprendizagem e debriefing.	Flight Safety Foundation (2021).
Grade de Análise de Resiliência (RAG)	O perfil dos quatro potenciais (responder, monitorar, antecipar, aprender) e as práticas, formais e informais, que os sustentam no trabalho cotidiano.	Acompanhamento longitudinal da capacidade adaptativa, reaplicando as mesmas perguntas ao mesmo grupo; na versão ancorada em observação, aproxima-se dos métodos de aprendizagem; exige facilitador treinado.	Hollnagel (2011, 2018); Trancoso, Patriarca e Henriqson (2024).
Análise de Tarefas Críticas para a Segurança (SCTA) e Processo de Melhoria de Tarefas (PMT)	Modos de falha humana e barreiras em tarefas críticas de segurança, com aplicação da hierarquia de controles.	Tarefas críticas de barreiras de acidentes maiores; requisito regulatório (ver Seção 3.4); exige especialista/ facilitador treinado.	IOGP (2022); ver Seção 3.4.

Fonte: *elaborado a partir de IOGP (2022), Flight Safety Foundation (2021), Hollnagel (2012, 2018, 2021) e Trancoso, Patriarca e Henriqson (2024).*

Duas observações sobre a tabela. A **Análise de Tarefas Críticas para a Segurança (SCTA)** e o **Processo de Melhoria de Tarefas (PMT)** foram incluídos por completude, mas com uma ressalva: são aplicações da Análise de Confiabilidade Humana (HRA) a tarefas críticas, exigidas por requisitos regulatórios em diversas jurisdições (IOGP, 2022), mais do que métodos de aprendizagem proativa no

sentido aqui empregado; seu desenvolvimento pertence à Seção 3.4 (Análise de Confiabilidade Humana – HRA – e Tarefas Críticas), à qual remetemos o leitor. O **FRAM**, por sua vez, figura aqui em sua aplicação proativa – a modelagem do trabalho normal –, complementando o uso investigativo discutido em 3.2.5.

Esses métodos são complementares, não concorrentes. Uma comparação direta entre uma Equipe de Aprendizagem e um WTTT aplicados à mesma atividade mostrou que cada um revela o que o outro não captura: o WTTT oferece exame mais granular das etapas, enquanto a Equipe de Aprendizagem amplia o campo de visão para dependências e fatores não restritos ao operador (IOGP, 2022). A escolha – e, com frequência, a combinação – depende da granularidade necessária, da criticidade da tarefa e dos recursos disponíveis. Há ainda um limite comum a todos: aquilo que se procura condiciona aquilo que se encontra, e a punição percebida inibe a abertura de que qualquer um desses métodos depende (IOGP, 2022), o que reconecta o repertório às condições habilitadoras tratadas adiante (3.2.10).

3.2.9 Equipes de Aprendizagem e Melhoria (LIT): a operacionalização da Aprendizagem Proativa

Entre os dispositivos desse repertório, as **Equipes de Aprendizagem e Melhoria** (*Learning and Improvement Teams* – LIT; referidas na literatura setorial também como *Equipes de Aprendizagem*, *Learning Teams*) configuram-se como uma das alternativas viáveis para sustentar a observação do trabalho como prática regular, e não como auditoria ou evento extraordinário, ao oferecer um arranjo dedicado à observação do trabalho enquanto ele se desenrola (Gherardi, 2012). Embora a expressão tenha circulado inicialmente na tradição *Human and Organizational Performance* (Conklin, 2019) e em experiências aplicadas como a da American Airlines (Flight Safety Foundation, 2021), o que caracteriza uma LIT não é uma metodologia fechada, mas o **propósito** de tornar visível o *knowing-in-practice* (conhecer na prática) que vive nas operações cotidianas.

Em termos práticos, uma sessão de LIT pode ser conduzida por um facilitador treinado em conjunto com a supervisão de linha, contemplando objetivos como: (i) observar a operação diária com foco em compreensão, não em fiscalização; (ii) facilitar o diálogo de aprendizagem em condições de segurança psicológica;

(iii) documentar o saber situado por meio de **objetos de fronteira** – relatórios de observação e de aprendizagem que circulam entre níveis organizacionais; (iv) identificar padrões preliminares – tanto adaptações benéficas, que sinalizam capacidades adaptativas a sustentar, quanto adaptações perigosas, pontos cegos e armadilhas de erro a tratar; e (v) traduzir essa expertise entre comunidades de prática, sustentando a institucionalização do conhecimento operacional. A configuração específica – número de níveis no sistema de aprendizagem, periodicidade das sessões, instrumentos formais adotados – varia conforme o contexto e a maturidade organizacional. Aplicações no setor de óleo e gás têm sido documentadas em diferentes empresas (Almeida, Bruno, & Capaverde, 2025).

O diálogo de aprendizagem pode ser estruturado em torno de três perguntas que deslocam o foco do erro individual para as condições reais do trabalho: **dependências** – que recursos e condições são necessários para realizar bem o trabalho?; **sensibilidades** – o que torna o trabalho mais fácil ou mais difícil?; e **práticas** – que práticas sustentam um trabalho seguro e eficaz? Essas perguntas orientam a observação para o sistema que cerca o operador, e não para o operador isolado, dando forma concreta ao objetivo (ii), acima, e conectando a sessão às dependências e aos fatores não restritos ao operador que distinguem a Equipe de Aprendizagem dos métodos centrados na tarefa.



A distinção em relação às auditorias comportamentais clássicas é ontológica antes de ser metodológica: a LIT não compara o desempenho a um padrão prescrito (Trabalho como Imaginado) para identificar desvios, mas observa o Trabalho como Realizado para *aprender com ele* – tanto com as adaptações benéficas, que normalmente permanecem invisíveis ao sistema de gestão e merecem ser sustentadas, quanto com as adaptações perigosas, os pontos cegos e as armadilhas de erro que revelam a fragilidade do sistema (IOGP, 2022; Hollnagel, 2018; Gherardi & Nicolini, 2002b). Nesse sentido, a Equipe de Aprendizagem não substitui a investigação de eventos adversos: complementa-a, acrescentando ao sistema de aprendizagem organizacional aquilo que os eventos não revelam – como o sucesso é produzido no trabalho normal.

Vale destacar o alcance do aprendizado. O trabalho cotidiano não se distribui apenas entre "certo" e "errado": como ilustra a Figura 3.2.1, os eventos que dão errado ocupam uma cauda estreita da distribuição do desempenho, enquanto a maior parte consiste em situações difíceis que, ainda assim, dão certo (mas poderiam dar errado) – e, na cauda oposta, em desempenho que produz excelência, inovação e conclusão antecipada (Hollnagel, 2018). Uma Equipe de Aprendizagem dirige o olhar a todo esse espectro: além de evitar o que dá errado, busca compreender como o sucesso é produzido sob condições variáveis, inclusive quando o desempenho supera o esperado.

CONDIÇÕES ORGANIZACIONAIS E SÍNTESE

3.2.10 Condições habilitadoras: Cultura Justa, Segurança Psicológica e Alta Confiabilidade

Os dois modos de aprendizagem examinados até aqui dependem de condições organizacionais que os tornam possíveis. Três delas merecem registro, ainda que desenvolvidas em outras seções deste compêndio.

A primeira é a **Cultura Justa**. A tensão entre aprender com falhas e responsabilizar (accountability) é um dos desafios centrais para organizações que buscam melhorar a segurança. A questão decisiva não é onde traçar a linha entre o comportamento aceitável e o inaceitável, mas quem tem legitimidade para traçá-la (Dekker, 2008). Responsabilizar e culpar são coisas distintas: culpar tende a reduzir a accountability, pois inibe relatos e a participação em esforços de melhoria (Woods et al., 2010). O tema é desenvolvido na Seção 3.3, em particular na distinção entre accountability retrospectiva, orientada à culpa por eventos passados, e accountability prospectiva, orientada às condições de segurança futura (Sharpe, em Dekker & Breakey, 2016).



A segunda é a **Segurança Psicológica**, que repousa sobre uma atmosfera de **Confiança**. Os dois modos de aprendizagem só se concretizam quando as pessoas se sentem seguras para reportar problemas, admitir erros e questionar práticas sem medo de retaliação (Edmondson, 2019). Convém não confundir os dois conceitos: a confiança é a expectativa, em geral interpessoal, de que o outro agirá de boa-fé; a segurança psicológica é a crença compartilhada, no nível da equipe, de que assumir riscos interpessoais não trará consequências negativas – distinção que Lloyd (2020) retoma de Edmondson, observando que a confiança alimenta a segurança psicológica sem com ela se confundir. E não se trata de condição acessória: a confiança figura entre os principais preditores do desempenho em segurança, e sua ausência corrói o próprio aparato de aprendizagem – sem ela, os relatos tornam-se superficiais, os quase-acidentes são banalizados e mesmo as iniciativas mais bem-intencionadas são recebidas com cinismo (Lloyd, 2020). A construção da confiança no relato – ancorada na Cultura Justa – é desenvolvida na Seção 3.3.6; é esse substrato que viabiliza o diálogo de aprendizagem em que se apoia a observação do trabalho (Seção 3.2.9), necessário tanto à aprendizagem reativa, que depende de relatos francos, quanto à proativa, que depende da disposição de tornar visível o trabalho real.

A terceira é a **alta confiabilidade**. Organizações que gerenciam operações perigosas com sucesso notável criam segurança por anteciparem e se prepararem para eventos inesperados e surpresas futuras – e não por evitarem riscos ou reduzirem erros. Para elas, a segurança é um valor que requer reforço e investimento contínuos, sustentado por um fluxo aberto de informação sobre a face mutável do potencial de falha (Weick & Sutcliffe, 2007; Woods et al., 2010). Esse fluxo aberto de informação caracteriza o que Westrum (2004) denominou cultura organizacional generativa. As características dessas organizações são tratadas na Seção 2.2.

Essas condições não operam isoladamente: Cultura Justa, segurança psicológica e alta confiabilidade – somadas ao engajamento das lideranças – são retomadas e sistematizadas como premissas do framework integrador na Seção 4.1.1.

3.2.11 Dez Passos para o Progresso em Segurança

Os dez passos a seguir, destilados por Woods et al. (2010) da pesquisa sobre como sistemas complexos falham, são a síntese operacional da tese deste capítulo e não um checklist procedural: cada passo traduz, em orientação prática, o deslocamento do erro-como-causa para a compreensão de como a prática cria e perde segurança.

#	Passo
1	Reconhecer que o erro humano é uma atribuição.
2	Buscar histórias secundárias para encontrar contribuintes mais profundos e múltiplos.
3	Escapar do viés de retrospectiva.
4	Entender o trabalho realizado na extremidade afiada do sistema.
5	Buscar vulnerabilidades sistêmicas.
6	Estudar como a prática cria segurança.
7	Buscar padrões subjacentes.
8	Examinar como a mudança produzirá novas vulnerabilidades.
9	Usar nova tecnologia para apoiar e melhorar a expertise humana.
10	**Domar a complexidade através de novas formas de feedback.**

3.2.12 Considerações Finais

Como esta seção procurou demonstrar, a aprendizagem organizacional para a segurança opera em duas frentes (ou dois modos): aprender com eventos adver-

sos (reativa) e com o trabalho cotidiano bem-sucedido (proativa). A segurança é um valor crônico que infunde todos os aspectos da prática, não uma commodity a ser tabulada. Pessoas criam segurança sob pressão, em todos os níveis dos sistemas sociotécnicos. Nenhum dos dois modos, contudo, opera no vazio: ambos dependem das condições organizacionais discutidas, – cultura justa, confiança e segurança psicológica, alta confiabilidade – sem as quais mesmo os métodos mais sofisticados degeneram em relatos superficiais e silêncio (Seção 3.2.10).

A segurança não é algo que um sistema tem, mas algo que um sistema faz. Na perspectiva baseada na prática (Gherardi, 2006; Gherardi & Nicolini, 2000a), essa realidade é ontológica: a segurança emerge das práticas coletivas das comunidades de trabalho, é socialmente construída, inovada e transmitida – e não pode ser plenamente capturada por repositórios de lições aprendidas ou por documentos de procedimentos. A aprendizagem genuína requer observar e compreender o *knowing-in-practice*: o conhecer que vive no fazer cotidiano dos praticantes.

> *"Progresso depende de estudar como a prática cria segurança face aos desafios, o que é necessário para ser um especialista em contexto"* (Woods et al., 2010).



No cotidiano das operações, como documentado no setor de óleo e gás (Almeida, Bruno, & Capaverde, 2025), esse movimento ganha sentido operacional. De um lado, tornar visível, sistemático e operacionalmente útil o saber-em-ação (*knowing-in-practice)* das turmas e os ajustes silenciosos que mantêm a operação segura no dia a dia: adaptações benéficas que raramente atravessam o ciclo formal de incidentes e, por isso, costumam permanecer invisíveis ao sistema de gestão. De outro, e simetricamente, tornar visíveis as adaptações perigosas, os sinais fracos e as decisões localmente racionais que, sob pressão crônica de produção, podem erodir defesas e margens de segurança numa deriva para o fracasso (Dekker, 2011), atuando sobre essa migração antes que o sinal se converta em incidente. Aprender com o trabalho normal é, assim, sustentar deliberadamente a resiliência que já existe e interceptar a fragilidade que se acumula em silêncio.

Referências da Seção 3.2

Almeida, R. C., Bruno, J. C. S., & Capaverde, C. B. (2025). A learning journey toward more resilient systems: The case of a Brazilian oil and gas company. *In Proceedings of the Joint 11th Biennial Symposium of the Resilience Engineering Association and 14th Annual Resilient Health Care Society Meeting* (pp. 47–54). REA/RHCS.

Antonello, C. S., & Godoy, A. S. (2010). A encruzilhada da aprendizagem organizacional: uma visão multiparadigmática. *Revista de Administração Contemporânea*, 14(2), 310–332.

Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley.

Biermann-Teuscher, D., Thissen, L., Horstman, K., & Meershoek, A. (2024). Safety: A collective and embedded competency. *Journal of Safety Research*, 88, 93–102.

Catino, M. (2008). A review of literature: Individual blame vs. organizational function logics in accident analysis. Journal of Contingencies and Crisis Management, 16(1), 53–62.

Conklin, T. (2019). *The 5 principles of human performance: A contemporary update of the building blocks of human performance for the new view of safety*. Pre-Accident Media.

de la Flor, A. R. (2021). Observing everyday work: Normal operations monitoring at ENAIRE. HindSight, 31, 22–24. EUROCONTROL.

Dekker, S. W. A. (2008). Just culture: Balancing safety and accountability. Ashgate.

Dekker, S. W. A. (2011). Drift into failure: From hunting broken components to understanding complex systems. Ashgate.

Dekker, S. W. A. (2014a). The field guide to understanding 'human error' (3rd ed.). Ashgate.

Dekker, S. W. A. (2014b). Safety differently: Human factors for a new era. CRC Press.

Dekker, S. W. A., & Breakey, H. (2016). 'Just culture:' Improving safety by achieving substantive, procedural and restorative justice. Safety Science, 85, 187–193.

Edmondson, A. C. (2019). The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth. Wiley.

Flight Safety Foundation. (2021). *Learning from all operations: Expanding the field of vision to improve aviation safety*. FSF White Paper.

Gherardi, S. (2006). *Organizational knowledge: The texture of workplace learning*. Blackwell.

Gherardi, S. (2012). *How to conduct a practice-based study: Problems and methods* (2nd ed.). Edward Elgar.

Gherardi, S., & Nicolini, D. (2000a). The organizational learning of safety in communities of practice. *Journal of Management Inquiry*, 9(1), 7–18.

Gherardi, S., & Nicolini, D. (2000b). To transfer is to transform: The circulation of safety knowledge. Organization, 7(2), 329–348. https://doi.org/10.1177/135050840072008

Gherardi, S., & Nicolini, D. (2002a). Learning in a constellation of interconnected practices: Canon or dissonance? *Journal of Management Studies*, 39(4), 419–436.

Gherardi, S., & Nicolini, D. (2002b). Learning the trade: A culture of safety in practice. *Organization*, 9(2), 191–223.

Gibbs, G. (1988). Learning by doing: A guide to teaching and learning methods. Further Education Unit, Oxford Polytechnic.

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

Hilton, D. J. (1990). Conversational processes and causal explanation. *Psychological Bulletin*, 107(1), 65–81.

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method*. Ashgate.

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

Hollnagel, E. (2018). *Safety-II in practice: Developing the resilience potentials*. Routledge.

Hollnagel, E. (2021). Conditions for learning. HindSight, 31, 9–11. EUROCONTROL

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Ashgate.

Hollnagel, E., & Dekker, S. W. A. (2025). The ironies of "human factors". Theoretical Issues in Ergonomics Science, 26(3), 349–359. https://doi.org/10.1080/1463922X.2024.2443976

International Association of Oil & Gas Producers [IOGP]. (2022). Learning from normal work (Report No. 642).

Ishikawa, K. (1986). Guide to quality control (2nd rev. ed.). Asian Productivity Organization.

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

Lloyd, C. F. (2020). Next generation safety leadership: From compliance to care. CRC Press.

Ohno, T. (1988). Toyota production system: Beyond large-scale production. Productivity Press.

Parris, R. (2025). Accountability: A lived experience [Master's thesis, Lund University]. Division of Risk Management and Societal Safety, Faculty of Engineering.

Rasmussen, J. (1997). Risk management in a dynamic society. *Safety Science*, 27(2–3), 183–213.

Reason, J. (1990). *Human error*. Cambridge University Press.

Rigaud, E., & Martin, C. (2013). Considering trade-offs when assessing resilience. In *Proceedings of the Resilience Engineering Symposium 2013*. Resilience Engineering Association

Shappell, S. A., & Wiegmann, D. A. (2000). *The Human Factors Analysis and Classification System — HFACS*. Federal Aviation Administration.

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of US Black Hawks over Northern Iraq*. Princeton University Press.

Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. Harvard Business Review, 85(11), 68–76.

Trancoso, R., Patriarca, R., & Henriqson, É. (2024). Assessing resilience in everyday work through observations: An assessment framework for complex sociotechnical systems. *Safety Science*, 173, 106461.

Underwood, P., & Waterson, P. (2014). Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. *Accident Analysis & Prevention*, 68, 75–94.

Vaughan, D. (1996). The Challenger launch decision: Risky technology, culture, and deviance at NASA. University of Chicago Press.

Weick, K. E., & Sutcliffe, K. M. (2007). Managing the unexpected: Resilient performance in an age of uncertainty (2nd ed.). Jossey-Bass.

Westrum, R. (2004). A typology of organisational cultures. *Quality and Safety in Health Care*, 13(Suppl 2), ii22–ii27.

Woods, D. D., Dekker, S. W. A., Cook, R., Johannesen, L., & Sarter, N. (2010). *Behind human error* (2nd ed.). Ashgate.

Woods, D. D. (2018). The theory of graceful extensibility: Basic rules that govern adaptive systems. *Environment Systems and Decisions*, 38, 433 457

3.3 Cultura Justa e *Accountability*

Autores: Rafael Ceni de Almeida e Priscilla Salles de Moraes

Revisão: Beatriz Gershenson

3.3.1 Conceito e Evolução Histórica

A cultura justa representa um paradigma organizacional que busca equilibrar a necessidade de aprender com erros e a necessidade de manter a responsabilização individual (Reason, 1997). O conceito emergiu como resposta às limitações tanto da cultura de culpa tradicional, que inibia o relato de incidentes, quanto da cultura sem culpa, que poderia comprometer a credibilidade aos olhos do público e permitir comportamentos deliberadamente inseguros (Dekker, 2017).

O conceito foi originalmente desenvolvido por James Reason na década de 1990, no contexto de sua pesquisa sobre erro humano e acidentes organizacionais. Reason (1997) argumentou que a grande maioria dos atos inseguros são erros honestos, incluindo deslizes, lapsos e enganos, que não deveriam ser punidos. Contudo, reconheceu que uma cultura totalmente isenta de culpa não seria viável nem desejável, pois deixaria impunes comportamentos deliberadamente negligentes ou maliciosos.

A definição legal de cultura justa foi consolidada na aviação europeia através do Regulamento (UE) nº 376/2014, que a define como:

> *"uma cultura na qual os operadores de linha de frente ou outras pessoas não são punidos por ações, omissões ou decisões tomadas por eles que sejam proporcionais à sua experiência e treinamento, mas onde negligência grave, violações deliberadas e atos destrutivos não são tolerados" (Pellegrino, 2019, p. 57).*

Vale notar, contudo, que essa consolidação legal, embora referencial, é ela própria objeto de crítica acadêmica contemporânea. Bergström (2019) argumenta que a transposição da cultura justa do campo acadêmico para o regulatório (notadamente via Regulamento 376/2014) produziu o efeito discursivo de empoderar o aparato judicial-regulatório como autoridade legítima para traçar a linha entre comportamentos aceitáveis e inaceitáveis – um efeito muitas vezes oposto à intenção declarada de empoderar profissionais de linha de frente. Esta crítica é desenvolvida em 3.3.9.

3.3.2 O que é *Accountability*?



É fundamental distinguir entre os conceitos de *responsabilidade* (*responsibility*), *responsabilização legal* (*liability*) e *accountability*. Enquanto responsabilidade refere-se à obrigação de executar uma tarefa específica, e responsabilização legal implica sujeição a consequências legais pelo não cumprimento de deveres, ***accountability*** deriva de ***account*** – relatar ou descrever eventos passados – e **significa literalmente a capacidade de prestar contas sobre ações e suas consequências** (Pellegrino, 2019). O termo será mantido em inglês neste compêndio por não haver tradução direta adequada em português.

Virginia Sharpe (2003) desenvolveu o conceito de *accountability prospectiva*, distinguindo-a da *retrospectiva*. A ***accountability retrospectiva*** foca em eventos passados, buscando atribuir culpa, enquanto a ***prospectiva*** orienta-se para a deliberação sobre processos práticos necessários para alcançar objetivos de segurança e os papéis que cada pessoa deve desempenhar para que isso aconteça (Dekker & Breakey, 2016; Sharpe, 2003). Esta visão permite que os trabalhadores sejam vistos como parte da solução a ser aproveitada prospectivamente, não apenas como problemas a serem controlados retrospectivamente.

A distinção operacional mais direta encontrada na literatura é a de Ieraci (2007): "*responsibility involves doing*; *accountability involves reporting*" - responsabilidade diz respeito à execução de obrigações; *accountability* diz respeito à prestação de contas sobre essas ações e suas consequências. Hoskin (1996) acrescenta que accountability ultrapassa o escopo da responsabilidade porque se estende por fronteiras hierárquicas e organizacionais e abrange situações não previstas antecipadamente. Pesquisa empírica com profissionais de indústrias de alto risco demonstra que essa distinção - embora clara na teoria - raramente é operacionalizada na prática organizacional, contribuindo para que sistemas disciplinares tratem de forma equivalente erros honestos e violações deliberadas (Parris, 2025).

Nota: O constructo *accountability* possui raízes conceituais que precedem a literatura de segurança. Roberts (1991), no campo da Contabilidade Crítica, definiu-o como uma tensão relacional dinâmica entre quem presta contas e quem as recebe - um processo social que estrutura identidades, relações de poder e a capacidade de aprender. Esta perspectiva, que vê *accountability* simultaneamente como processo e como resultado (Lilley, 1996), é relevante para a indústria de energia porque revela que o modo como *accountability* é enquadrada - como controle hierárquico ou como diálogo - determina se ela inibe ou favorece a aprendizagem organizacional (Roberts, 1996; Parris, 2025).

3.3.2.1 Formas de *Accountability* e seus Efeitos sobre a Aprendizagem

A literatura identifica múltiplas formas de *accountability*, cada uma com propriedades e efeitos distintos sobre a aprendizagem organizacional (Tetlock, 1985; Roberts, 1991, 1996; Lerner & Tetlock, 1999; Parris, 2025). O que essas perspectivas têm em comum é o reconhecimento de que a *accountability* não é um construto único, mas uma família de práticas com efeitos diferenciados, uns favoráveis à aprendizagem, outros inibidores. As formas **tradicionais** - hierárquica, *backward* e *outcome* - focam nas consequências de ações individuais, geram ambientes potencialmente ameaçadores e favorecem comportamentos defensivos, inibindo a aprendizagem de ciclo duplo. As formas **orientadas ao processo e à melhoria** - *process* e *forward* - deslocam a atenção do resultado para a qualidade do processo decisório e para a identificação de fatores sistêmicos. As formas **relacionais**

e informais - *socializing* e *lateral* - emergem entre pares que se reconhecem mutuamente como competentes, constroem confiança e geram comprometimento coletivo com a segurança.

Tabela 3.3.1: Formas de *accountability* e efeitos sobre a aprendizagem organizacional

Forma	Efeitos sobre a Aprendizagem Organizacional
Hierárquica	Individualiza; foco na autoimagem; inibe relato; sustenta a lógica de culpa individual (*IBL - Individual Blame Logic)*
***Backward* / Retributiva**	Foca em culpa e punição; sustenta *IBL*; inibe ciclo duplo
Outcome	Aumenta estresse decisório; incentiva autojustificação
Process	Melhora a qualidade decisória; favorece avaliação de alternativas; lógica de função organizacional (*OFL - Organizational Function Logic*)
***Forward* / Prospectiva**	Orienta para melhoria sistêmica; favorece *OFL*
***Socializing* / Lateral**	Constrói confiança; gera comprometimento coletivo; favorece relato
***Felt* (Sentida)**	Percepção interna de ser accountable; pode gerar confusão com responsabilidade
Legítima / Ilegítima	Modula todos os demais efeitos via confiança e percepção de intenção

Fontes: *Tetlock, 1985; Roberts, 1991, 1996; Lerner & Tetlock, 1999; Hall et al., 2017; Arbin et al., 2021; Parris, 2025.*

Conceitualmente, é útil articular explicitamente a relação entre os três construtos centrais desta seção (***cultura justa***, ***accountability*** *e* ***aprendizagem organizacional***). A **cultura justa** opera como sistema organizacional. O conjunto de regras, processos e disposições institucionais que regulam respostas a desvios e erros. Dentro desse sistema, **accountability** materializa-se em práticas específicas (hierárquica, processual, prospectiva, restaurativa, entre outras formas mapeadas na Tabela 3.3.1), cada qual com efeitos distintos sobre o comportamento dos profissionais. A qualidade dessas práticas, particularmente quanto à percepção de legitimidade e à orientação retrospectiva ou prospectiva, determina, por sua vez, a capacidade da organização de extrair lições de erros e incidentes, ou seja,

sua **aprendizagem organizacional**. Em síntese: cultura justa é o sistema; accountability *são as* práticas; aprendizagem é o resultado. Esta articulação ancora as discussões subsequentes sobre culpabilidade (3.3.3), dimensões de justiça (3.3.4), abordagens retributivas e restaurativas (3.3.5), cultura de relato (3.3.6) e desafios de implementação (3.3.7).

3.3.3 Classificação de Comportamentos e Determinação de Culpabilidade

Um elemento central das abordagens de cultura justa é a categorização de comportamentos para determinar respostas apropriadas. Reason (1997) propôs uma árvore de decisão para discriminar a culpabilidade de atos inseguros, baseada primariamente na natureza da intenção. Marx (2001) desenvolveu posteriormente um modelo que distingue entre erro humano, comportamento de risco e comportamento imprudente, categorias que envolvem graus crescentes de intencionalidade e desconsideração.

Reason (1997) introduziu o teste de substituição de Neil Johnston como ferramenta fundamental para avaliar culpabilidade: deve-se substituir mentalmente o indivíduo envolvido por outro com qualificações e experiência comparáveis e perguntar se, à luz de como os eventos se desenrolaram e foram percebidos em tempo real, esse novo indivíduo teria se comportado diferentemente. Se a resposta for "provavelmente não", atribuir culpa não tem papel material, servindo apenas para obscurecer deficiências sistêmicas.

A árvore de decisão de Reason considera questões-chave como: as ações e consequências foram intencionais? Houve uso de substâncias não autorizadas? O indivíduo estava violando procedimentos operacionais seguros? Os procedimentos eram disponíveis, funcionais e inteligíveis? A experiência sugere que aproximadamente 90% ou mais dos atos inseguros recaem em categorias isentas de culpa (Reason, 1997).

Na prática organizacional, a aplicação dessas categorias frequentemente recai sobre o que Catino (2008) denomina lógica de culpa individual (*IBL - Individual Blame Logic*): identificam-se culpados individuais, atribuem-se rótulos de negligência e aplicam-se sanções, sem examinar os fatores latentes e sistêmicos que

tornaram o comportamento provável. A abordagem alternativa - a lógica de função organizacional (*OFL - Organizational Function Logic*) – tem como objetivo central aprender com erros e acidentes por meio da identificação de causas indiretas e condições sistêmicas. A distinção entre *IBL* e *OFL* determina não apenas a qualidade das investigações, mas o nível de confiança que os profissionais depositam no sistema de consequências e, portanto, sua disposição para relatar (Catino, 2008; Parris, 2025).

> **Implicações para a investigação de eventos**: *a distinção entre IBL e OFL não é apenas teórica – orienta escolhas metodológicas concretas. Investigações que operam sob lógica IBL tendem a parar na identificação do agente proximal e na proposição de medidas disciplinares; investigações sob lógica OFL avançam para a análise de condições latentes, falhas de barreira e fatores organizacionais que tornaram o evento provável. O teste de substituição de Johnston (Reason, 1997) funciona, na prática, como filtro inicial: se um substituto com qualificações equivalentes teria agido de forma semelhante no mesmo contexto, a investigação deve aprofundar-se na análise sistêmica, não nas características do indivíduo envolvido.*

3.3.4 Três Dimensões da Justiça Organizacional

Dekker e Breakey (2016) argumentam que uma cultura verdadeiramente justa deve abordar três dimensões fundamentais da justiça, que vão além da simples categorização retributiva de comportamentos:

- **Justiça Substantiva:** Refere-se à legitimidade e equidade das próprias regras, regulamentos e procedimentos. Procedimentos percebidos como injustos, inadequados ou desatualizados minam a base moral para responsabilizar indivíduos por não os seguir. Se os trabalhadores veem as regras como arbitrárias ou desconectadas da realidade operacional, a aplicação de sanções será percebida como ilegítima.
- **Justiça Processual:** Estabelece processos legítimos para determinar violações de regras, oferece proteções ao acusado e governa quem deve fazer tais determinações. Inclui garantias como presunção de inocência, direito a representação, julgamento por pares com conhecimento do

trabalho, separação entre investigação de segurança e procedimentos disciplinares, e possibilidade de recurso.

- **Justiça Restaurativa:** Visa restaurar o status do indivíduo envolvido e curar relacionamentos e danos das vítimas e da comunidade após uma falha ética. Enquanto a justiça retributiva sugere que se o erro causou dano, a resposta também deve causar dano (punição), a justiça restaurativa sugere que se o erro causou dano, a resposta deve curar.

Este framework das três dimensões, como qualquer construção teórica, opera como grade interpretativa, não como descrição neutra de propriedades do mundo. Sua utilidade analítica é considerável, mas é importante reconhecer que produz seus próprios objetos (o que conta como justiça substantiva, processual ou restaurativa) e seus próprios silêncios, particularmente quanto às assimetrias de poder entre quem categoriza e quem é categorizado (Henriqson et al., 2014; cf. 3.3.9).

Transversal às três dimensões está a questão da legitimidade percebida. Lerner e Tetlock (1999) documentaram que a accountability é vivenciada pelos indivíduos como legítima ou ilegítima, e que essa percepção - moldada pela confiança depositada em quem a exerce, pela clareza de suas intenções e pela razoabilidade das demandas - determina seus efeitos sobre o comportamento e a aprendizagem. *Accountability* percebida como ilegítima produz efeitos contrários aos desejados: polarização de atitudes, declínio de motivação intrínseca e aumento de estresse. Isso implica que estruturas formalmente corretas de justiça substantiva, processual e restaurativa podem fracassar se as relações de confiança entre trabalhadores e liderança não forem cultivadas (Tyler, 1997).

> **Implicações para a governança organizacional**: *as três dimensões da justiça (substantiva, processual e restaurativa) operam como filtro analítico para diagnosticar pontos de fragilidade em sistemas de cultura justa. Procedimentos desatualizados ou desconectados da realidade operacional fragilizam a justiça substantiva; mecanismos disciplinares opacos ou sem garantias mínimas (representação, recurso) fragilizam a justiça processual; ausência de mecanismos de reparação e reintegração fragiliza a justiça restaurativa. A maturidade do sistema é avaliável pelas três dimensões simultaneamente – uma cultura justa que satisfaz apenas uma ou duas dimensões opera, na prática, com legitimidade reduzida.*

3.3.5 Cultura Justa Retributiva versus Cultura Justa Restaurativa

A literatura contemporânea distingue duas abordagens fundamentais para a cultura justa. A abordagem retributiva, predominante nas implementações organizacionais atuais, foca na correspondência entre tipos de ação humana e respostas gerenciais proporcionais, utilizando algoritmos e árvores de decisão para categorizar comportamentos em graus de culpabilidade (Reason, 1997; Marx, 2001).

Contudo, críticos apontam limitações significativas desta abordagem. Dekker (2008, 2017) argumenta que a linha entre comportamento aceitável e inaceitável não é uma propriedade inerente do ato, mas o resultado de processos de interpretação e atribuição que ocorrem após o ato. A culpabilidade é socialmente construída, e diferentes narrativas sobre o mesmo incidente são sempre possíveis. Ademais, pesquisas demonstram que, conhecendo o resultado, tendemos a superestimar o grau de previsibilidade que o indivíduo poderia ou deveria ter tido – o viés retrospectivo (Dekker, 2017).

A abordagem restaurativa, em contraste, define-se como um processo em que todas as partes interessadas afetadas por uma injustiça têm oportunidade de discutir como foram afetadas e decidir o que deve ser feito para reparar o dano (Dekker & Breakey, 2016). Esta abordagem reconhece múltiplas vítimas em um incidente: não apenas as vítimas primárias (pacientes, passageiros), mas também as segundas vítimas – os profissionais envolvidos que podem sofrer consequências psicológicas significativas.





Figura 3.3.1: Comparação entre os paradigmas retributivo e restaurativo da cultura justa. A diferença entre eles começa, segundo Gershenson, na pergunta que fazemos primeiro. **Fonte:** Gershenson (2026).

Em síntese consolidada por Dekker, Rafferty e Oates (2022, p. 198), a cultura justa restaurativa pode ser definida como uma cultura de confiança, aprendizagem e accountability prospectiva – em oposição à cultura justa retributiva, que se organiza em torno do ofensor, da regra descumprida e da sanção proporcional. Operacionalmente, a resposta restaurativa estrutura-se em torno de três perguntas: quem foi impactado, quais são suas necessidades e de quem é a obrigação de atendê-las? Turner, Stapelberg, Sveticic e Dekker (2022), em compilação utilizada como referência metodológica em Dekker, Rafferty e Oates (2022, p. 201), identificam nove sinais distintivos (*hallmarks*) de uma cultura justa restaurativa em implementação:

1. promoção da cura da confiança, das relações e das pessoas;
2. reconhecimento e apoio às primeiras e segundas vítimas;
3. deslocamento da pergunta "quem fez algo errado" para "o que foi responsável pelo que deu errado";
4. responsabilização dos profissionais como parte do processo de cura, aprendizagem e melhoria;
5. reconhecimento simultâneo das próprias necessidades desses profissionais;
6. atribuição de papéis e responsabilidades a todos os envolvidos;

7. preferência por accountability prospectiva (orientada a salvaguardas e melhorias) em detrimento da retrospectiva (orientada à culpa e à punição);
8. engajamento de todos os stakeholders na revisão pós-incidente; e
9. atribuição explícita de obrigações às lideranças quanto ao apoio aos afetados.

Esses sinais distintivos oferecem critérios verificáveis para distinguir uma implementação genuinamente restaurativa de uma reformulação meramente nominal de práticas retributivas (Dekker, Rafferty & Oates, 2022).

Vale notar, contudo, que os *hallmarks* têm caráter duplo. Como critérios diagnósticos, auxiliam a identificar implementações genuínas; mas, como qualquer conjunto formalizado de critérios, podem também operar como dispositivos disciplinares, gerando novas exigências, técnicas de medição e categorias de adequação/inadequação organizacional (Henriqson et al., 2014). A vigilância crítica sobre seu uso – sobre quem avalia, sobre quem, e com que efeitos sobre as relações de poder na organização – é, por isso, parte integrante da própria implementação restaurativa madura (cf. 3.3.9).

> **Implicações para a gestão da transição**: a passagem do paradigma retributivo ao restaurativo não se decreta – exige escolhas operacionais visíveis e consistentes. Os nove *hallmarks* funcionam, neste sentido, como critérios diagnósticos: organizações em transição genuína apresentam progresso simultâneo em múltiplos *hallmarks*, enquanto reformulações apenas nominais tendem a concentrar-se em mudanças discursivas (renomeação de comitês, novos slogans, comunicação institucional) sem alteração das práticas de resposta a eventos. O acompanhamento longitudinal desses *hallmarks* pode constituir, portanto, instrumento concreto de avaliação da maturidade do sistema.

3.3.6 Cultura de Relato e Construção de Confiança

A cultura justa é um componente essencial de uma cultura de segurança mais ampla, que também inclui uma cultura de relato, uma cultura flexível e uma cultura de aprendizagem (Reason, 1997). A disposição para relatar incidentes está diretamente relacionada à confiança de que a informação fornecida de boa-fé não será usada contra aqueles que a reportaram.

Van Marum et al. (2022) identificaram três categorias principais de barreiras e facilitadores para a confiança no relato de erros em uma cultura justa: ***fatores organizacionais*** (apoio da gestão, abertura sobre tratamento de erros, foco na segurança em vez de culpa individual), ***fatores de equipe*** (relacionamento próximo entre funcionários e supervisores, clareza de papéis, discussão sobre natureza dos erros) e ***experiência*** (treinamento em segurança, confiança em habilidades clínicas, conhecimento do sistema de relato).

A literatura empírica indica que sistemas de relato bem-sucedidos compartilham características comuns: acessibilidade, confidencialidade protegida, separação do processo punitivo, feedback aos relatores demonstrando que ações foram tomadas e envolvimento dos profissionais no processo de melhoria (Dekker, 2017). Como observação prática frequentemente reiterada na mesma literatura, a confiança é difícil de construir e fácil de destruir – uma única resposta organizacional que demonstre que informações divulgadas podem ser usadas contra o relator pode destruir meses ou anos de construção de boa vontade.

Pesquisas em psicologia organizacional acrescentam uma dimensão importante: os efeitos do monitoramento sobre a motivação dependem da percepção das intenções de quem monitora. Quando os profissionais percebem o monitoramento como não-controlador - ou seja, como apoio à qualidade do processo -, não há inibição de motivação ou relato. O efeito negativo aparece quando o monitoramento é percebido como instrumento de controle e punição, mesmo que o sistema formal declare intenções distintas (Enzle & Anderson, 1993). Na indústria de energia, isso implica que inspeções, auditorias e investigações podem servir como facilitadores ou como barreiras ao relato, dependendo não de seu design formal, mas da relação de confiança que os líderes constroem com as equipes operacionais ao longo do tempo.

3.3.7 Desafios na Implementação

A implementação efetiva de uma cultura justa enfrenta diversos desafios. Wachter e Pronovost (2009) destacaram a necessidade de equilibrar a abordagem sem culpa com a responsabilização individual, argumentando que um foco unidimensional em criar uma cultura livre de culpa carrega seus próprios riscos de

segurança. Para certas práticas de segurança maduras, onde sistemas adequados estão em vigor, a falha persistente em aderir deve resultar em consequências.

Heraghty et al. (2020), em estudo empírico sobre o uso de mecanismos de justiça retributiva na análise de acidentes no setor de energia, encontraram que tais mecanismos impactam negativamente a saúde mental do indivíduo, a aprendizagem organizacional e o desempenho organizacional. Identificaram também uma lacuna significativa entre as percepções dos trabalhadores submetidos a punição e aqueles em posição de autoridade para aplicá-la, com gestores tendendo a ver o tratamento como justo mesmo quando trabalhadores expressam discordância.

Reis-Dennis (2018) oferece uma perspectiva contrária, argumentando que o movimento de cultura justa, ao focar exclusivamente em consequências prospectivas orientadas para a segurança, demonstra uma compreensão empobrecida do valor das práticas punitivas voltadas ao passado. A punição apropriada, argumenta, respeita todos os participantes do sistema ao restaurar um equilíbrio de status social e moral que o comportamento inadequado perturbou.

Um desafio adicional diz respeito ao modo de introdução de programas de cultura justa e Fatores Humanos. Arbin et al. (2021) demonstraram que o enquadramento de novas iniciativas em termos de *accountability hierárquica* - comunicando que os trabalhadores "serão responsabilizados" pela adoção das novas práticas – é percebido como mecanismo de controle e tende a gerar resistência. O enquadramento em termos de accountability *socializing* – criando fóruns de discussão entre pares, construindo normas de grupo e apelando ao comprometimento coletivo - produz maior engajamento e sustentabilidade. Este achado tem implicação direta para a gestão da mudança organizacional na indústria de energia: a forma pela qual a liderança comunica e faz cumprir os princípios de cultura justa importa tanto quanto o conteúdo desses princípios (Arbin et al., 2021; Parris, 2025).



Com base na literatura de cultura justa restaurativa (Dekker & Breakey, 2016; Dekker, Rafferty & Oates, 2022), Gershenson (2026)[1] propõe uma interpretação inspirada na teoria das revoluções científicas (Kuhn, 1962/2017) para compreender a transição entre os paradigmas retributivo e restaurativo de cultura justa. A proposta é explicitamente metafórica: aproxima a distinção kuhniana entre cientista normal e cientista extraordinário à oposição entre profissionais que operam dentro do paradigma vigente e profissionais que abrem caminho ao paradigma emergente nas organizações. Por essa leitura, organizações que aprendem com erros operam simultaneamente em dois registros: o do profissional "normal" – que opera processos, garante conformidade e refina o conhecimento existente dentro do paradigma vigente – e o do profissional "extraordinário" – que questiona pressupostos, propõe novas formas de ver o problema e abre caminho para um novo paradigma (Figura 3.3.2, parte superior). Lideranças restaurativas, facilitadores, profissionais de segurança, RHs estratégicos e equipes de compliance humanizado constituem, organizacionalmente, os candidatos a esses agentes "extraordinários" (Figura 3.3.2, parte inferior). A síntese de Gershenson é direta:

> *"Uma cultura justa restaurativa não é mais branda – ela é mais completa. Ela protege, responsabiliza e aprende"* (Gershenson, 2026).

> ***Nota metodológica:*** *a referência a Gershenson (2026) é utilizada nesta seção, com a autorização da autora, como fonte de natureza conceitual e ilustrativa, apoiando a discussão sobre modelos organizacionais de cultura justa restaurativa. Por se tratar de apresentação técnica em contexto institucional (grupo de trabalho na Constellation) – e não de artigo acadêmico publicado e revisado por pares – sua inclusão constitui grey literature aplicada (modelo conceitual desenvolvido em contexto organizacional), não devendo ser interpretada como evidência empírica ou teórica consolidada na literatura científica.*

Para a indústria de energia, essa chave de leitura tem implicação prática: a transformação da cultura justa não se decreta por política – ela requer a identificação e a proteção dos profissionais que, em diferentes níveis hierárquicos, já operam segundo a lógica restaurativa, e a criação de *espaço seguro* para que esse repertório "extraordinário" emerja sem ser silenciado pelo paradigma dominante (Gershenson, 2026; Dekker, Rafferty & Oates, 2022).

Outro desafio é o da accountability sentida (*felt accountability*): profissionais em posições de alta responsabilidade formal frequentemente experienciam *accountability* difusa - sentem-se *accountable* não apenas por suas obrigações definidas, mas por todos os resultados associados à sua área, mesmo quando não detinham controle técnico sobre eles. Quando os sistemas organizacionais reforçam essa *accountability* difusa - atribuindo consequências por eventos fora do controle razoável do indivíduo - criam-se as condições para comportamentos defensivos, ocultação de informações e inibição de relato (Hall et al., 2017; Parris, 2025).



Figura 3.3.2: O paradigma kuhniano aplicado à Cultura Justa organizacional. *A parte superior representa a transição entre o paradigma vigente (profissionais "normais") e o emergente (profissionais "extraordinários"), com a síntese de que organizações maduras não eliminam o "normal", mas criam espaço seguro para o "extraordinário" emergir. A parte inferior identifica os candidatos típicos a esses profissionais na organização.*
Fonte: *Gershenson (2026).*

3.3.8 Implicações para a Indústria de Energia

A indústria de energia, particularmente o setor de óleo e gás offshore, opera em ambientes de alto risco onde a cultura justa é especialmente relevante. A complexidade das operações, o acoplamento estreito entre sistemas e a presença de múltiplas organizações (operadores, contratados, subcontratados) criam desafios únicos para a implementação de princípios de cultura justa.

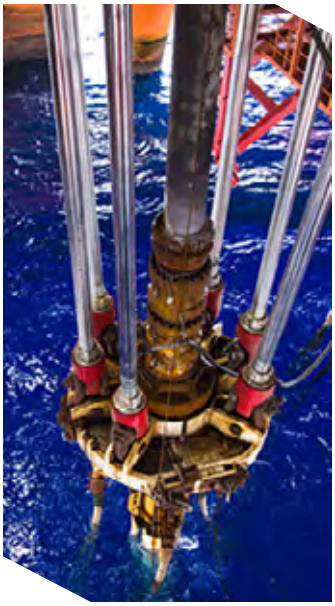
A aplicação bem-sucedida requer consideração da lacuna entre trabalho como imaginado e trabalho como realizado (Hollnagel, 2014). Procedimentos desenvolvidos em escritórios corporativos podem não refletir as realidades e *trade-offs* enfrentados pelos operadores de linha de frente. Uma cultura justa genuína deve reconhecer que violações frequentemente emergem de tentativas de equilibrar múltiplas demandas concorrentes – segurança, produção, eficiência – em contextos em que recursos são limitados e pressões são intensas.



A integração da cultura justa com outros elementos do sistema de gestão de segurança é essencial. Isso inclui alinhamento com processos de investigação de incidentes, sistemas de relato voluntário, programas de observação comportamental e iniciativas de feedback de segurança. O objetivo final é criar um ambiente onde as pessoas sintam segurança psicológica para compartilhar informações sobre riscos e erros, ao mesmo tempo em que compreendem claramente os limites do comportamento aceitável.

Um risco específico para a indústria de energia é o que pode ser denominado captura punitiva do sistema de *accountability*: quando investigações de acidentes - conduzidas por reguladores, comissões de segurança ou pelos próprios gestores – são percebidas pelos profissionais como processos orientados à identificação de culpados e à conformidade legal, em vez de à aprendizagem sistêmica, os mecanismos de cultura justa são esvaziados independentemente de sua formalização. Evidências empíricas de setores de alto risco análogos indicam que essa percepção é comum entre profissionais de linha de frente e está associada ao silêncio organizacional, aumento de procedimentos sem melhoria real de segurança e persistência de eventos repetidos (Catino, 2008; Parris, 2025). Bergström (2019) descreve esse fenômeno como manifestação concreta da apropriação jurídico-gerencial da cultura justa: o que foi concebido como instrumento de empoderamento da linha de frente termina por reforçar a autoridade do aparato regulatório e disciplinar como autoridade para traçar a linha sobre comportamentos individuais – efeito desenvolvido em 3.3.9. A transição genuína para uma cultura justa requer, portanto, que o regulador e as lideranças organizacionais façam

escolhas explícitas e visíveis sobre o papel da *accountability*: é para aprender ou para punir? A resposta a essa pergunta - comunicada não em declarações formais, mas nas respostas concretas a eventos adversos - determina a credibilidade de toda a arquitetura de cultura justa.



Antes de propor indicadores e aplicações concretas, registra-se uma advertência metodológica. A literatura crítica de orientação foucaultiana (Henriqson et al., 2014; Bergström, 2019) demonstra que a operacionalização da cultura justa em indicadores e protocolos é, ela mesma, um movimento discursivo com efeitos – incluindo a produção de novas técnicas de governamentalidade organizacional. Os indicadores e aplicações abaixo devem, portanto, ser tratados não como receita técnica neutra, mas como pontos de observação para diagnóstico crítico e diálogo institucional, atentos à pergunta de Dekker (2017): quem desenha a linha? A subseção 3.3.9 desenvolve esta nota.

Indicadores observáveis de maturidade de cultura justa

Para evitar que o diagnóstico desta seção permaneça em nível abstrato, sugere-se que a avaliação da maturidade do sistema de cultura justa na organização contemple, no mínimo, os seguintes indicadores observáveis (Reason, 1997; Dekker, 2017; EUROCONTROL, 2020):

1. distinção formal, em procedimentos institucionais, entre erro honesto, comportamento de risco e violação deliberada, com critérios de avaliação documentados e conhecidos antecipadamente;
2. separação institucional entre investigação de segurança e procedimentos disciplinares, incluindo, quando aplicável, separação de equipes, prazos e canais de reporte;
3. canal de relato confidencial em operação, com feedback documentado aos relatores sobre as ações tomadas;

4. indicadores de aprendizagem, não apenas taxas de incidentes, incorporados ao painel de desempenho de segurança das unidades operacionais;
5. política formal de proteção e apoio a segundas vítimas, com responsabilidades atribuídas;
6. condições estruturais de cultura justa – incluindo desenho do trabalho, alocação de recursos, margens de manobra dos profissionais e estruturas de autoridade – submetidas a revisão periódica e tratadas como variáveis primárias do sistema; o treinamento de lideranças (até primeiro nível supervisório) nos princípios conceituais é instrumento complementar, não substituto da atenção a essas condições estruturais (Bergström, 2019; cf. 3.3.9).

Aplicações concretas na investigação de eventos de segurança



Em complemento aos indicadores estruturais, a transição para uma cultura justa restaurativa manifesta-se, na prática da investigação de eventos, em pelo menos quatro escolhas metodológicas: (i) uso explícito do teste de substituição de Johnston como filtro inicial, antes de qualquer encaminhamento disciplinar – com reconhecimento explícito de que o teste é aplicado por alguém sobre o caso de outrem, exigindo salvaguardas processuais contra seu uso instrumental (representação do profissional avaliado, transparência do processo, possibilidade de revisão; cf. 3.3.9); (ii) inclusão sistemática da análise de fatores latentes (Reason, 1997) e de condições organizacionais como componentes obrigatórios da Root Cause Analysis (RCA); (iii) inclusão, no protocolo pós-evento, de avaliação e cuidado da segunda vítima, em processo separado da apuração disciplinar; (iv) revisão por pares com conhecimento do trabalho real antes de qualquer recomendação de consequência individual. Estas práticas são consistentes com os hallmarks de implementação restaurativa identificados por Turner et al. (2022) e operacionalizam, no nível da rotina de investigação, os princípios discutidos ao longo da seção.

3.3.9 Nota reflexiva: cultura justa como objeto discursivo

Esta seção construiu um percurso teórico-prático da cultura justa para a indústria de energia, culminando em indicadores operacionais e aplicações na investigação de eventos. Para encerrar com honestidade intelectual, é necessário um movimento reflexivo: reconhecer que a própria construção discursiva da cultura justa, incluindo este compêndio, produz efeitos que merecem atenção crítica.

Henriqson, Schuler, van Winsen e Dekker (2014), em análise arqueogenealógica de inspiração foucaultiana, demonstram que a cultura de segurança emergiu como objeto discursivo em resposta a necessidades políticas específicas, a explicação de grandes acidentes industriais entre as décadas de 1970 e 1990 – e que sua consolidação produziu quatro efeitos identificáveis: (i) homogeneidade normativa, que silencia conflitos entre segurança, produção, custo e qualidade ao tratar a segurança como compromisso moral compartilhado; (ii) efeitos disciplinares sobre os corpos e comportamentos dos trabalhadores; (iii) efeitos biopolíticos sobre populações organizacionais, via técnicas de medição, classificação e comparação; e (iv) governamentalidade, articulando a conduta individual à norma organizacional.

Bergström (2019) avança o argumento examinando especificamente a trajetória da cultura justa – do conceito acadêmico (Reason, Dekker) ao mercado de consultoria e à apropriação regulatória (notadamente a EASA 376/2014 na aviação europeia). Sua tese: a cultura justa, introduzida com a intenção de empoderar profissionais de linha de frente a reportar erros sem medo de retaliação, produziu o efeito discursivo oposto – empoderou o aparato judicial e regulatório como autoridade para traçar a linha. Em pesquisa com profissionais de manutenção aeronáutica, Woodlock (2017, apud Bergström, 2019) documenta que a governança da EASA é experimentada "como uma força coercitiva… uma relação assimétrica de poder".

Para a indústria de energia, essa advertência tem implicações práticas. **Primeiro**, os indicadores e aplicações propostos em 3.3.8 devem ser lidos não como receita técnica neutra, mas como conjunto de práticas que produzem seus próprios efeitos, incluindo o risco de transformar o profissional de linha de frente no objeto principal da reforma cultural, em detrimento da atenção às estruturas organizacionais e às assimetrias de poder. **Segundo**, vale interrogar permanentemente

quem define o que conta como erro honesto, comportamento de risco ou violação deliberada – pergunta que Dekker (2017) sintetiza: "não há linha; só há pessoas que a desenham". **Terceiro**, Bergström (2019) sugere uma agenda descritiva, e não apenas normativa, para a ciência da segurança: tão importante quanto prescrever práticas é descrever criticamente os efeitos das práticas existentes, inclusive os desta seção.

Esta nota reflexiva não invalida o conteúdo anterior. Fortalece-o ao explicitar seus limites: a cultura justa é uma intervenção discursiva valiosa, mas não neutra; sua operacionalização requer vigilância crítica contínua sobre os efeitos de poder que produz. A literatura de Henriqson et al. (2014) e Bergström (2019) deve, portanto, ser tratada não como contraponto a Reason, Dekker e Pellegrino, mas como parte integrante do quadro intelectual da cultura justa – a dimensão crítica que impede que o conceito se torne, ele próprio, mecanismo de captura.



Referências da Seção 3.3

Arbin, K., Frostenson, M., Helin, S., & Borglund, T. (2021). Explaining workers' resistance against a health and safety programme: An understanding based on hierarchical and social accountability. Safety Science, 136, 105131. https://doi.org/10.1016/j.ssci.2020.105131

Bergström, J. (2019). The discursive effects of safety science. In J.-C. Le Coze (Ed.), Safety science research: Evolution, challenges and new directions (pp. 173–186). CRC Press.

Catino, M. (2008). A review of literature: Individual blame vs. organizational function logics in accident analysis. Journal of Contingencies and Crisis Management, 16(1), 53–62.

Dekker, S. W. A. (2008). Just culture: Who gets to draw the line? Cognition, Technology & Work, 10(4), 249–253. https://doi.org/10.1007/s10111-008-0110-7

Dekker, S. W. A. (2017). Just culture: Restoring trust and accountability in your organization (3rd ed.). CRC Press.

Dekker, S. W. A., & Breakey, H. (2016). 'Just culture:' Improving safety by achieving substantive, procedural, and restorative justice. Safety Science, 85, 187–193. https://doi.org/10.1016/j.ssci.2016.01.018

Dekker, S. W. A., Rafferty, J., & Oates, A. (Eds.). (2022). *Restorative just culture in practice: Implementation and evaluation*. Routledge/Productivity Press. https://doi.org/10.4324/9781003162582

Enzle, M. E., & Anderson, S. C. (1993). Surveillant intentions and intrinsic motivation. Journal of Personality and Social Psychology, 64(2), 257–266. https://doi.org/10.1037/0022-3514.64.2.257

EUROCONTROL. (2020). Just Culture: Guidance material for interfacing with the judicial system. EUROCONTROL Performance Review Commission.

Gershenson, B. (2026). *Cultura justa restaurativa: um desafio para todas as camadas da cultura organizacional* [Apresentação ao Grupo de Trabalho de Cultura Justa]. Constellation, Macaé, 21 maio 2026.

Hall, A. T., Frink, D. D., & Buckley, M. R. (2017). An accountability account: A review and synthesis of the theoretical and empirical research on felt accountability. Journal of Organizational Behavior, 38(2), 204–224.

Henriqson, É., Schuler, B., van Winsen, R., & Dekker, S. W. A. (2014). The constitution and effects of safety culture as an object in the discourse of accident prevention: A Foucauldian approach. Safety Science, 70, 465–476. https://doi.org/10.1016/j.ssci.2014.07.004

Heraghty, D., Rae, A. J., & Dekker, S. W. A. (2020). Managing accidents using retributive justice mechanisms: When the just culture policy gets done to you. Safety Science, 126, 104677. https://doi.org/10.1016/j.ssci.2020.104677

Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate.

Hoskin, K. (1996). The 'awful idea of accountability': Inscribing people into the measurement of objects. In R. Munro & J. Mouritsen (Eds.), Accountability: Power, ethos and the technologies of managing (pp. 265–282). Thomson.

Ieraci, S. (2007). Responsibility versus accountability in a risk-averse culture. Emergency Medicine Australasia, 19(1), 63–64. https://doi.org/10.1111/j.1742-6723.2007.00963.x

Kuhn, T. S. (2017). A estrutura das revoluções científicas (13ª ed., B. V. Boeira & N. Boeira, Trads.). Perspectiva. (Obra original publicada em 1962).

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. Psychological Bulletin, 125(2), 255–275. https://doi.org/10.1037/0033-2909.125.2.255

Lilley, S. (1996). Refusing the gift of empowerment: A study of management response to a recognition of dependency. In R. Munro & J. Mouritsen (Eds.), Accountability: Power, ethos and the technologies of managing (pp. 117–131). Thomson.

Marx, D. (2001). Patient safety and the 'just culture': A primer for health care executives. Columbia University.

Parris, R. (2025). Accountability: A lived experience [Master's thesis, Lund University]. Division of Risk Management and Societal Safety, Faculty of Engineering.

Pellegrino, F. (2019). The just culture principles in aviation law. Springer.

Reason, J. (1997). Managing the risks of organizational accidents. Ashgate.

Reis-Dennis, S. (2018). What 'Just Culture' doesn't understand about just punishment. Journal of Medical Ethics, 44(12), 1–4. https://doi.org/10.1136/medethics-2018-104911

Roberts, J. (1991). The possibilities of accountability. Accounting, Organizations and Society, 16(4), 355–368. https://doi.org/10.1016/0361-3682(91)90027-C

Roberts, J. (1996). From discipline to dialogue: Individualising and socialising forms of accountability. In R. Munro & J. Mouritsen (Eds.), Accountability: Power, ethos and the technologies of managing (pp. 40–61). Thomson.

Sharpe, V. A. (2003). Promoting patient safety: An ethical basis for policy deliberation. Hastings Center Report, 33(5 suppl), S1–S20. https://doi.org/10.2307/3528148

Tetlock, P. E. (1985). Accountability: The neglected social context of judgment and choice. Research in Organizational Behavior, 7, 297–332.

Turner, K., Stapelberg, N. J., Sveticic, J., & Dekker, S. W. A. (2022). Inconvenient truths in suicide prevention: Why a restorative just culture should be implemented alongside a zero suicide framework. *Australian & New Zealand Journal of Psychiatry, 56*(6), 571–581. https://doi.org/10.1177/0004867420918659

Tyler, T. R. (1997). The psychology of legitimacy: A relational perspective on voluntary deference to authorities. Personality and Social Psychology Review, 1(4), 323–345. https://doi.org/10.1207/s15327957pspr0104_4

Van Marum, S., Verhoeven, D., & de Rooy, D. (2022). The barriers and enhancers to trust in a just culture in hospital settings: A systematic review. Journal of Patient Safety, 18(8), e1205–e1211. https://doi.org/10.1097/PTS.0000000000001048

Wachter, R. M., & Pronovost, P. J. (2009). Balancing 'no blame' with accountability in patient safety. New England Journal of Medicine, 361(14), 1401–1406. https://doi.org/10.1056/NEJMsb0903885

3.4 Análise de Confiabilidade Humana (HRA) e Tarefas Críticas

Autores: André Gandini e Rafael Ceni de Almeida

3.4.1 Introdução e Contexto Regulatório

A Análise de Confiabilidade Humana (HRA, do inglês *Human Reliability Analysis*) é uma abordagem sistemática para identificar, analisar e quantificar a contribuição humana para o risco em sistemas complexos. Originalmente desenvolvida na indústria nuclear, a HRA evoluiu para métodos específicos da indústria de petróleo e gás, permitindo avaliar a probabilidade de erros humanos em tarefas críticas de segurança operacional.

No contexto regulatório brasileiro, a NT 10/2023 da ANP estabelece que devem ser avaliadas por análise de confiabilidade humana **apenas as tarefas críticas contidas em procedimentos críticos**. Esta delimitação é fundamental para direcionar os recursos de análise para onde há maior impacto na prevenção de acidentes operacionais associados a grandes emergências.

A HRA busca responder a questões fundamentais: quais erros humanos são possíveis em uma determinada tarefa? Qual a probabilidade desses erros? Quais fatores influenciam essa probabilidade? Como os erros podem ser prevenidos ou mitigados através do design de sistemas, procedimentos e condições de trabalho?

3.4.2 Elementos Críticos de Segurança Operacional

Conforme a NT 10/2023 e o regulamento SGSO, os elementos são considerados críticos quando: (i) essenciais para prevenção ou mitigação de acidente operacional associado a grandes emergências; ou (ii) em caso de falha, falta ou degradação possam provocar tal acidente. A classificação inclui três categorias:

- **Equipamento Crítico:** qualquer equipamento, componente ou elemento estrutural da instalação essencial para prevenção ou mitigação, ou que em caso de falha possa provocar acidente operacional.
- **Sistema Crítico:** sistemas de controle, detecção, alarme ou intertravamento com função de segurança operacional.
- **Procedimento Crítico:** Um procedimento ou critério capaz de prevenir ou mitigar um acidente operacional associado a grandes emergências; ou cuja falha ou ausência de execução possa causar ou contribuir para acidente operacional associado a grandes emergências.

Critérios para Identificação de Procedimentos Críticos

Um procedimento é considerado crítico quando atende a pelo menos um dos seguintes critérios:

a. Em análise de risco vinculada ao HSE Case (*Health, Safety and Environment Case* - documento de segurança da instalação; análogo ao *Safety Case*) da unidade, o procedimento é salvaguarda correlacionada a cenários de acidentes operacionais associados a grandes emergências, com alta severidade para pessoas e meio ambiente.
b. Já se sabe que ocorreram incidentes (acidentes ou quase-acidentes) de segurança de processo, correlacionados a cenários de acidentes operacionais associados a grandes emergências, com impactos reais ou potenciais de alta severidade a pessoas e meio ambiente.
c. O procedimento é de teste, inspeção e/ou manutenção de equipamentos e sistemas críticos, abrangendo atividades de teste e/ou, inspeção que sejam correspondentes a Verificações de Elemento Crítico de Segurança Operacional (realizadas como parte e durante a execução da sequência operacional de construção ou intervenção no poço, ou outras atividades operacionais como navegação, entrada na locação etc. Em relação a manutenção, entende-se a não aplicabilidade para tarefas rotineiras de manutenção, exceto caso as tarefas sejam relacionadas a manutenção dos conjuntos solidários de barreiras em caráter operacional.
d. O procedimento foi criado como contingência a uma falha ou degradação de equipamento ou sistema crítico, na medida em que esses pro-

cedimentos de contingência já estejam previstos dentro do sistema de gestão na empresa / lista de equipamentos críticos. Do contrário seriam tratados por gestão de mudança.

Tarefa Crítica de Segurança Operacional

Tarefa Crítica de Segurança Operacional é aquela cuja falha de execução ou omissão possa causar, contribuir ou deixar de reduzir os efeitos de um acidente associado a grandes emergências. Normalmente, esta tarefa está relacionada a uma interação humano-máquina, ou seja, a interação com algum equipamento ou sistema crítico.

Verificação de Elemento Crítico de Segurança Operacional (VECSO): atividade programada para testar e confirmar, com base nos Padrões de Desempenho estabelecidos, se os Elementos Críticos de Segurança Operacional estão desempenhando ou desempenharão sua função requerida quando demandada.

3.4.3 Processo de Identificação e Seleção de Tarefas Críticas para HRA

A identificação e análise de tarefas críticas segue um processo estruturado conforme a NT 10/2023 e o *Guidance on Human Factors Safety Critical Task Analysis* do *Energy Institute*:

Identificação de Tarefas Críticas

A identificação de tarefas críticas pode ser baseada em três abordagens:

a. **Matriz de risco:** considerando o cruzamento entre nível de envolvimento humano e consequência potencial. Para efeito de HRA, incluem-se as tarefas operacionais (excluem-se as puramente administrativas ou de gestão) de impacto médio-alto, alto-médio ou alto-alto.
b. **Estudos Bow-tie existentes:** tarefas que são por si só barreiras nos Bow-ties, ou que suportam diretamente a efetividade de barreiras, podem ser consideradas como tarefas críticas de segurança.

c. **HSE Case da unidade:** vinculando procedimentos a cenários de acidentes operacionais associados a grandes emergências identificados nos estudos HAZID e Bow-tie. Esta é a abordagem central para *drilling contractors* que organizam sua gestão de risco em torno do HSE Case (IADC, 2015), conforme detalhado na seção 3.6.

As três abordagens são complementares: a matriz de risco oferece triagem inicial ampla; os *Bow-ties* existentes apontam tarefas diretamente conectadas as barreiras de MAH; o HSE Case fornece a vinculação formal e auditável entre procedimentos e cenários de grandes emergências, garantindo cobertura sistemática e rastreabilidade para fins regulatórios.

3.4.4 Métodos de Análise de Confiabilidade Humana

Conforme as seções 6.1 a 6.5 da NT 10/2023, existem diversas técnicas de análise de confiabilidade humana validadas para a indústria de óleo e gás. As metodologias são validadas por bancos de dados que comprovam o impacto de fatores influenciadores de desempenho (PSFs - *Performance Shaping Factors*) no desempenho humano, sendo o risco medido através da probabilidade de erro humano (HEP - *Human Error Probability*).

Este compêndio, recomenda a aplicação dos seguintes métodos:

PetroHRA

O método PetroHRA foi desenvolvido especificamente para a indústria de petróleo e gás pelo IFE (*Institute for Energy Technology*). Contém fatores modeladores de performance específicos para o contexto offshore, incluindo: complexidade da tarefa, tempo disponível, procedimentos, ambiente de trabalho e suporte organizacional.

O método foi originalmente desenvolvido para avaliar a probabilidade de falhas humanas em cenários de eventos pós-iniciadores (eventos do Tipo C), que ocorrem no lado direito do diagrama Bow-tie. Entretanto, mediante ajustes metodológicos propostos por Monteiro et al. (2024), o método pode ser aplicado também a tarefas pré-iniciadoras e iniciadoras.

Vantagens do PetroHRA: mediante a padronização pela indústria, com o tempo sua aplicação pode tornar a análise quantitativa de confiabilidade humana mais simples e consistente entre diferentes organizações.

APOA (Analysis of Pre-Accident Operator Actions)

A Análise das Ações Pré-Acidente do Operador (APOA) é um método **qualitativo** que pode ser aplicado para analisar tarefas críticas de segurança nas quais o desempenho humano tem papel vital na prevenção de acidentes. O foco do APOA está em:

- Operações críticas de segurança nas quais erros podem desencadear eventos (eventos do Tipo B - iniciadores).
- Tarefas nas quais o desempenho incorreto pode degradar barreiras (eventos do Tipo A - pré-iniciadores).

O método APOA foi desenvolvido especificamente para capturar e reduzir riscos associados a erros pré-iniciadores e iniciadores, que geralmente ocorrem no lado esquerdo do diagrama Bow-tie.

Outros Métodos Aceitos

A NT 10/2023 também reconhece como melhores práticas da indústria:

- **HEART e HEART+ (*Human Error Assessment and Reduction Technique*):** métodos baseados em fatores de condição de erro.
- **SPAR-H (*Standardized Plant Analysis Risk – Human Reliability Analysis*):** método simplificado de ampla utilização, que serviu de base para o PetroHRA.
- **CREAM (*Cognitive Reliability and Error Analysis Method*):** método baseado em modelo contextual de controle cognitivo.
- **THERP** (***Technique for Human Error Rate Prediction*):** método pioneiro desenvolvido para a indústria nuclear.

3.4.5 Estabelecimento de Efetivo Mínimo

O estabelecimento de efetivo mínimo é requisito da NT 10/2023 para garantir pessoal adequado para operação segura. **Efetivo mínimo** é a quantidade mínima necessária de mão de obra para operar uma instalação com segurança.

A quantidade de trabalhadores deve ser calculada considerando uma análise temporal de todas as tarefas contidas nos procedimentos críticos operacionais e no plano de resposta a emergência.

Metodologia de Cálculo

Conforme o Guia IADC Brasil (2025), o efetivo mínimo é calculado separadamente para dois cenários:

- Efetivo mínimo para tarefas críticas operacionais (exceto PRE).
- Efetivo mínimo para tarefas do Plano de Resposta a Emergência (PRE).

O efetivo mínimo a ser considerado deve ser **o maior entre os calculados nos dois cenários**. A separação justifica-se porque, em situação de emergência, todas as atividades são interrompidas e o efetivo a bordo ou se dedica à emergência ou se prepara para abandono da unidade.

Etapas do Estudo de Efetivo Mínimo

1. **Análise de tarefas:** decomposição em sub etapas, podendo utilizar a HTA da análise de confiabilidade humana.
2. **Identificação de funções:** determinação das funções/cargos responsáveis por cada subtarefa.
3. **Levantamento dos tempos:** a análise temporal pode utilizar, conforme aplicável, os seguintes métodos (Guia IADC Brasil, 2025; Energy Institute, 2017):

a. Tempos padrão previstos em procedimentos ou instruções de trabalho;
b. Estimativa pelo pessoal que executa, experiente na função;
c. Histórico de plataformas similares;
d. Cronometragem de exercícios simulados;
e. Cronometragem da execução real das tarefas (referência para refinamento posterior).

1. **Consolidação:** agregação dos tempos por função e cargo, considerando tempo de deslocamento, dificuldades de acesso (a válvulas, equipamentos e demais componentes) e tarefas com execução simultânea.
2. **Determinação do efetivo:** divisão do tempo total pelo tempo disponível durante o turno (descontados intervalos regulamentares como refeições e reuniões periódicas), arredondando para cima ao próximo número inteiro.

Nota sobre refinamento progressivo: *O Guia IADC Brasil (2025) reconhece que a cronometragem real de tarefas é a base de referência ideal, mas pode não ser viável durante a implantação do estudo ou para tarefas executadas apenas em situações reais de emergência.* **É aceitável que o levantamento inicial seja construído com base em tempos padrão de procedimento, estimativas de pessoal experiente ou histórico de unidades similares, sendo progressivamente substituído por medições reais à medida que as tarefas críticas são executadas e cronometradas em campo ou em exercícios simulados**. *Esta abordagem iterativa é coerente com a natureza dos estudos de efetivo mínimo como instrumentos vivos de gestão, sujeitos a revisão periódica e atualização à luz da experiência operacional acumulada.*

Nota 2: *Em termos de equipes de resposta à emergência, o mínimo não pode ser inferior ao estabelecido por regulamento da Marinha do Brasil, ainda que valor inferior seja estimado pela metodologia. Esta restrição está alinhada à Resolução A.1047(27) da IMO e é normalmente refletida no Certificado de Segurança de Tripulação (CTS) da unidade.*

Articulação com a HRA e a Segurança de Processos

O estudo de efetivo mínimo é metodologicamente independente da HRA quantitativa, mas compartilha com ela a base de análise de tarefas (HTA). Na prática, o pipeline recomendado é: (i) identificação das tarefas críticas a partir do HSE Case e dos Bow-ties (seção 3.6); (ii) decomposição via HTA, reutilizada para HRA e para efetivo mínimo; (iii) levantamento e refinamento progressivo dos tempos; (iv) determinação do efetivo mínimo. Esta integração evita duplicação de esforço, garante coerência entre estudos e responde de forma articulada aos requisitos correlatos da NT 10/2023 sobre confiabilidade humana, tarefas críticas e dimensionamento de equipe.



Referências da Seção 3.4

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. (2007). *Resolução ANP nº 43/2007 – Regulamento Técnico do SGSO*. ANP.

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. (2023). *Nota Técnica nº 10/2023/SSO-CSO/SSO/ANP-RJ*. ANP.

Center for Chemical Process Safety, & Energy Institute. (2018). Bow ties in risk management: A concept book for process safety. Wiley

Energy Institute. (2017). *Guidance on ensuring safe staffing levels* (1ª ed.). Energy Institute.

Energy Institute. (2020). *Guidance on human factors safety critical task analysis* (2ª ed.). Energy Institute.

Energy Institute. (2022). *Guidance on quantified human reliability analysis (QHRA)* (2ª ed.). Energy Institute;

Health and Safety Executive. (2009). *Review of human reliability assessment methods* (RR679). HSE Books.

International Association of Drilling Contractors. (2015). *Health, safety and environment case guidelines for mobile offshore drilling units* (Issue 3.6). IADC.

International Maritime Organization. (2011). *Resolution A.1047(27) — Principles of minimum safe manning*. IMO.

Institute for Energy Technology. (2022). *The Petro-HRA guideline* (Revisão 1, Vols. 1–2). Institute for Energy Technology.

Kirwan, B. (2017). *A guide to practical human reliability assessment*. CRC Press.

Monteiro, G. P., Fernander, M., Diniz, F., & Sertã, C. S. B. (2024). *Human reliability analysis of pre-initiator and initiator events*. DNV.

Øie, S., & Fernander, M. (2022). *Analysis of pre-accident operator actions (APOA) – Methodology guide*. Institute for Energy Technology.

3.5 Engenharia de Fatores Humanos (HFE)

Autores: André Gandini e Rafael Ceni de Almeida

3.5.1 Introdução à Engenharia de Fatores Humanos (HFE)

A Engenharia de Fatores Humanos (HFE, do inglês *Human Factors Engineering*) aplica princípios de ergonomia física e cognitiva ao design de sistemas sociotécnicos. O objetivo é assegurar que sistemas, equipamentos e ambientes de trabalho sejam projetados considerando as capacidades e limitações humanas, reduzindo a probabilidade de erro e otimizando o desempenho.

O IOGP 454 (*Human Factors Engineering in Projects*) e a NT 10/2023 da ANP estabelecem diretrizes específicas para aplicação de HFE na indústria de energia brasileira. O design de salas de controle, interfaces humano-máquina e sistemas de alarme é considerado área fundamental para HFE devido ao alto impacto na gestão de riscos de grandes acidentes (MAHs, do inglês *Major Accident Hazards*).

3.5.2 Atividades-Chave de HFE conforme IOGP 454

O IOGP 454 estabelece sete atividades centrais de HFE que devem ser consideradas ao longo de todo o ciclo de vida do projeto:

1. **Análise dos requisitos das tarefas:** ocorre em fase preliminar do projeto, analisando quanto os equipamentos/sistemas/tecnologias selecionados demandam interação humana.
2. **Análise da criticidade de válvulas:** categorização de válvulas conforme criticidade para operações normais e de emergência.
3. **Triagem e revisão de pacotes de fornecedores:** avaliação de HFE em equipamentos fornecidos por terceiros.
4. **Análise e revisão da sala de controle:** design do ambiente operacional

para tomada de decisão e resposta a emergências.

5. **Análise e revisão de interfaces humano-máquina (IHM):** design de interfaces para operação segura e eficiente.
6. **Análise e revisão de sistemas de alarme:** racionalização e gerenciamento de alarmes.
7. **Revisão do projeto de layout:** arranjo físico para operações seguras, acessíveis e eficientes.

> **Nota**: *Para instalações já em operação, as atividades 1 (Análise dos requisitos das tarefas) e 3 (Triagem de pacotes de fornecedores) são geralmente consideradas não aplicáveis, a menos que haja modificações significativas.*

3.5.3 Análise de Sala de Controle

A análise de sala de controle visa garantir que o ambiente operacional proporcione condições adequadas para tomada de decisão e resposta a emergências. Conforme IOGP 454, os aspectos a avaliar incluem:

- Layout e arranjo físico.
- Visibilidade de displays e indicadores.
- Níveis de ruído e iluminação.
- Acesso a controles críticos.
- Ergonomia dos postos de trabalho.

Campo de Aplicação para Plataformas de Perfuração

Para a aplicação da NT 10/2023 em plataformas de perfuração offshore, a análise deve abranger, no mínimo:

- **Passadiço:** sala de controle de navegação marítima (*wheelhouse*).
- **Cabine do sondador:** sala de controle de perfuração (*driller's control room* ou *doghouse*).
- **Sala de Controle de Motores (ECR):** *Engine Control Room*.

3.5.4 Interface Humano-Máquina (IHM)

Quando um projeto envolve a introdução de novas Interfaces Humano-Máquina (IHMs) ou a modificação de IHMs existentes, a aplicação de HFE é essencial para garantir a usabilidade do sistema e reduzir o risco de erro humano.

A revisão de IHM avalia se as interfaces existentes permitem operação segura e eficiente. Aspectos críticos incluem:

- Clareza e consistência das telas.
- Organização lógica da informação.
- Feedback adequado das ações do operador.
- Prevenção de erros de entrada de dados.
- Suporte à consciência situacional do operador.

Em projetos de óleo e gás, a aplicação de HFE é mais frequentemente necessária no desenvolvimento de Sistemas de Controle Distribuído (DCS). Qualquer alteração significativa nas interfaces de equipamentos locais também deve passar por revisão de HFE.

3.5.5 Sistemas de Alarme



Um sistema de alarmes tem como propósito identificar anomalias durante os processos operacionais e de manutenção, com objetivo principal de garantir a segurança das pessoas e do meio ambiente, redução de custos e oportunidades de melhoria.

A análise de sistemas de alarme segue as diretrizes da IEC 62682 e EEMUA 191. Os sistemas-alvo em plataformas de perfuração incluem:

- Posicionamento dinâmico e navegação.
- Lastro e propulsão.
- Geração de energia.

- Combate a incêndio e monitoramento de fogo e gás.
- Perfuração e controle de poço.
- Guindastes.

Para unidades em operação, recomenda-se realizar um *gap analysis* para identificar desvios em relação às boas práticas de gerenciamento de alarmes.

3.5.6 Análise de Criticidade de Válvulas

A análise de criticidade de válvulas categoriza válvulas conforme sua importância para operações normais e de emergência. Conforme ASTM F1166-23, as válvulas são classificadas em três categorias:

- **Categoria 1:** válvulas essenciais para operações normais ou de emergência onde acesso rápido e desimpedido é essencial (ex.: válvulas de desligamento de emergência, válvulas de controle, válvulas de alívio).
- **Categoria 2:** válvulas não críticas para operações normais ou de emergência, mas que precisam ser acessadas para operações ou manutenção de rotina.
- **Categoria 3:** válvulas usadas ou inspecionadas raramente ou com pouca frequência.

Válvulas de Categoria 1 devem ter acesso permanente no nível do convés ou por superfície elevada permanente. Exemplos típicos incluem: válvulas de controle e seus by-passes, válvulas de alívio e despressurização, válvulas de desligamento de emergência (ESD), e válvulas de transferência de carga líquida de hidrocarbonetos.

3.5.7 Revisão de Layout

A revisão de layout assegura que espaços de trabalho permitam operações seguras, acessíveis e eficientes. Os aspectos a avaliar incluem:

- Rotas de acesso e saídas de emergência.

- Escadas e passarelas.
- Iluminação e sinalização.
- Acessibilidade e conforto térmico.

3.5.8 Aplicação em Unidades em Operação

Para instalações existentes em fase de operação, espera-se que possuam documentação de projeto (Filosofia de Segurança, Guia de HFE, ou Especificações Técnicas) que demonstre quais normas e práticas foram utilizadas.

Para os casos em que o projeto não tenha adotado as melhores práticas indicadas, espera-se:

1. ***Gap analysis*:** identificação de não conformidades em relação às melhores práticas.
2. **Vistoria presencial:** validação das condições reais versus documentação.
3. **Análise de trade-offs:** quando modificações físicas não são viáveis.
4. **Priorização baseada em risco:** considerando risco operacional e viabilidade técnico-financeira.
5. **Plano de ação e evidências de implementação:** para encerrar não conformidades identificadas.
6. **Medidas mitigadoras:** para gaps não resolvidos.



Referências da Seção 3.5

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. (2023). *Nota Técnica nº 10/2023/SSO-CSO/SSO/ANP-RJ*. ANP.

American Petroleum Institute. (s.d.). *Human factors in new facility design tool*. API.

ASM Consortium. (2008). *Effective console operator HMI design practices*. ASM Consortium.

ASTM International. (2023). *Standard practice for human engineering design for marine systems, equipment, and facilities* (ASTM F1166-23). ASTM International.

Engineering Equipment and Materials Users' Association. (2010). *Process plant control desks utilizing human-computer interfaces* (EEMUA 201, 2ª ed.). EEMUA.

Engineering Equipment and Materials Users' Association. (2013). *Alarm systems – A guide to design, management and procurement* (EEMUA 191, 3ª ed.). EEMUA.

International Electrotechnical Commission. (2022). *IEC 62682: Management of alarm systems for the process industries*. IEC.

International Association of Drilling Contractors Brasil. (2025). *Guia de boas práticas – Fatores humanos com foco na ANP NT 10/2023* (Revisão J). IADC Brasil.

International Association of Oil & Gas Producers, & Energy Institute. (2014). *Human factors engineering in projects* (IOGP Report 454). IOGP.

International Organization for Standardization. (2000–2013). *ISO 11064: Ergonomic design of control centres* (Partes 1–7). ISO.

International Organization for Standardization. (s.d.). *ISO 9241: Ergonomics of human-system interaction* (várias partes). ISO.

International Organization for Standardization. (2011). ISO 26800: Ergonomics – General approach, principles and concepts. ISO.

NORSOK. (2018). NORSOK S-002: Working environment. Standards Norway.

SINTEF. (2011). CRIOP: A scenario method for crisis intervention and operability analysis (Report A4312). SINTEF.

3.6 Segurança de Processo

Autores: André Gandini e Rafael Ceni de Almeida

Revisão: Gilsa Monteiro

3.6.1 Introdução e Contexto Histórico

A Segurança de Processos (Process Safety) constitui uma das disciplinas mais críticas no ecossistema de Fatores Humanos da indústria de energia. Seu objeto é a prevenção e mitigação de eventos acidentais de grande magnitude decorrentes de falhas em processos industriais – vazamentos de hidrocarbonetos, explosões, incêndios e emissões tóxicas – que têm potencial para causar múltiplas fatalidades, danos ambientais severos e perdas catastróficas de ativos (CCPS, 2007; Hopkins, 2012). Este escopo a distingue fundamentalmente da segurança pessoal (segurança ocupacional)[2], cujo foco recai sobre lesões individuais de trabalhadores – distinção que, conforme demonstrado pelos desastres de Texas City (2005) e Macondo (2010), pode ter consequências fatais quando negligenciada.

A disciplina tem raízes nos grandes acidentes industriais das décadas de 1970 e 1980 – Flixborough (1974), Seveso (1976), Bhopal (1984) e Piper Alpha (1988) – que revelaram a insuficiência das abordagens de segurança centradas no comportamento individual para prevenir catástrofes sistêmicas. O desastre de Flixborough, com 28 mortos, expôs a ausência de gestão formal de modificações; Bhopal, com mais de 3.500 mortos, revelou como barreiras de contenção podem degradar-se sistematicamente sem que a organização perceba; Piper

2 Adota-se neste compêndio a expressão segurança pessoal (*personal safety*), seguindo Hopkins (2008), por ser conceitualmente mais precisa para designar o ramo aqui contrastado com a segurança de processos. Na primeira menção, mantém-se "segurança ocupacional" entre parênteses, por ser a expressão consagrada no contexto brasileiro. A ressalva de Hopkins fundamenta a escolha: todos os perigos presentes no ambiente de trabalho, pessoais ou de processo, afetam a segurança ocupacional em sentido amplo; a expressão "segurança pessoal" delimita com maior rigor o ramo voltado às lesões que atingem o trabalhador individualmente, reservando "segurança de processos" aos eventos de perda de contenção e de integridade. Essa precisão terminológica é especialmente relevante para a discussão de SIF/Potencial SIF (Seção 4.4.2), cujo objeto é justamente a exposição a consequências severas no ramo pessoal.



Alpha, com 167 mortos, demonstrou como falhas em sistemas de permissão de trabalho e comunicação entre turnos podem precipitar cascatas fatais (Lees, 2012; Hopkins, 2000).

Estes eventos catalisaram o desenvolvimento de regulamentações específicas – a Diretiva Seveso na Europa (1982, revisada em 1996 e 2012), o Process Safety Management standard nos Estados Unidos (OSHA 29 CFR 1910.119, 1992) – e da própria disciplina de Segurança de Processos como campo estruturado de conhecimento. No Brasil, a NT 10/2023 da ANP estabelece os requisitos regulatórios para a gestão de Fatores Humanos integrada à segurança operacional, com ênfase explícita na prevenção de acidentes associados a grandes emergências (ANP, 2023).

A distinção crítica: Segurança Pessoal versus Segurança de Processos. Indicadores de segurança pessoal – taxas de frequência de lesões, dias perdidos, LTI (*Lost Time Injury* – lesão com afastamento) e TRI (*Total Recordable Incident* – incidente registrável, ou TRIR para sua taxa) – medem a frequência de eventos que afetam trabalhadores individualmente, mas são indicadores que não possuem a capacidade de refletir o estado das barreiras que previnem acidentes catastróficos. Conforme documentaram Rosness et al. (2010) com base nos estudos do SINTEF, "acidentes ocupacionais menores e acidentes organizacionais maiores frequentemente surgem de padrões diferentes de problemas de segurança" (tradução nossa). Hopkins (2008, 2012) demonstrou empiricamente, a partir das investigações de Texas City e Macondo, que indicadores ocupacionais aparentemente satisfatórios podem coexistir com a erosão progressiva das defesas de processo – fenômeno conhecido como falácia do uso de indicadores ocupacionais (LTI, TRI/TRIR) como proxy da segurança de processos.

3.6.2 Pressupostos Críticos

A Segurança de Processos como disciplina apoia-se em pressupostos distintos que orientam sua abordagem metodológica:

- **Origem sistêmica dos MAH:** Os riscos de acidentes maiores (*Major Accident Hazards* – MAH) são propriedades inerentes dos sistemas de processo. Decorrem da natureza das substâncias manipuladas, das condições operacionais e das interações entre seus componentes sociotécnicos – não primariamente de comportamentos individuais. A pergunta central da disciplina, tanto na análise prospectiva de riscos quanto na aprendizagem com eventos, é "quais barreiras falharam, ou podem falhar, e por quê?", e não "quem cometeu o erro?" (Reason, 1997; CCPS, 2007).
- **Necessidade de defesa em profundidade:** A prevenção efetiva de acidentes maiores requer múltiplas camadas de proteção independentes, de diferentes naturezas (física, instrumental, processual, humana), de modo que a falha de uma não comprometa imediatamente as demais. A independência entre camadas é condição necessária para a validade do modelo de defesa em profundidade (IEC 61511, 2016).
- **Princípio da degradação incremental:** O acidente maior é o desfecho de uma sequência de degradações de barreiras que ocorrem ao longo do tempo, frequentemente de forma não percebida pela organização, por vezes sob a ação de causas organizacionais que operam como modos de falha comuns, a exemplo de fragilidades nos processos de integridade (manutenção, inspeção, testes), capazes de degradar simultaneamente mais de uma barreira. Cada barreira isoladamente parece funcional; é apenas sua falha simultânea que abre o caminho para a catástrofe. Este princípio, formalizado no Modelo do Queijo Suíço de Reason (1997) e aprofundado pelo conceito de Conjuntos Solidários de Barreiras, tem implicações profundas para o monitoramento contínuo.
- **Segurança como processo, não como estado:** A segurança de processos não é um estado a ser atingido, mas um processo contínuo que envolve a identificação de cenários acidentais, o levantamento das barreiras capazes de reduzir o risco a níveis aceitáveis, e o monitoramento, avaliação e manutenção dessas barreiras. A erosão das defesas é a con-

dição esperada em sistemas sob pressão produtiva; sua integridade precisa ser ativamente sustentada (Rasmussen, 1997; Hollnagel, 2004).

- **Gestão baseada em risco:** A quantidade e a robustez das barreiras requeridas para cada cenário são definidas com base no risco: busca-se evitar riscos intoleráveis e manter os riscos dos cenários em níveis tão baixos quanto razoavelmente praticáveis (ALARP – *As Low As Reasonably Practicable*). Esta orientação estrutura o modelo de Gestão de Segurança de Processo Baseada em Risco (RBPS – *Risk Based Process Safety*) do CCPS (2007), amplamente adotado pela indústria, e encontra paralelo no processo decisório informado pelo risco (*risk-informed decision-making*) da área nuclear. Segurança pode, então, ser entendida como a capacidade organizacional de sustentar a saúde das barreiras de proteção e manter os riscos dos cenários em níveis ALARP.

3.6.3 Conceitos Fundamentais

O gerenciamento sistemático dos perigos/condições perigosas de acidentes maiores estrutura-se, no padrão internacional consolidado pela ISO 17776:2016, em três etapas iterativas: (i) identificação dos perigos mediante técnicas estruturadas como HAZID e HAZOP; (ii) avaliação dos riscos, orientada por critérios de triagem (*screening criteria*, na terminologia da ISO 17776 e do guia IADC) e por critérios de tolerabilidade de riscos, que definem severidade, frequência de ocorrência e limites de aceitação; e (iii) identificação das medidas de redução de risco e correspondente definição dos requisitos funcionais das barreiras (passivas, ativas e humanas — ver subseção Barreiras de Segurança). A Figura 3.6.1 apresenta esta estrutura, adotada por organizações da indústria – incluindo drilling contractors, em alinhamento às diretrizes do IADC (2015) e às práticas recomendadas que se consolidaram como RAGAGEPs – como espinha dorsal do processo de elaboração do HSE Case da unidade (documento que demonstra, de forma integrada, como os riscos da instalação são identificados, avaliados e controlados; ver subseção HSE / Safety Case, adiante).





Figura 3.6.1: Processo de Gestão de Riscos conforme ISO 17776:2016. *Adaptado de ISO 17776:2016 e IADC (2015) – Health, Safety and Environment Case Guidelines for Mobile Offshore Drilling Units.*

Cada uma das etapas é instanciada por técnicas e ferramentas específicas, descritas nas subseções que seguem: HAZID e HAZOP para identificação estruturada de perigos; matriz de risco e critérios de tolerabilidade para avaliação; Bow-tie e LOPA para modelagem e quantificação de barreiras; HSE Case (Safety Case) para demonstração integrada da gestão de riscos da instalação.

Major Accident Hazards (MAH) e Cenários de Risco

O conceito de ***Major Accident Hazard*** (MAH) – perigo de acidente maior (evento principal) – refere-se a situações com potencial para acidentes com múltiplas fatalidades, danos ambientais de grande escala ou perdas catastróficas de ativos. Na indústria de óleo e gás offshore, os MAHs típicos incluem perda de controle de poço (blowout), explosão e incêndio na instalação, colisão de embarcações, afundamento da unidade, e liberações tóxicas. Sua identificação sistemática é o ponto de partida de qualquer sistema de gestão de segurança de processos baseada em risco (ISO 17776, 2016).

A identificação de MAHs estrutura-se em torno de cenários de risco – representações de como um perigo pode evoluir para um acidente, incluindo a cadeia de causas (ameaças), o evento central (top event) e as possíveis consequências. Esta estrutura é formalmente capturada na ferramenta **Bow-tie** (Figura 3.6.2), que representa graficamente as barreiras de prevenção (entre ameaças e evento central) e as barreiras de mitigação (entre evento central e consequências).

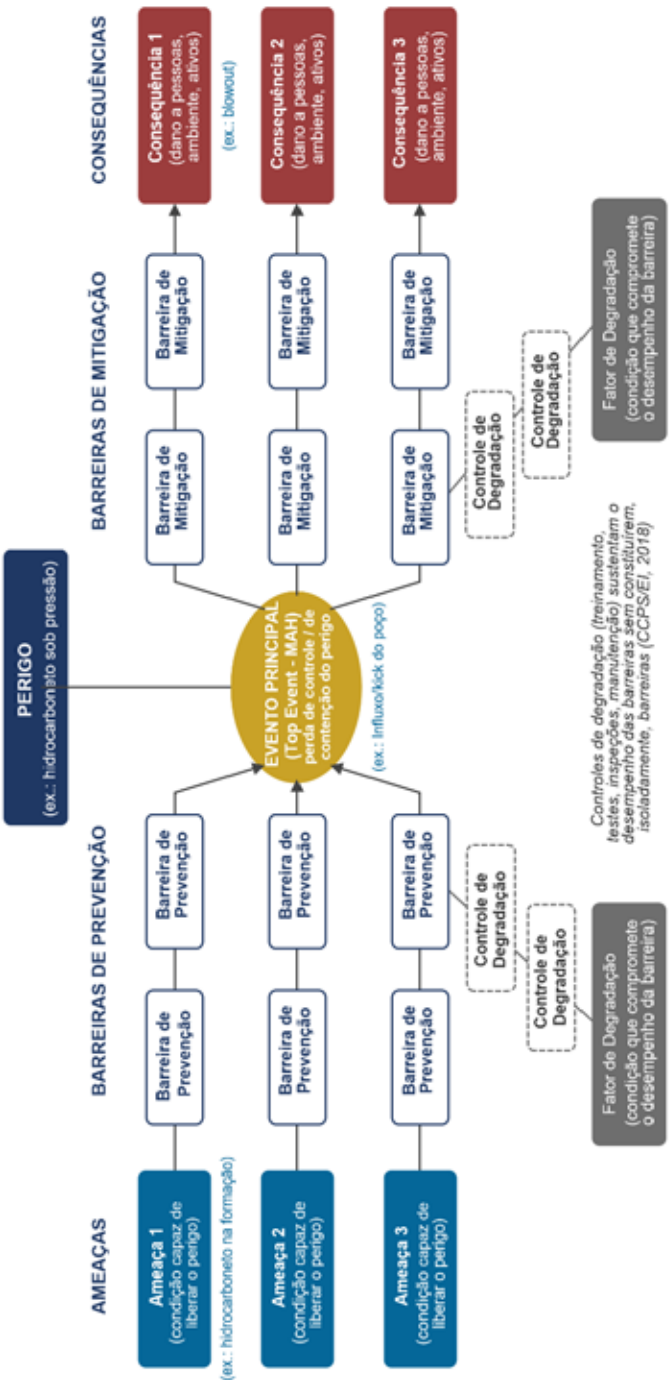


Figura 3.6.2: Estrutura do diagrama Bow-tie – ameaças, barreiras de prevenção, evento central (top event), barreiras de mitigação e consequências, com fatores e controles de degradação. Adaptado de CCPS/Energy Institute (2018) e IOGP 544 (2016).

A identificação e análise de MAHs fundamenta-se em estudos estruturados como: **HAZID** (*Hazard Identification*) para identificação qualitativa de perigos; **FERA** (*Fire and Explosion Risk Analysis*) e **EERA** (*Escape, Evacuation and Rescue Analysis*) para quantificação de riscos de incêndio e explosão e para análise de rotas de evacuação; estudos de colisão de embarcações e de queda de objetos (Ship Collision / Dropped Objects Studies), que analisam tipologias capazes de operar como cargas acidentais dimensionantes e de comprometer funções principais de segurança, conforme a abordagem da NORSOK Z-013; **QRA** (*Quantitative Risk Assessment*) para estimativa de riscos individuais e coletivos; e **FMEA/FMECA** (*Failure Mode and Effects Analysis/Criticality Analysis*) para análise de modos de falha de sistemas e componentes (Lees, 2012; CCPS, 2007). As duas técnicas centrais de identificação e análise estruturada de perigos, contudo, são o HAZID e o HAZOP, complementares entre si e distintas quanto à granularidade e aos requisitos de documentação: o HAZID permite o levantamento inicial de cenários perigosos desde as fases mais precoces do projeto, ao passo que o HAZOP requer a emissão dos P&IDs – tipicamente disponíveis a partir do projeto básico.

HAZID – *Hazard Identification*

O **HAZID** (*Hazard Identification*) é uma técnica qualitativa e estruturada de identificação de perigos, conduzida por equipe multidisciplinar em conjunto de reuniões facilitadas. Diferentemente do HAZOP, que examina desvios de parâmetros de processo em sistemas projetados (tipicamente sobre P&IDs), o HAZID opera em nível mais amplo de granularidade: divide a operação ou instalação em atividades ou áreas e, sistematicamente, revisa cada uma para identificar perigos, cenários acidentais associados, possíveis causas, consequências e salvaguardas existentes (ISO 17776, 2016).

Em instalações offshore – particularmente em **unidades móveis de perfuração** (MODUs - *Mobile Offshore Drilling Units*) – o HAZID, ancorado no Anexo F da ISO 17776:2016, constitui a técnica de referência para a identificação dos Major Accident Hazards (MAHs) e a elaboração do HSE Case da unidade, conforme as diretrizes do IADC para Mobile Offshore Drilling Units (IADC, 2015). Sua aplicabilidade ao longo de todo o ciclo de vida – projeto, operação e modificação – e a flexibilidade de granularidade tornam o HAZID particularmente adequado para

unidades onde HAZOPs de processo detalhados, típicos de plantas de produção fixas, têm menor aplicabilidade.

A metodologia HAZID emprega tipicamente uma classificação em duas etapas: primeiramente, classifica-se o risco inicial (frequência × severidade) desconsiderando as barreiras e salvaguardas existentes; em seguida, avalia-se o risco residual considerando todas as medidas de controle existentes. Cenários cujo risco residual permanece nos patamares superiores da matriz de risco da organização, tipicamente os de severidade catastrófica ou de classificação de risco alta, são promovidos a MAHs (eventos principais) da unidade, formalmente capturados em diagramas Bow-tie para análise de barreiras de prevenção e mitigação (Figura 3.6.2).

A integração entre HAZID, Bow-tie e HSE Case constitui o eixo metodológico recomendado pelo IOGP e amplamente adotado por *drilling contractors* (empresas de perfuração). No contexto regulatório brasileiro, esta integração responde diretamente aos requisitos do SGSO (Resolução ANP 43/2007) e da NT 10/2023 quanto à identificação sistemática de cenários de acidentes operacionais associados a grandes emergências e ao estabelecimento dos Elementos Críticos de Segurança Operacional (ECSO). Registre-se que a regulamentação brasileira não exige a abordagem de HSE Case (Safety Case) nem estabelece critério de tolerabilidade de riscos de acidentes maiores para as operações de E&P: a integração aqui descrita constitui prática da indústria, que suporta o atendimento aos requisitos regulatórios sem deles decorrer. A documentação resultante do HAZID alimenta diretamente a análise de barreiras (Bow-tie), a quantificação semiquantitativa (LOPA -*Layers of Protection Analysis*, quando aplicável) e a identificação das Tarefas Críticas de Segurança Operacional (TCSO) que serão objeto de Análise de Confiabilidade Humana (HRA), conectando-se à seção 3.4 deste compêndio.

HAZOP – *Hazard and Operability Study*

O **HAZOP** (*Hazard and Operability Study*) é uma técnica estruturada de análise de desvios em sistemas de processo, desenvolvida na ICI (Imperial Chemical Industries) no Reino Unido nos anos 1960 e hoje consolidada como padrão internacional para análise sistemática de perigos e operabilidade em instalações de processo (IEC 61882, 2016; CCPS, 2008). Em unidades móveis de perfuração

(MODUs), o HAZOP é tipicamente aplicado na fase de projeto da unidade (a partir do projeto básico/FEED – Front-End Engineering Design – ou na engenharia de detalhe), sendo o HAZID a técnica primária de gerenciamento de risco ao longo da operação. Em unidades de produção fixas e refinarias, a aplicação do HAZOP estende-se de forma mais sistemática ao longo de todo o ciclo de vida operacional.A diferença tem fundamento técnico: em MODUs, o sistema de processo representado nos P&IDs permanece relativamente estável após a construção, enquanto o perfil de risco dominante varia com o programa de cada poço, a locação e a campanha – cenários de natureza operacional que a granularidade flexível do HAZID captura de forma mais adequada do que a análise de desvios de parâmetros de processo. Em unidades de produção e refinarias, por sua vez, interligações de novos poços (tie-ins), mudanças na composição dos fluidos e modificações brownfield alteram continuamente o próprio processo, justificando a revalidação periódica do HAZOP ao longo da operação.

O HAZOP é conduzido por uma equipe multidisciplinar – tipicamente composta por engenheiro de processo, operador experiente, engenheiro de segurança, especialista em instrumentação e controle, e um facilitador treinado na técnica – que examina sistematicamente cada trecho do sistema ou nó de análise (node), utilizando palavras-guia (guide words) combinadas com parâmetros de processo (vazão, pressão, temperatura, nível, composição) para identificar desvios possíveis e suas consequências. As palavras-guia clássicas – Nenhum/Não, Mais, Menos, Bem como, Parte de, Reverso e Outro que – são aplicadas sistematicamente a cada parâmetro relevante do nó em análise. Cada desvio identificado é então analisado quanto às causas, consequências, salvaguardas existentes e recomendações de melhoria (Kletz, 2006; CCPS, 2008).

O resultado é uma documentação estruturada que constitui insumo fundamental para a construção dos bow-ties, para a identificação dos Elementos Críticos de Segurança Operacional (ECSO) exigidos pelo SGSO (Resolução ANP 43/2007) e para o HSE Case da instalação.

Human HAZOP – Integração de Fatores Humanos

A integração de perspectivas de Fatores Humanos ao HAZOP é uma evolução importante da técnica clássica. O *Human HAZOP* (ou *Human Factors HAZOP*) incorpora explicitamente a análise das tarefas críticas executadas por operadores como parte do sistema de processo: as palavras-guia são aplicadas não apenas a parâmetros físicos, mas também a ações humanas – identificando desvios como "ação não executada", "ação executada no momento errado", "ação executada na sequência errada" ou "ação executada no objeto errado". Os resultados alimentam diretamente a identificação de Tarefas Críticas de Segurança Operacional (TCSO) e a priorização de análises de confiabilidade humana (IEC 61882, 2016; Energy Institute, 2020).

HAZOP no Ciclo de Vida das Instalações

O HAZOP, como instrumento de gestão de risco, é aplicado em diferentes fases do ciclo de vida da instalação, com ênfase na fase de projeto:

- **Fase de projeto:** principal momento de aplicação, conduzida sobre P&IDs a partir do projeto básico/FEED ou em engenharia de detalhe, identificando perigos e estabelecendo salvaguardas antes da construção – momento de menor custo e maior facilidade para a implementação de modificações.
- **Pré-operação:** revisão (HAZOP de pré-startup ou PSSR – *Pre-Startup Safety Review*) realizada antes da entrada em operação, verificando se as recomendações do HAZOP de projeto foram implementadas.
- **Operação em curso:** HAZOP periódico ou de revalidação – tipicamente quinquenal ou após modificações significativas – que incorpora lições de acidentes e quase-acidentes e atualiza a documentação de risco da instalação. Para MODUs, esta revalidação pode ser substituída ou complementada por revisões periódicas do HAZID, conforme a natureza da unidade, pela justificativa técnica apresentada na abertura desta subseção.
- **Modificações (MOC - *Management of Change*):** HAZOP de modificação integrado ao processo de Gestão de Mudança, garantindo que alterações em equipamentos, sistemas ou operações não introduzam novos perigos

não analisados – prática alinhada aos requisitos de Gestão de Mudança do SGSO (Resolução ANP 43/2007) e da NT 10/2023, que estabelecem a obrigação de avaliar os riscos das mudanças sem prescrever técnica específica.

Nota técnica: As análises estruturadas de perigos – HAZID e HAZOP, conforme aplicáveis – constituem meios consolidados pela prática setorial para o atendimento ao gerenciamento de riscos operacionais exigido pelo SGSO (ANP, 2007) e pela NT 10/2023 (ANP, 2023) – regulamentos que estabelecem o requisito sem prescrever técnicas específicas. Boas práticas setoriais recomendam que organizações assegurem, além da realização inicial dos estudos: (i) revisão periódica (tipicamente quinquenal ou após modificações significativas); (ii) rastreabilidade do tratamento das recomendações geradas; e (iii) integração com o HSE Case da unidade e com o sistema de Gestão de Mudanças (MOC). Estes elementos são reconhecidos internacionalmente como indicadores de maturidade da gestão de riscos de processo (IEC 61882, 2016; IOGP 544, 2016).

Barreiras de Segurança

O conceito de **barreira de segurança** é estruturante para a Segurança de Processos. Hollnagel (2004, p. 22) define barreiras como "meios físicos ou funcionais que impedem uma ação ou ocorrência indesejada, ou que protegem contra as consequências de tais eventos". A contribuição seminal de Haddon (1980) estabeleceu que a prevenção de danos pode ser alcançada pela interposição de barreiras entre a fonte de energia perigosa e o alvo vulnerável – princípio que permanece central na engenharia de segurança de processos.

Sklet (2006) propõe distinções amplamente adotadas na indústria, diferenciando as barreiras quanto ao modo de atuação (passivas ou ativas) e quanto à natureza de seus sistemas (físicos/técnicos ou humano-operacionais). Em coerência com as definições consolidadas pelo CCPS e pelo Energy Institute (2018), as barreiras podem ser agrupadas em:

- **Passivas (físicas):** cumprem sua função de proteção pela simples presença, sem demanda de ativação – diques de contenção, proteção passiva contra incêndio (revestimentos e paredes corta-fogo) e sistemas

dedicados de drenagem aberta.

- **Ativas (técnicas):** sistemas físicos que requerem detecção de condições anormais, decisão e ação – tipicamente automáticas – para cumprir sua função: sistemas de detecção e supressão de incêndio, sistemas de intertravamento (SDI/ESD) e válvulas de alívio.
- **Humanas (operacionais):** barreiras cuja sequência de detecção, decisão e ação é cumprida por pessoas, tipicamente conforme especificado em procedimentos operacionais e de emergência – a exemplo da resposta do operador a um alarme crítico ou do fechamento do poço pelo sondador ante sinais de influxo (*kick*). Sua eficácia depende de clareza procedimental, treinamento e condições de execução; são as mais vulneráveis à deriva prática e à normalização de desvio.

Para serem contabilizados como barreiras, esses sistemas devem atender a três critérios de validade: efetividade – capacidade de, atuando com sucesso quando demandados, impedir a evolução da ameaça ao evento principal ou mitigar suas consequências; independência – em relação às demais barreiras do cenário e à própria causa iniciadora; e auditabilidade – possibilidade de verificação, efetivamente exercida, de seu desempenho (CCPS/EI, 2018). Requisitos de competência, treinamento e certificação – assim como as atividades de teste, inspeção e manutenção — são condições necessárias ao bom desempenho das barreiras, especialmente das humanas, mas não atendem, por si sós, ao conceito de barreira: atuam como controles de degradação (CCPS/EI, 2018). O conceito de guardião da barreira – o indivíduo responsável pela manutenção e verificação de um conjunto específico de barreiras – permanece central nos sistemas de gerenciamento dinâmico.

Uma barreira raramente é composta por um único elemento. Na prática, barreiras complexas são formadas por conjuntos de elementos interdependentes que precisam funcionar em conjunto para cumprir a função de proteção. Esta compreensão fundamenta o conceito de Conjunto Solidário de Barreiras.

Conjuntos Solidários de Barreiras (CSB)

O conceito de **Conjunto Solidário de Barreiras** (CSB) reconhece que barreiras de segurança são compostas por múltiplos elementos – hardware, sistemas ins-

trumentados, procedimentos e competências – que funcionam de forma integrada e solidária. A degradação ou perda de qualquer elemento compromete a funcionalidade do conjunto como um todo, independentemente do estado dos demais elementos.

Esta perspectiva contrasta com abordagens que tratam os elementos de barreira de forma independente. Quando se considera apenas a integridade técnica de um equipamento, mas não o treinamento do operador que deve ativá-lo ou a atualidade do procedimento que orienta sua operação, cria-se uma ilusão de proteção que pode ser fatal (Reason, 1997; Hollnagel, 2004).

O modelo de CSB tipicamente desdobra cada barreira em quatro categorias de elementos: (1) integridade de equipamentos e sistemas (hardware e instrumentação); (2) tarefas críticas de segurança operacional (ações humanas necessárias para que a barreira cumpra sua função); (3) verificações de elementos críticos (inspeções e testes regulares que confirmam a prontidão das barreiras); e (4) competência dos guardiões (capacitação e certificação das pessoas responsáveis pelas barreiras). A perda de qualquer um destes quatro elementos compromete a barreira como um todo.

Há convergência direta entre esta perspectiva e os elementos do diagrama Bow-tie na formulação do CCPS/EI (2018): os **fatores de degradação** (*degradation factors*) representam condições capazes de comprometer o desempenho de uma barreira, e os **controles de degradação** (*degradation controls*) – treinamento, testes, inspeções, manutenção – são as medidas que sustentam esse desempenho sem constituírem, isoladamente, barreiras. O CSB pode, assim, ser lido como a expressão integrada de uma barreira e de seus controles de degradação: enquanto o bow-tie os representa em ramificações específicas do diagrama, o CSB os agrupa como um conjunto solidário cuja saúde deve ser monitorada de forma unitária.

Bow-tie e Análise de Camadas de Proteção (LOPA - *Layers of Protection Analysis*)

O **Bow-tie** é a representação visual mais amplamente utilizada para comunicar MAH cenários e suas barreiras associadas (IOGP 544, 2016). O diagrama organi-

za-se em torno de um evento central (*top event*), que representa a perda de contenção do perigo. À esquerda do evento central estão as ameaças e as barreiras de prevenção (que visam impedir a ocorrência do top event); à direita estão as consequências potenciais e as barreiras de mitigação (que visam limitar as consequências após a ocorrência do top event).

Sua força como ferramenta de gestão – e não apenas de análise – reside na capacidade de conectar, de forma intuitiva, os cenários de risco às barreiras específicas que os controlam, e às pessoas e sistemas responsáveis por mantê-las. Organizações que implementam bow-ties de forma dinâmica – atualizando-os em tempo real conforme o estado das barreiras muda – transformam-nos de documentos estáticos de análise em instrumentos vivos de gestão de risco (IOGP 544, 2016).

A **Análise de Camadas de Proteção** (LOPA – Layers of Protection Analysis) é uma metodologia semiquantitativa que avalia se as camadas de proteção existentes reduzem o risco residual de um cenário de MAH a um nível aceitável (CCPS, 2001). Para cada camada de proteção independente (IPL – Independent Protection Layer), o LOPA estima uma Probabilidade de Falha na Demanda (PFD – Probability of Failure on Demand), que representa a probabilidade de que a barreira falhe em prevenir ou mitigar o evento quando acionada. O risco residual do cenário é calculado como o produto da frequência do evento iniciador pelo produto das PFDs de todas as IPLs.

A condição de independência entre as IPLs é fundamental para a validade do modelo. Barreiras que compartilham componentes, dependem do mesmo operador, ou falham por causas comuns não podem ser contabilizadas como camadas independentes – violação frequentemente identificada em investigações de acidentes. Para ser contabilizada como IPL, uma camada deve atender aos três requisitos que a caracterizam: **independência** – em relação às demais IPLs atribuídas ao cenário e à própria causa iniciadora –, **efetividade** – capacidade de, atuando com sucesso quando demandada, evitar a evolução da ameaça ao evento topo ou mitigar seus efeitos – e **auditabilidade** – a barreira deve ser auditável, e efetivamente auditada (CCPS, 2001; CCPS/EI, 2018).

HSE / Safety Case



O **HSE Case** (*Health, Safety and Environment Case* - documento de segurança da instalação; análogo a Safety Case) é um documento de segurança desenvolvido especificamente para cada instalação, que demonstra como os riscos associados às suas operações são identificados, avaliados e controlados a um nível ALARP (*As Low As Reasonably Practicable* - Tão Baixo Quanto Razoavelmente Praticável). Reúne evidências de engenharia, análises de risco, descrição de sistemas de gestão e planos de resposta a emergências, demonstrando como riscos maiores são controlados e como barreiras críticas são mantidas em conformidade com padrões de desempenho rigorosos (ISO 17776, 2016).

O conceito originou-se no Reino Unido após o desastre de Piper Alpha (1988), quando a investigação de Lord Cullen concluiu que o regime regulatório prescritivo então vigente era insuficiente para garantir a segurança de instalações complexas. A adoção de um regime baseado em objetivos – no qual a empresa demonstra que os riscos são ALARP – deslocou a responsabilidade da conformidade com regras para a demonstração de adequação das medidas de controle ao risco específico de cada instalação.

O HSE Case não é um documento estático. Para ser efetivo como instrumento de gestão, deve refletir continuamente o estado atual da instalação, sendo atualizado sempre que modificações, mudanças operacionais ou novos dados de risco alterem as premissas que fundamentaram sua elaboração (Hopkins, 2000; IOGP 544, 2016). Para *drilling contractors*, o HSE Case é tipicamente elaborado seguindo as diretrizes do IADC para *Mobile Offshore Drilling Units* (IADC, 2015), tendo o HAZID como técnica central de identificação de perigos.

3.6.4 Gerenciamento Dinâmico de Barreiras

O **Gerenciamento Dinâmico de Barreiras** (GDB) representa a evolução do modelo estático de análise de risco para um sistema de monitoramento contínuo da integridade das barreiras de segurança. Parte da constatação de que o risco real de uma instalação não é uma função constante determinada no momento da análise – é uma função dinâmica que varia continuamente em resposta à degradação de equipamentos, ao estado de manutenção, à disponibilidade de pessoal, à vigência de procedimentos e às condições operacionais (Rasmussen, 1997; Hollnagel, 2004).

A premissa fundamental é que toda barreira pode degradar-se ao longo do tempo, e que a degradação de uma única barreira, enquanto as demais permanecem íntegras, geralmente não produz efeitos imediatos visíveis – a instalação continua operando normalmente, o risco nominal permanece aparentemente controlado, mas a margem de segurança real está sendo progressivamente erodida. Este fenômeno, diretamente relacionado ao conceito de deriva prática (Snook, 2000) e à normalização do desvio (Vaughan, 1996), é um dos mais insidiosos mecanismos de incubação de acidentes maiores.

Elementos de Monitoramento das Barreiras

O monitoramento dinâmico das barreiras requer o acompanhamento sistemático de múltiplas dimensões do estado de cada elemento de barreira. Cada dimensão representa uma classe de sinais que indicam a prontidão da barreira para cumprir sua função quando demandada:

- **Integridade dos Ativos:** Integridade física dos ativos que compõem cada barreira – equipamentos degradados, sistemas inoperantes ou com certificação vencida indicam comprometimento direto da camada de proteção.
- **Estado de Manutenção, Testes e Inspeções:** Estado das ordens de serviço e dos planos de teste e inspeção associados a elementos críticos – manutenções preventivas em atraso, corretivas críticas abertas, testes periódicos não realizados (ex.: válvulas SDV, bombas de combate a incêndio) e inspeções de contenção primária pendentes são sinais de degradação progressiva.

- **Estado das Análises de Risco:** Vigência e conclusão das análises de risco que fundamentam a identificação e o projeto das barreiras – análises não realizadas ou em atraso significam que o estado das barreiras pode não refletir as condições operacionais atuais.
- **Competência e Treinamentos:** Atualidade e completude dos treinamentos dos guardiões das barreiras – treinamentos vencidos ou não realizados comprometem a componente humana de cada CSB.
- **Estado dos Procedimentos:** Atualidade dos procedimentos associados a cada barreira e confirmação de que os guardiões conhecem a versão vigente – procedimentos desatualizados são fonte direta de deriva prática.

A agregação destes indicadores por barreira e por cenário de MAH permite calcular, de forma dinâmica, a PFD atual de cada camada de proteção e, consequentemente, o risco residual real da instalação em cada momento – não o risco calculado na última análise estática, mas o risco efetivo dado o estado atual de todas as barreiras.

Contingenciamento de barreiras degradadas

Quando uma barreira se encontra degradada ou indisponível, medidas temporárias de contingenciamento (mitigações compensatórias) são adotadas para prover alguma redução de risco até o seu restabelecimento. Tais medidas exigem o mesmo rigor de gestão dispensado às barreiras permanentes: avaliação de risco da condição degradada, definição de prazos e responsáveis e – sobretudo – verificação da efetividade real do contingenciamento adotado. Contingenciamentos presumidos efetivos, mas não verificados na prática, constituem vulnerabilidade recorrente na gestão de barreiras .

Degradação de Barreiras e Risco Residual

O risco residual dinâmico de um cenário de MAH é tipicamente calculado pela combinação da frequência do evento iniciador com as probabilidades de falha na demanda das barreiras que o controlam. Quando uma barreira se degrada – por falha de equipamento, manutenção em atraso, procedimento desatualizado ou

guardião sem treinamento vigente – sua PFD aumenta, elevando o risco residual do cenário associado.

A fórmula de cálculo fundamenta-se na relação:

$$\mathbf{Risk_k = \Sigma(f_i \times \Pi\ PFD_{ij})}$$

onde $Risk_k$ é o risco residual do cenário k, f_i é a frequência do evento iniciador i, e PFD_{ij} é a probabilidade de falha na demanda da j-ésima IPL que protege contra a consequência do evento iniciador i (IEC 61511, 2016; CCPS, 2001). Note-se que esta formulação expressa a frequência esperada do cenário de perda de contenção – ou da consequência especificada na análise LOPA – e não, diretamente, o risco individual. A comparação com critérios de risco individual, como os limites de fatalidade por pessoa exposta por ano referidos a seguir, requer a quantificação completa dos riscos (QRA), incorporando a probabilidade de ignição, a probabilidade de presença de pessoas e a probabilidade de fatalidade dadas as intensidades dos efeitos físicos.

O **critério ALARP** (*As Low As Reasonably Practicable*) estabelece três zonas de tolerabilidade do risco: (i) **inaceitável** – risco acima do limite superior, que deve ser reduzido independentemente do custo; (ii) **tolerável se ALARP** – risco entre os limites superior e inferior, tolerado somente mediante a demonstração de que medidas adicionais de redução teriam custos grosseiramente desproporcionais ao benefício obtido em segurança; e (iii) **amplamente aceitável** – risco abaixo do limite inferior, que prescinde de ações adicionais (HSE UK, 2001). Os limites tipicamente adotados na indústria de óleo e gás offshore são 10^{-3} e 10^{-5} fatalidades por pessoa exposta por ano para os limites superior e inferior, respectivamente (HSE UK, 2001; ISO 17776, 2016).

A verificação periódica do risco residual frente ao critério ALARP não é uma exigência apenas do momento da análise inicial – é um processo contínuo que deve ser sensível às mudanças no estado das barreiras. Esta perspectiva dinâmica é um dos elementos centrais dos sistemas modernos de gestão de segurança de processos.

3.6.5 Indicadores de Desempenho em Segurança de Processos

O desenvolvimento de indicadores específicos para segurança de processos representa um avanço fundamental em relação à dependência histórica de indicadores de segurança pessoal como proxy do estado de saúde das barreiras de processo. A estrutura de indicadores proposta pelo API RP 754 (2021) teve sua aplicação expandida para o segmento upstream da indústria de óleo e gás – através do relatório 456 da IOGP (2018) - e foi adotada por organizações industriais globais. Os indicadores são agrupados em quatro níveis (ou tiers), como descrito a seguir e ilustrado na Figura 3.6.3:

- **Nível 1 – Eventos de perda de contenção primária (LOPC) de maior consequência:** eventos de perda de contenção primária que excedem os limiares superiores definidos pela prática recomendada – fatalidade ou lesão com afastamento, incêndios ou explosões com custo direto igual ou superior ao limiar estabelecido, liberações acima das quantidades-limite – os eventos de maior severidade e menor frequência esperada.
- **Nível 2 – Eventos de perda de contenção primária (LOPC) de menor consequência:** eventos que excedem limiares inferiores aos do Nível 1 – lesão registrável, incêndios ou explosões com custo direto igual ou superior ao limiar inferior, liberações acima de quantidades-limite reduzidas – relevantes para a identificação de tendências antes que ocorram consequências mais graves.
- **Nível 3 – Desafios aos sistemas de segurança:** demandas às camadas de proteção (ativações de sistemas instrumentados de segurança, válvulas de alívio, sistemas de detecção), excursões de limites operacionais seguros e resultados de testes ou inspeções fora dos critérios de aceitação – indicadores que revelam a frequência com que o sistema opera próximo a seus limites e o estado real das barreiras quando demandadas ou verificadas.
- **Nível 4 – Desempenho da disciplina operacional e do sistema de gestão:** indicadores que monitoram a realização, frente ao planejado, dos processos de trabalho críticos à segurança – cumprimento de planos de manutenção, testes e inspeções, atualização de procedimentos, realização de treinamentos e fechamento de ações – refletindo a saúde do sistema de gestão que sustenta as barreiras.



Figura 3.6.3: Pirâmide de Indicadores de Segurança de Processos (Níveis/Tiers 1–4). Adaptado de API RP 754 (2021) e IOGP 456 (2018)

Um sistema maduro de indicadores combina métricas de naturezas complementares: indicadores reativos de eventos de perda de contenção (Níveis 1 e 2); indicadores de demandas às camadas de proteção e de resultados de testes e inspeções (Nível 3) – que possuem caráter antecipatório em relação à perda de contenção; e indicadores de realização dos processos de trabalho críticos (Nível 4). A distinção entre realização e resultado é essencial: o cumprimento integral do plano de testes de válvulas de segurança, por exemplo, é informação necessária, mas insuficiente se parcela expressiva das válvulas reprova nos testes – é a leitura combinada das duas dimensões que fornece o quadro abrangente de monitoramento que a Segurança de Processos requer. Nenhum nível isolado é, portanto, "o mais importante": a capacidade preditiva emerge da leitura conjunta das quatro camadas.



Nota sobre indicadores de processo versus ocupacionais: Programas de segurança que usam exclusivamente métricas ocupacionais – LTI (Lost Time Injury), TRI/TRIR (Total Recordable Incident / Rate) e demais taxas de frequência de acidentes – como indicadores de gestão criam uma ilusão de controle que pode mascarar a erosão progressiva das barreiras de processo. A distinção entre os dois domínios de indicadores – e a implementação de sistemas específicos para o monitoramento da segurança de processos – é orientação consolidada de organizações como CCPS, API e IOGP.

3.6.6 Integração com o Ecossistema de Fatores Humanos

A Segurança de Processos não opera de forma isolada no Ecossistema de Fatores Humanos – é atravessada por praticamente todas as demais disciplinas e abordagens apresentadas nas Partes II e III deste compêndio. Esta integração é necessária porque as barreiras de processo não são apenas artefatos técnicos: são sistemas sociotécnicos cujo funcionamento depende criticamente das pessoas que as operam, mantêm e verificam (França, 2024; Hollnagel, 2004).

As principais zonas de contato com outras disciplinas do ecossistema incluem:

- **HRA e Novas Visões de Segurança:** A HRA **[ver Seção 3.4]** quantifica a probabilidade de erro humano em tarefas críticas que constituem elementos de CSBs, contribuindo para o cálculo realista da PFD de barreiras que possuem componente humano significativo, incluindo o uso das probabilidades de erro humano estimadas (por métodos como o Petro-HRA) para calibrar frequências de eventos iniciadores em análises QRA e LOPA, em substituição a valores genéricos de bancos de dados que nem sempre refletem os fatores contextuais vigentes (Monteiro, 2024). A inversão lógica também é relevante: o design inadequado de barreiras gera pressões sobre os operadores que aumentam a probabilidade de erro – perspectiva que as Novas Visões de Segurança **[ver Seções 1.2, 1.4 e 2.4]** e a HFE **[ver Seção 3.5]** tratam de forma complementar.
- **Engenharia de Fatores Humanos (HFE) [ver Seção 3.5]:** Os estudos de HFE requeridos pela NT 10/2023 – os sete estudos-chave do IOGP Report 454, entre eles a análise do projeto de salas de controle, o gerenciamento de alarmes e os estudos de criticidade de válvulas – buscam

assegurar que os projetos dos sistemas sociotécnicos favoreçam o bom desempenho humano, condição para que as barreiras com componentes humanos operem conforme especificado. Monteiro (2024) detalha os objetivos e as etapas de cada um desses estudos no contexto regulatório brasileiro, ilustrando, a partir de casos como Texas City (2005), o FPSO Cidade de São Mateus (2015) e Longford (1998), como deficiências de projeto de interfaces e de sistemas de alarme degradam diretamente o desempenho das barreiras com componente humano.

- **Aprendizagem com Eventos e Perspectivas Teóricas da Parte II:** A investigação sistêmica de acidentes de processo [ver Seção 3.2] – utilizando ferramentas como AcciMap (*Accident Mapping* – Rasmussen), FRAM (*Functional Resonance Analysis Method* – Hollnagel) e STAMP (*Systems-Theoretic Accident Model and Processes* – Leveson), detalhadas na Seção 3.2.5. Aplicadas a acidentes maiores, estas ferramentas revelam como as perspectivas de dependência de trajetória [ver Seção 2.5] (normalização do desvio, deriva prática) e de migração rasmusseniana às fronteiras [ver Seção 2.3] explicam a sequência de degradações de barreiras que precede a catástrofe. Acidentes como os de Texas City e Macondo são exemplares desta articulação (Hopkins, 2008, 2012).
- **Cultura Justa [ver Seção 3.3]:** A Cultura Justa é condição necessária para que os sinais de degradação de barreiras – observados e relatados por trabalhadores da linha de frente – cheguem ao conhecimento da organização sem distorção ou supressão. Sistemas de reporte que punem trabalhadores por revelarem vulnerabilidades produzem o silêncio organizacional que permite que a deriva em direção a falha continue sem intervenção.
- **Framework Integrador da Parte IV:** O Movimento III (Aprendizagem Operacional) do framework da Parte IV é especialmente relevante para a Segurança de Processos: a compreensão de como o trabalho realmente acontece – incluindo as adaptações cotidianas que os operadores realizam para manter sistemas funcionando – revela desvios entre WAI (*Work As Imagined* – Trabalho Como Imaginado) e WAD (*Work As Done* – Trabalho Como Realizado) **[conceitos detalhados na Seção 2.4]** que podem constituir sinais precoces de degradação de barreiras.

3.6.7 Implicações para a Indústria de Energia

A indústria de óleo e gás offshore apresenta uma combinação de características que a torna especialmente suscetível a acidentes de processo: volumes significativos de hidrocarbonetos a alta pressão e temperatura, espaço físico limitado que aumenta a complexidade interativa (Perrow, 1984), acoplamento estreito entre sistemas que permite propagação rápida de falhas, e operações remotas que dificultam intervenções de emergência. O potencial catastrófico é, portanto, elevado.

As contribuições mais relevantes da abordagem de Segurança de Processos para a indústria de energia incluem:

- **Gestão sistemática de MAHs:** Identificar todos os MAH associados à instalação, com base em estudos HAZID, HAZOP, FERA e outros, e estruturá-los em bow-ties com barreiras claramente definidas e atribuídas a responsáveis.
- **Monitoramento dinâmico das barreiras:** Ir além do monitoramento de falhas de equipamentos para monitorar continuamente a integridade do conjunto de elementos que compõem cada CSB – incluindo treinamento, procedimentos e verificações.
- **Indicadores específicos de processo:** Adotar e monitorar indicadores específicos de segurança de processos (níveis 1 a 4), não apenas indicadores de segurança pessoal.
- **HSE Case como instrumento vivo:** Manter o HSE Case como documento vivo, revisado a cada modificação significativa da instalação ou das condições operacionais, refletindo o estado atual do risco e das barreiras.
- **Cultura de reporte de degradações:** Criar e manter sistemas nos quais trabalhadores da linha de frente que identificam sinais de degradação de barreiras possam reportá-los sem medo de represálias – condição necessária para que o monitoramento dinâmico seja efetivo.
- **Aprendizagem interorganizacional:** Desenvolver mecanismos de aprendizagem que extraiam lições de acidentes de processo em toda a indústria, não apenas de eventos internos, resistindo à tendência de "distanciamento por diferenças" (Woods et al., 2010).

Tabela 3.6.1: Quadro-Resumo: Segurança de Processos

Dimensão	Segurança de Processos
Objeto central	Prevenção e mitigação de acidentes maiores (MAH) com potencial para múltiplas fatalidades, danos ambientais severos ou perdas catastróficas de ativos, decorrentes de falhas em processos industriais, incluindo a resposta e a restauração dos sistemas após liberações não planejadas ou não controladas de produtos ou energias perigosas, dimensão que aproxima a disciplina da noção de resiliência [ver Seção 2.4].
Distinção crítica	Difere fundamentalmente da segurança pessoal: indicadores de LTI não refletem o estado das barreiras de processo. Excelentes indicadores ocupacionais podem coexistir com erosão progressiva das defesas de processo.
Conceitos-chave	Cenários de acidentes maiores - MAH; Barreiras de segurança; Conjuntos Solidários de Barreiras (CSB); Bow-tie; LOPA; HSE Case; ALARP.
Princípio da degradação	Barreiras podem se degradar sob pressão produtiva sem produzir efeitos imediatos visíveis. O gerenciamento dinâmico monitoriza o estado real das barreiras – não o risco calculado na última análise estática.
Ferramentas analíticas	HAZID, HAZOP (incluindo Human HAZOP), FERA, EERA, estudos de colisão e de queda de objetos, QRA, FMEA/FMECA (identificação e quantificação); Bow-tie, LOPA (modelagem de barreiras); Pirâmide de Indicadores de Segurança de Processo – níveis (tiers) 1 a 4 ; HSE Case (demonstração integrada).
Integração com FH	HRA (componente humana das barreiras); Aprendizagem com eventos (investigação sistêmica de acidentes de processo); Cultura Justa (reporte de degradações); Perspectivas Teóricas da Parte II (mecanismos de incubação); Parte IV Movimentos I–III (governança, fluência e aprendizagem operacional).
Referências regulatórias	NT 10/2023 ANP; OSHA 29 CFR 1910.119; ISO 17776; IEC 61511; API RP 754; IOGP 544; Resolução ANP 43/2007 (SGSO); IADC HSE Case Guidelines for MODUs.

Dimensão	Segurança de Processos
Forças	Foco explícito nos riscos catastróficos; framework quantitativo de gestão de barreiras; integração com requisitos regulatórios; indicadores específicos de segurança de processo que superam as limitações do LTI.
Limitações / Cautelas	Risco de tratar barreiras apenas como artefatos técnicos, ignorando sua componente humana e organizacional; tendência à dependência excessiva de análises estáticas; necessidade de integração com cultura de aprendizagem para que o monitoramento dinâmico seja efetivo.



Referências da Seção 3.6

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. (2007). *Resolução ANP nº 43/2007 — Regulamento Técnico do Sistema de Gerenciamento da Segurança Operacional (SGSO)*. ANP.

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. (2023). *Nota Técnica nº 10/2023/SSO-CSO/SSO/ANP-RJ*. ANP.

American Petroleum Institute. (2021). *API RP 754: Process safety performance indicators for the refining and petrochemical industries* (3ª ed.). API.

Center for Chemical Process Safety. (2001). *Layer of protection analysis: Simplified process risk assessment*. AIChE.

Center for Chemical Process Safety. (2007). *Guidelines for risk based process safety*. Wiley.

Center for Chemical Process Safety. (2008). *Guidelines for hazard evaluation procedures* (3ª ed.). AIChE/Wiley.

Center for Chemical Process Safety, & Energy Institute. (2018). *Bow ties in risk management: A concept book for process safety*. AIChE/Wiley.

Energy Institute. (2020). *Guidance on human factors safety critical task analysis* (2ª ed.). Energy Institute.

França, J. E. M. (2024). *Human factors ecosystem – How human performance and process safety builds the energy transition and a low-carbon future for O&G industry* (SPE-220793-MS). Society of Petroleum Engineers. https://doi.org/10.2118/220793-MS

Haddon, W. (1980). The basic strategies for reducing damage from hazards of all kinds. *Hazard Prevention, 16*(5), 8–12.

Health and Safety Executive. (2001). *Reducing risks, protecting people: HSE's decision-making process*. HSE Books.

Hollnagel, E. (2004). *Barriers and accident prevention*. Ashgate.

Hopkins, A. (2000). *Lessons from Longford: The Esso gas plant explosion*. CCH Australia.

Hopkins, A. (2008). *Failure to learn: The BP Texas City refinery disaster*. CCH Australia.

Hopkins, A. (2012). *Disastrous decisions: The human and organisational causes of the Gulf of Mexico blowout*. CCH Australia.

International Association of Drilling Contractors. (2015). *Health, safety and environment case guidelines for mobile offshore drilling units* (Issue 3.6). IADC.

International Association of Oil & Gas Producers. (2016). *Standardization of barrier definitions* (IOGP Report 544). IOGP.

International Association of Oil & Gas Producers. (2018). *Process safety – Recommended practice on key performance indicators* (IOGP Report 456, 2ª ed.). IOGP.

International Association of Oil & Gas Producers. (2020). *Human factors engineering in projects* (IOGP Report 454, 2ª ed.). IOGP.

International Electrotechnical Commission. (2016a). *IEC 61511: Functional safety – Safety instrumented systems for the process industry sector*. IEC.

International Electrotechnical Commission. (2016b). *IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide*. IEC.

International Organization for Standardization. (2016). *ISO 17776: Petroleum and natural gas industries – Offshore production installations – Major accident hazard management during the design of new installations*. ISO.

Kletz, T. (2006). *HAZOP and HAZAN: Identifying and assessing process industry hazards* (4ª ed.). IChemE.

Mannan, S. (Ed.). (2012). *Lees' loss prevention in the process industries* (4ª ed.). Butterworth-Heinemann.

Monteiro, G. (2024). *Demystifying the human factors regulatory requirements in the Brazilian offshore oil and gas industry* [Apresentação de trabalho]. ROG.e 2024 – Rio Oil & Gas Energy Conference, Instituto Brasileiro de Petróleo e Gás (IBP).

NORSOK. (2010). *NORSOK Z-013: Risk and emergency preparedness assessment* (3ª ed.). Standards Norway.

Occupational Safety and Health Administration. (1992). *29 CFR 1910.119: Process safety management of highly hazardous chemicals*. OSHA.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærø, I. (2010). *Organisational accidents and resilient organisations: Six perspectives* (Report SINTEF A17034, Revisão 2). SINTEF Technology and Society.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*(5), 494–506.

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of U.S. Black Hawks over northern Iraq*. Princeton University Press.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.

Woods, D. D., Dekker, S. W. A., Cook, R., Johannesen, L., & Sarter, N. (2010).

Behind human error (2ª ed.). Ashgate.







Parte IV

Modelo integrador para aplicação setorial

Autor: Rafael Ceni de Almeida, José Carlos Bruno, Eder Henriqson, Josué E. Maia França

"A integração de Fatores Humanos requer um processo de mudança organizacional profundo, gradual e sustentado. Deve ser entendida como uma jornada – um processo contínuo de experimentação e descoberta, de desconstrução e construção do conhecimento, de forma iterativa e participativa – envolvendo lideranças e força de trabalho, própria e terceirizada, parceiros e todos os demais públicos de interesse." – Bruno (2020).

4.1 Da Teoria à Transformação Organizacional: Fatores Humanos como Jornada de Aprendizagem

As Partes I, II e III deste compêndio apresentaram os fundamentos históricos, as perspectivas teóricas fundamentais e as abordagens complementares que compõem o Ecossistema de Fatores Humanos. Conforme destacado pelo SINTEF (Rosness et al., 2010), estas contribuições teóricas são "parcialmente sobrepostas, parcialmente complementares e parcialmente contraditórias" – característica que não é limitação a ser superada, mas riqueza a ser explorada.

Mas como traduzir esta riqueza conceitual em transformação organizacional efetiva? A resposta não está em uma solução única, prescritiva e universal. Está em reconhecer que **implementar Fatores Humanos de forma efetiva não significa adotar um novo conjunto de ferramentas ou metodologias**, mas desenvolver uma **capacidade organizacional de aprendizagem contínua** – de compreender, questionar e aprimorar continuamente a relação entre pessoas, tecnologia e organização (Almeida et al., 2025; Bruno, 2020).

Esta transformação opera através de um mecanismo fundamental: **princípios orientam práticas; práticas transformadas reconfiguram cultura**. Os princípios de Fatores Humanos funcionam como políticas de governo das práticas – postulados que criam um referencial comum sobre como pensar segurança, erro e desempenho humano (Conklin, 2019; Henriqson, 2023). A partir desse referencial,

os princípios orientam a revisão das práticas organizacionais – tudo o que a organização efetivamente faz, de forma formal ou informal. Se cultura é, na formulação clássica de Deal e Kennedy (1982), *"o modo como fazemos as coisas por aqui"*, então mudança cultural genuína não é produto de "programas de cultura", mas **efeito** da revisão sistemática das práticas à luz de novos princípios (Henriqson, 2023).

Nesse sentido, é importante distinguir duas estratégias de implementação. Na abordagem **do local para o global**, a organização começa introduzindo ferramentas específicas sem antes estabelecer os princípios que orientam seu uso – abordagem que frequentemente resulta em ferramentas rejeitadas pelo sistema ou cooptadas pela Visão Tradicional. Na abordagem **do global para o local**, a organização começa pelos princípios, constrói referenciais comuns e, a partir deles, mobiliza a revisão das práticas e a introdução de ferramentas coerentes com o novo paradigma (Henriqson, 2023). O modelo integrador adota explicitamente essa segunda abordagem.

Esta Parte IV propõe um **modelo integrador** que reconhece a natureza processual e iterativa desta transformação. Não se trata de um modelo de maturidade com estágios sequenciais a serem "atingidos", mas de uma arquitetura de **movimentos** – direções de desenvolvimento que se sobrepõem, se reforçam mutuamente e evoluem em ciclos contínuos de aprendizagem. A escolha da palavra "movimentos" é deliberada. Diferente de "estágios" ou "fases", que sugerem progressão linear e pontos de chegada definidos, movimentos capturam a natureza dinâmica da transformação organizacional: **simultaneidade** (os movimentos não ocorrem em sequência rígida, mas organizações trabalham em múltiplos movimentos simultaneamente), **recursividade** (não há "conclusão" de um movimento – a organização retorna continuamente a cada um deles em ciclos iterativos), **interdependência** (cada movimento alimenta e é alimentado pelos demais), e **contextualidade** (a intensidade e foco em cada movimento variam conforme o contexto organizacional, setorial e regulatório).

4.1.1 Premissas Fundamentais

O modelo integrador está ancorado em sete premissas fundamentais que orientam sua aplicação:

1. **Pluralismo teórico é virtude, não fraqueza.** Diferentes perspectivas iluminam diferentes aspectos dos sistemas sociotécnicos. A riqueza analítica emerge da consideração de múltiplas lentes – não da busca por uma única "teoria correta".
2. **Transformação é jornada, não destino.** Não existe "estado final" de implementação de Fatores Humanos. Organizações evoluem continuamente, enfrentando novos desafios que demandam novas adaptações.
3. **Contexto determina aplicabilidade.** Não há prescrição universal. Cada organização deve traduzir os conceitos para sua realidade específica, considerando seu setor, maturidade, cultura e desafios particulares.
4. **Mudança estrutural precede mudança comportamental sustentável.** Intervenções focadas apenas em comportamentos individuais, sem alteração das condições organizacionais que os produzem, tendem a gerar conformidade temporária, não transformação genuína.
5. **Aprendizagem demanda segurança psicológica.** Organizações só aprendem quando pessoas se sentem seguras para reportar problemas, admitir erros e questionar práticas estabelecidas sem medo de retaliação (Edmondson, 2019).
6. **Liderança é condição necessária, mas não suficiente.** Sem comprometimento genuíno da alta liderança, iniciativas de Fatores Humanos permanecem periféricas. Contudo, liderança comprometida sem estruturas organizacionais de suporte também não produz transformação sustentável.
7. **Cultura Justa é pré-requisito para aprendizagem organizacional.** Organizações que tratam todos os desvios como transgressões individuais a serem punidas inibem o reporte de problemas e impedem a aprendizagem sistêmica. Uma Cultura Justa distingue entre erro honesto (decorrente de condições sistêmicas), comportamento de risco e negligência deliberada – aplicando respostas proporcionais e transparentes (Dekker, 2012). Políticas de consequência tradicionais, ao não fazer esta distinção, frequentemente punem adaptações necessárias e silenciam a linha de frente.

4.1.2 O Ponto de Partida: A Mudança do Modelo Mental

Antes de apresentar os movimentos, é fundamental reconhecer o obstáculo central que toda jornada de Fatores Humanos deve enfrentar: **a mudança de modelo mental**. Como muitos dos paradigmas propostos por Fatores Humanos desafiam conceitos há muito enraizados – quase como verdades absolutas –, não há como incorporá-los aos sistemas de gestão da noite para o dia (Bruno, 2020).

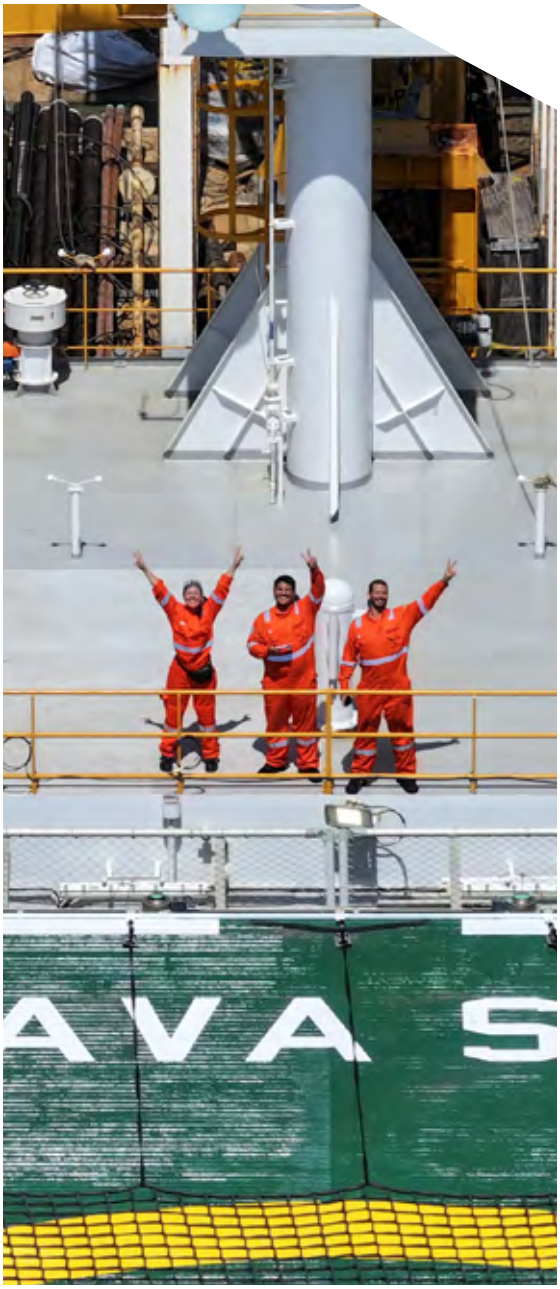
A Visão Tradicional (*Old View*), apresentada na Parte I, permanece profundamente enraizada na cultura organizacional da indústria: a crença de que "segurança é escolha do indivíduo", que acidentes resultam primariamente de "falhas humanas", e que o caminho para a segurança passa pelo controle comportamental. Esta visão é intuitiva, culturalmente reforçada e juridicamente conveniente – o que explica sua persistência. Pesquisa conduzida por Bruno (2020) revelou que, apesar das lições catastróficas de eventos como Macondo, a indústria continua demonstrando dependência esmagadora de paradigmas da Visão Tradicional que veem o erro humano como causa primária de falhas.

Existe uma **relação íntima entre o modo como uma organização explica seus acidentes e o modo como ela os previne**. Organizações que explicam acidentes como "falhas humanas" constroem sistemas orientados ao controle do trabalhador. Organizações que compreendem os acidentes como emergências sistêmicas investem em compreender e melhorar as condições de trabalho (Henriqson, 2023). Mudar o modelo explanatório é, portanto, pré-requisito para mudar o modelo preventivo.

A formalização de novos princípios é frequentemente motivada pelo reconhecimento de que sua **antítese** prevalece na organização. Se uma empresa sente necessidade de declarar que "errar é humano e sistêmico", é porque, na prática, erros continuam sendo tratados como falhas individuais. Se precisa lançar um "programa de segurança psicológica", é porque reconhece que seu ambiente ainda não oferece segurança psicológica de fato. Esse reconhecimento honesto do estado atual é o verdadeiro ponto de partida (Henriqson, 2023).

A transição para a Nova Visão (*New View*) não é simplesmente uma questão de "treinamento" ou "conscientização". Requer um processo genuíno de reflexão crí-

tica, experimentação e construção coletiva de novos significados. É por isso que o **engajamento das lideranças** constitui o movimento fundacional da jornada – não como etapa a ser "completada", mas como processo contínuo de transformação que deve permear todos os demais movimentos.



4.2 Os Cinco Movimentos da Jornada de Fatores Humanos

O modelo integrador organiza a jornada em cinco movimentos interdependentes, inspirados na experiência da Jornada de Fatores Humanos da Petrobras e da Constellation Serviços de Petróleo (Almeida et al., 2025; Bruno, 2020). Cada movimento representa uma direção de desenvolvimento organizacional, não uma etapa a ser "concluída". A Tabela 4.2.1 ilustra a natureza dinâmica e interconectada destes movimentos, e a Figura 4.2.1 apresenta sua representação visual.

Tabela 4.2.1: Visão geral dos cinco movimentos da Jornada de Fatores Humanos

Movimento	Foco Central	Pergunta Orientadora
I. Engajamento das Lideranças & Governança	Mudança de modelo mental, comprometimento estratégico e estrutura de governança.	Como vemos o papel das pessoas em nosso sistema? Quem delibera sobre a jornada?
II. Fluência nos Fundamentos	Disseminação do conhecimento e construção de linguagem comum	Nossa organização fala a mesma linguagem sobre FH?
III. Aprendizagem Operacional	Conexão com o trabalho real e valorização da expertise operacional	Conhecemos como o trabalho realmente acontece?
IV. Alinhamento e Integração	Revisão de sistemas, processos e estruturas organizacionais	Nossos sistemas reforçam ou contradizem nossos princípios?
V. Resiliência e Capacidade Adaptativa	Desenvolvimento de capacidades de antecipar, responder e aprender	Estamos preparados para o que ainda não sabemos?



Figura 4.2.1: Os cinco movimentos da Jornada de Fatores Humanos. *Movimentos simultâneos e interdependentes – não etapas sequenciais. Modelo aplicado nas Jornadas de Fatores Humanos da Petrobras e da Constellation Serviços de Petróleo. Fonte: elaboração própria a partir de Almeida, Bruno e Capaverde (2025) e Bruno (2020). Citação inferior: Henriqson (2023).*

4.2.1 Movimento I – Engajamento das Lideranças & Governança

Essência: Este movimento representa a oportunidade – e a necessidade – das lideranças de topo tomarem ciência dos conceitos e princípios de Fatores Humanos e iniciarem o processo de mudança do modelo de pensamento vigente. É o movimento fundacional porque, sem o comprometimento genuíno da alta liderança, as iniciativas de Fatores Humanos tendem a permanecer periféricas, incapazes de influenciar as decisões que realmente moldam as condições de trabalho (Almeida et al., 2025). Além do engajamento individual, este movimento estabelece a **estrutura de governança** que sustentará a jornada ao longo do tempo.

Por que é crítico: São as lideranças, especialmente no topo, que assumem a responsabilidade ética de criar as condições para que a organização evolua. Isso significa identificar e eliminar elementos que podem fomentar um ambiente de medo e silêncio organizacional – a linguagem utilizada, as interações com as pessoas, os sistemas de reporte, as auditorias, as investigações e os processos de aprendizado. Ademais, decisões estratégicas sobre revisão de práticas, alo-

cação de recursos e mudanças estruturais requerem legitimidade organizacional que apenas a alta liderança pode conferir. **Cultura Justa como pré-requisito:** a aprovação de revisões de políticas de consequência e de sistemas disciplinares – discutidas em detalhe no Movimento IV – exige da governança fluência prévia em Cultura Justa (Seção 3.3), pois é nesse fórum que se delibera sobre como a organização responderá institucionalmente a erros honestos, comportamentos de risco e negligência deliberada.

Manifestações práticas: Laboratórios de Fatores Humanos para lideranças (espaços de construção conjunta de conhecimento, não palestras informativas); definição participativa de Princípios de Fatores Humanos organizacionais; constituição de estrutura de governança para a jornada (Comitê de FH ou atribuição a comitês existentes); alocação de recursos; revisão crítica da linguagem organizacional sobre segurança e erro.

Sinal de progresso: Lideranças questionam espontaneamente explicações simplistas baseadas em "erro humano"; decisões organizacionais começam a refletir compreensão sistêmica; linguagem de culpabilização individual diminui em comunicações oficiais.

Governança da Jornada e Avaliação Crítica de Práticas

A sustentação da jornada de Fatores Humanos ao longo do tempo recomenda estrutura de governança específica – como um **Comitê de Fatores Humanos** – ou a atribuição de responsabilidades a comitês estratégicos já constituídos pela organização (por exemplo, Comitê de SMS ou Comitê Executivo). Independentemente do arranjo adotado, as seguintes atribuições devem ser formalmente designadas:

- **Deliberar** sobre propostas de revisão, simplificação ou descontinuação de práticas existentes;
- **Acompanhar** a implementação das ações acordadas a partir das reflexões organizacionais (ver Tabela 1.4.2 na Parte I);
- **Priorizar** investimentos e alocação de recursos para a jornada;
- **Monitorar** indicadores de progresso nos cinco movimentos;

- **Aprovar** revisões de políticas de consequência e sistemas disciplinares propostas no Movimento IV;
- **Assegurar** alinhamento entre iniciativas de Fatores Humanos e diretrizes estratégicas da organização.

Esta estrutura de governança constitui o fórum adequado para tratar uma das questões mais sensíveis da jornada: a **avaliação crítica de práticas existentes**. Conforme Rae, Weber e Dekker (2018) demonstraram, organizações frequentemente acumulam *safety clutter* – trabalho rotulado como "segurança" que não contribui efetivamente para a segurança operacional, mas consome recursos e atenção que poderiam ser direcionados para riscos genuínos. Procedimentos acumulados ao longo de anos podem ter perdido seu propósito original; intervenções bem-intencionadas podem estar produzindo efeitos paradoxais.

A decisão de descontinuar, simplificar ou ressignificar tais práticas é estratégica e frequentemente enfrenta resistências – razão pela qual deve ser conduzida pela alta liderança, não delegada a níveis operacionais. Avaliar criticamente práticas estabelecidas não é necessariamente eliminá-las, mas perguntar: *esta prática ainda serve ao propósito para o qual foi criada?*

Tabela 4.2.2: Critérios orientadores para avaliação de práticas pelo Comitê/estrutura de governança

Perguntas Orientadoras	Possíveis Ações
Esta prática ainda serve ao propósito para o qual foi criada?	Manter, ressignificar ou descontinuar
Esta prática gera conformidade burocrática sem valor operacional?	Simplificar ou descontinuar
Esta prática consome recursos desproporcionais ao benefício gerado?	Redesenhar ou descontinuar
Esta prática contradiz princípios de Fatores Humanos declarados?	Revisar urgentemente ou descontinuar
Esta prática foi adicionada como reação a evento específico e perdeu contexto?	Avaliar relevância atual

Interdependências com os demais movimentos: A estrutura de governança estabelecida neste movimento sustenta e é alimentada por todos os demais. Do **Movimento II** (Fluência nos Fundamentos), a governança recebe subsídios conceituais que qualificam suas deliberações – lideranças que compreendem princípios de Fatores Humanos tomam decisões mais alinhadas à nova visão. Do **Movimento III** (Aprendizagem Operacional), recebe os achados do trabalho real que demandam deliberação sobre ressignificação de práticas. Do **Movimento IV** (Alinhamento e Integração), recebe propostas de revisão de políticas, sistemas e processos que requerem aprovação estratégica – particularmente políticas de consequência e modelos de accountability. Do **Movimento V** (Resiliência e Capacidade Adaptativa), recebe sinais sobre a capacidade da organização de antecipar e responder a desafios emergentes, informando decisões sobre investimentos em capacidades adaptativas. A governança não apenas delibera: ela modela comportamentos e sinaliza prioridades organizacionais.

4.2.2 Movimento II – Fluência nos Fundamentos

Essência: Envolve a disseminação dos princípios e fundamentos em Fatores Humanos por toda a organização, até o nível operacional, construindo linguagem comum e repertório conceitual compartilhado. Vai além da simples "conscientização" – busca criar fluência genuína que permita às pessoas reconhecer, discutir e aplicar conceitos de FH em seu contexto de trabalho.



Manifestações práticas: Programas de capacitação para toda linha gerencial e lideranças formais e informais, próprias e contratadas; capacitação avançada para especialistas que atuarão como coaches e/ou facilitadores internos; inclusão de Fatores Humanos em cursos de formação; treinamentos específicos em investigação de acidentes, times de aprendizagem, gestão de riscos com foco em FH, dentre outros.

Expansão micro → macro: A fluência não deve se limitar a conceitos de nível micro (erro, decisão individual). Deve incluir compreensão de dinâmicas organizacionais, pressões de produção, estruturas de poder e dependência de trajetória (*path dependency*) – expandindo o olhar para os fatores macro que moldam comportamentos.

Sinal de progresso: Conceitos de FH aparecem naturalmente em discussões operacionais; pessoas utilizam termos como "racionalidade local", "WAI vs WAD" e "visão sistêmica" com propriedade; explicações simplistas são questionadas em todos os níveis.

Interdependência com outros movimentos: A construção de linguagem comum e repertório conceitual compartilhado serve como infraestrutura para todos os demais movimentos. No **Movimento I**, a fluência nos fundamentos qualifica as deliberações da governança – lideranças que compreendem conceitos como *safety clutter*, racionalidade local e deriva prática tomam decisões mais coerentes com a nova visão. No **Movimento III**, a fluência permite que equipes de Aprendizagem Operacional reconheçam padrões sistêmicos no trabalho cotidiano, superando explicações simplistas baseadas em "erro humano". No **Movimento IV**, o vocabulário compartilhado facilita o diagnóstico de desalinhamentos entre sistemas de gestão e princípios declarados. No **Movimento V**, conceitos como capacidade adaptativa, extensibilidade graciosa e margem de manobra tornam-se ferramentas práticas de análise. A fluência não é pré-requisito sequencial, mas recurso que se aprofunda recursivamente à medida que a organização avança em todos os movimentos.

4.2.3 Movimento III – Aprendizagem Operacional

Essência: Este é talvez o movimento mais crítico da jornada, porque é aqui que ocorre a conexão entre a nova visão de segurança e as práticas operacionais cotidianas. Envolve desenvolver capacidade organizacional de compreender como o trabalho *realmente* acontece – não como imaginamos ou prescrevemos que aconteça (Hollnagel, 2014).

Por que é crítico: É neste movimento que a liderança, sobretudo aquela mais próxima do ambiente operacional, tem a oportunidade de perceber o que signi-



fica, na prática, a diferença entre o trabalho como realizado (WAD) e o trabalho como imaginado (WAI), e por que ajustes e adaptações são elementos necessários e fundamentais para a continuidade operacional de forma segura e eficiente.

Atenção importante: É possível que no início este movimento passe a impressão de que "as coisas estão piorando", já que é natural que aumente o volume de notificações de segurança e as más notícias fiquem mais evidentes no processo de tomada de consciência da real situação do trabalho. Isto é sinal de progresso, não de retrocesso – **e só se sustenta se a organização tiver consolidado os fundamentos de Cultura Justa (Seção 3.3)**: sem distinção clara entre erro honesto, comportamento de risco e negligência deliberada, o aumento de reportes será interpretado como "deterioração da disciplina" e produzirá retração defensiva ao invés de aprendizado.

Manifestações práticas: Learning and Improvement Teams (LIT) que integram linha de frente e gestão; programas de Aprendizagem Operacional que estudam trabalho cotidiano (não apenas incidentes); observações no campo com foco em compreensão (não fiscalização); canais de escuta ativa para expertise operacional; portais de aprendizado e melhoria (Almeida et al., 2025).

Sinal de progresso: Volume de reportes aumenta (indicando maior confiança psicológica); lideranças demonstram curiosidade genuína sobre o trabalho real; adaptações operacionais são discutidas abertamente; a lacuna WAI-WAD torna-se tema legítimo de conversação organizacional.

Interdependência com outros movimentos: A Aprendizagem Operacional constitui o ponto de conexão entre a nova visão e a realidade do trabalho, gerando insumos críticos para todos os demais movimentos. Para o **Movimento I**, fornece evidências do trabalho real que fundamentam deliberações da governança

– incluindo achados sobre práticas que perderam propósito ou geram conformidade sem valor, demandando decisão sobre ressignificação ou descontinuação. Quando tais achados emergem, devem ser encaminhados à estrutura de governança para deliberação; a decisão de alterar práticas estabelecidas requer legitimidade organizacional que apenas a alta liderança pode conferir. Para o **Movimento II**, revela lacunas de compreensão conceitual que orientam programas de capacitação – onde a linguagem de Fatores Humanos ainda não penetrou, onde conceitos são mal compreendidos ou aplicados de forma superficial. Para o **Movimento IV**, identifica desalinhamentos concretos entre WAI e WAD, sinalizando sistemas, processos e políticas que requerem revisão. Para o **Movimento V**, mapeia-se as adaptações cotidianas que criam segurança, revelando capacidades adaptativas existentes que podem ser fortalecidas e vulnerabilidades que demandam atenção.

4.2.4 Movimento IV – Alinhamento e Integração

Essência: Neste movimento, a organização identifica desalinhamentos entre seus sistemas, processos e estruturas e a nova visão proposta por Fatores Humanos, promovendo realinhamentos estruturais sustentáveis – não apenas iniciativas pontuais.

Áreas de revisão prioritárias: investigação e análise de acidentes; auditorias e inspeções; indicadores e métricas de segurança; políticas de consequência e sistemas disciplinares; processos de recrutamento, seleção e capacitação; políticas e diretrizes; modelos de contratação e gestão de terceiros.

Por que é crítico: sem mudanças estruturais, a transformação permanece superficial. A **cultura justa** é o ponto mais sensível deste movimento – a revisão dos sistemas de consequência e processos disciplinares (Seção 3.3) é tipicamente onde mais se manifesta a tensão entre o discurso institucional e a prática organizacional. Reformar esses sistemas sem a fluência adequada (Movimento II) e sem o respaldo deliberativo da governança (Movimento I) tende a produzir reformas apenas nominais – exatamente o risco caracterizado em 3.3.8 como captura punitiva do sistema de *accountability*.

Sinal de progresso: investigações de incidentes geram recomendações sistêmicas, não apenas identificação de "culpados"; métricas de segurança incluem indicadores de aprendizagem, e não somente taxas de incidentes; políticas de consequência são revisadas, comunicadas com transparência e aplicadas de forma consistente entre níveis hierárquicos; processos de contratação de terceiros incluem critérios de alinhamento a princípios de Fatores Humanos.

Interdependência com outros movimentos: o realinhamento de sistemas, processos e estruturas organizacionais requer legitimidade e insumos dos demais movimentos. Do **Movimento I**, recebe autorização e priorização para mudanças estruturais – propostas de revisão de políticas de consequência, sistemas disciplinares, métricas e modelos de contratação devem ser submetidas à governança para deliberação. Do **Movimento II**, recebe o vocabulário e os critérios conceituais que permitem diagnosticar desalinhamentos – sem fluência nos fundamentos, é difícil reconhecer quando um sistema de gestão contradiz princípios declarados. Do **Movimento III**, recebe os achados do trabalho real que evidenciam onde os desalinhamentos se manifestam na prática – a lacuna WAI–WAD torna-se visível através da Aprendizagem Operacional. Para o **Movimento V**, cria as condições estruturais que sustentam ou limitam a capacidade adaptativa – sistemas de gestão podem tanto ampliar quanto restringir a margem de manobra organizacional.

Revisão de Políticas de Consequência e Cultura Justa

Um dos desalinhamentos mais críticos – e frequentemente mais difíceis de enfrentar – envolve as **políticas de consequência**. Grande parte das empresas do setor opera com modelos disciplinares que não distinguem entre tipos qualitativamente diferentes de comportamento: o erro honesto cometido por profissional competente em contexto desafiador (caso típico do teste de substituição de Johnston; cf. 3.3.3) recebe tratamento similar ao de violação deliberada. A abordagem é tanto injusta quanto contraproducente: silencia a força de trabalho, incentiva a ocultação de problemas e bloqueia a aprendizagem organizacional (cf. 3.3.6).

A transição para uma **cultura justa restaurativa** (Dekker, 2017; Dekker, Rafferty & Oates, 2022) requer:

- distinção clara entre erro (predominantemente sistêmico), comportamento de risco (limites negociáveis) e violação deliberada (negligência consciente), com critérios de avaliação conhecidos antecipadamente pela organização;
- deslocamento da pergunta-guia de "quem fez algo errado?" para "o que foi responsável pelo que deu errado e quais necessidades precisam ser atendidas?" (cf. Figura 3.3.1);
- preferência por *accountability* prospectiva – orientada a salvaguardas e melhorias – em detrimento da accountability retrospectiva orientada à culpa e à punição (cf. 3.3.2);
- reconhecimento de que punir o erro honesto é incompatível com os princípios de Fatores Humanos e com a construção de segurança psicológica.

A revisão de políticas de consequência é frequentemente o **teste mais difícil** do comprometimento real da liderança com a transformação. Organizações que declaram adotar Fatores Humanos mas mantêm sistemas punitivos tradicionais enviam mensagens contraditórias que minam a credibilidade da jornada – e essa contradição é lida, antes de tudo, pelos próprios profissionais de linha de frente.

4.2.5 Movimento V – Resiliência e Capacidade Adaptativa

Essência: Neste movimento, a organização desenvolve capacidades que permitem não apenas aprender com o passado, mas antecipar desafios futuros e criar segurança proativamente. A organização "aprende a aprender", promovendo reforço preventivo às salvaguardas que a tornarão mais forte e segura frente às incertezas e riscos residuais das operações (Hollnagel, 2018).

Por que é crítico: Sistemas cada vez mais resilientes podem ser projetados para ajudar a organização na construção de capacidades positivas adicionais para melhor antecipar, reagir, mitigar e se recuperar das falhas, incluindo até a capacidade de "falhar com segurança". Este movimento representa a maturação da jornada, **operando recursivamente sobre os demais** – não como ponto de chegada, mas como propriedade emergente que se consolida à medida que os outros movimentos se aprofundam.

Manifestações práticas: Integração das quatro capacidades da Engenharia de Resiliência (responder, monitorar, antecipar, aprender); mecanismos de detecção de deriva e normalização de desvio; investimento contínuo em redundância e capacidade adaptativa; desenvolvimento de indicadores antecipatórios (*leading indicators*) além de reativos; simulações e exercícios que testam capacidade de resposta a cenários não previstos.

Sinal de progresso: A organização demonstra capacidade de antecipar riscos emergentes; existe monitoramento ativo de sinais fracos e mudanças no ambiente operacional; a capacidade de resposta a situações não previstas é testada regularmente; a aprendizagem ocorre tanto com falhas quanto com sucessos; princípios de Fatores Humanos são incorporados progressiva e consistentemente na gestão de tecnologias, processos e pessoas.

Interdependência com outros movimentos: O desenvolvimento de capacidades adaptativas emerge da integração recursiva dos movimentos anteriores. Do **Movimento I**, depende de comprometimento sustentado da governança com investimentos em capacidades de antecipar, monitorar, responder e aprender – capacidades que frequentemente não geram retorno imediato visível. Do **Movimento II**, requer fluência avançada em conceitos de Engenharia de Resiliência que permitam à organização monitorar sua própria capacidade adaptativa. Do **Movimento III**, recebe o fluxo contínuo de aprendizados do trabalho cotidiano que alimenta a capacidade de antecipar e responder – organizações resilientes aprendem tanto com o que dá certo quanto com o que falha. Do **Movimento IV**, depende de sistemas e estruturas alinhados que não constranjam excessivamente a variabilidade adaptativa necessária para lidar com situações imprevistas. A resiliência organizacional emerge como propriedade sistêmica quando todos os movimentos operam de forma integrada e recursiva.

4.2.6 Síntese: A Natureza Interdependente dos Movimentos

A Tabela 4.2.3 sintetiza as interdependências entre os cinco movimentos, evidenciando que a jornada de Fatores Humanos não é linear, mas constitui um sistema dinâmico onde cada movimento alimenta e é alimentado pelos demais.

Tabela 4.2.3: Matriz de interdependências entre os movimentos

Movimento	Fornece para os demais	Recebe dos demais
I. Governança	Legitimidade, priorização, recursos, modelagem de comportamentos	Insumos para deliberação, propostas de mudança, evidências do trabalho real
II. Fluência	Linguagem comum, critérios conceituais, capacidade de diagnóstico	Demandas de capacitação, lacunas identificadas na prática
III. Aprendizagem	Achados do trabalho real, evidências de desalinhamento, adaptações cotidianas	Conceitos para interpretação, legitimidade para investigar, estruturas de escuta
IV. Alinhamento	Condições estruturais, coerência sistêmica, sustentabilidade	Autorização para mudanças, critérios de diagnóstico, evidências de lacunas
V. Resiliência	Capacidade de antecipar e responder, integração sistêmica	Investimentos, conceitos, aprendizados, estruturas habilitadoras

Esta arquitetura de movimentos interdependentes reforça que a transformação em Fatores Humanos não ocorre através de projetos sequenciais com início, meio e fim, mas através de ciclos contínuos de engajamento, aprendizagem e adaptação. Organizações maduras trabalham simultaneamente em todos os movimentos, com intensidade variável conforme seu contexto e desafios particulares.

Um princípio transversal: a expansão do olhar do micro para o macro. Embora a ênfase em indivíduos, decisões e adaptações nas linhas de frente seja necessária, por si só não é suficiente. Uma jornada transformadora também examina estruturas de poder, projetos e recursos existentes, pressões de produção e dinâmicas organizacionais que moldam o comportamento e o desempenho. A Perspectiva

Rasmusseniana é particularmente valiosa aqui, ao demonstrar como decisões em níveis macro (regulatório, corporativo, gerencial) criam gradientes de pressão que empurram atividades em direção às fronteiras de segurança no nível micro (operacional). Sem esta compreensão multinível, intervenções tratam sintomas enquanto causas estruturais permanecem intocadas (Rasmussen, 1997). Esta expansão atravessa todos os cinco movimentos – não como movimento adicional, mas como princípio orientador da prática de cada um.



4.3 Dinâmicas da Mudança: Obstáculos, Resistências e Armadilhas da Transformação

Lançar-se numa jornada de Fatores Humanos é lançar-se num processo de transformação organizacional profundo. É fundamental que organizações reconheçam, desde o início, que este processo enfrentará resistências e dinâmicas indesejadas – não como exceções, mas como características inerentes a qualquer mudança organizacional (Henriqson, 2023).

Fontes de resistência sistêmica

Tudo em volta convida a organização a continuar fazendo exatamente como estava fazendo. As fontes de resistência incluem: o **modelo de comando e controle** institucionalizado, que é confortável tanto para líderes quanto para liderados; dimensões culturais brasileiras, como a combinação de **alta aversão à incerteza** e **alto distanciamento de poder** (Hofstede, 2001), que reforçam a demanda por controle hierárquico; o **modelo regulatório e jurídico**, que incentiva conformidade documental; e a **pressão por performatividade** – tudo tem que ser rápido, com resultados imediatos e visíveis (Henriqson, 2023). Um trabalho de evolução e desenvolvimento organizacional, contudo, requer tempo, consistência e persistência.

A dinâmica da incoerência

Um dos riscos mais significativos da jornada é a construção de incoerências entre o que a organização *diz* e o que efetivamente *faz*. A empresa declara seus princípios – "errar é normal" – mas a primeira investigação subsequente conta a história do erro do trabalhador: desatento, cometedor do ato inseguro. Quando se constrói incoerência, gera-se desconfiança e silêncio organizacional (Henriqson, 2023).

A **coerência entre o que se diz e o que se faz** é, portanto, uma das métricas mais importantes da jornada – e requer atenção constante da governança.

O fenômeno dos "heróis" e a personalização

No meio do processo, inevitavelmente surgem indivíduos que tentam personificar a jornada e construir a transformação em torno de si e de uma agenda própria. O risco é que se tornem estereótipos idealizados de uma visão que a organização como um todo ainda não incorporou – gerando mais resistência do que adesão. A jornada precisa ser **institucionalizada**, não personalizada. Quando a transformação depende de um indivíduo, ela é frágil; quando é incorporada às estruturas e processos da organização, torna-se sustentável (Henriqson, 2023).

Dinâmica sociológica de "não ver"

Quando segurança é avaliada exclusivamente por indicadores de estados estáticos – taxas de frequência, dias sem acidentes –, constrói-se uma dinâmica que simultaneamente revela e oculta: revela o esforço de prevenção, mas oculta a erosão de defesas, a normalização de desvios e a deriva para falhas que operam sob a superfície dos bons indicadores. Esta apego aos indicadores estáticos pode coexistir com a migração real em direção às fronteiras de segurança – como tragicamente demonstrado nos desastres de Texas City (Hopkins, 2008) e Macondo (Hopkins, 2012).

Armadilhas analíticas da Engenharia de Resiliência

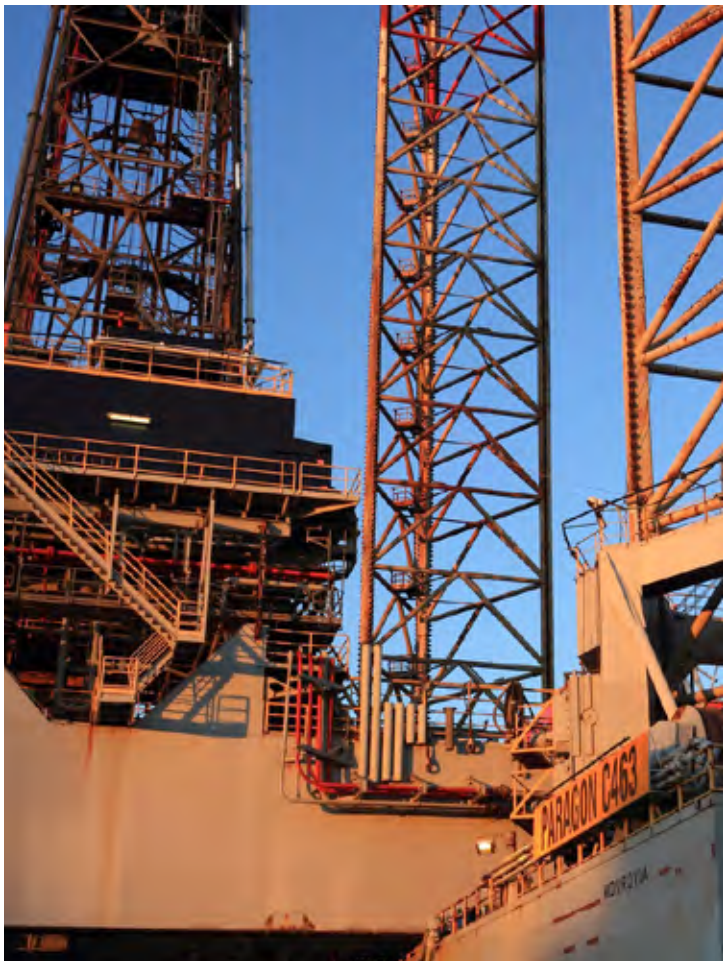
Além das resistências e dinâmicas culturais descritas acima, Bergström e Dekker (2019) identificam três **armadilhas analíticas** a que a Engenharia de Resiliência – e, por extensão, qualquer framework apoiado em capacidades adaptativas – se mostra particularmente vulnerável. Essas armadilhas são especialmente relevantes para a aplicação na indústria de óleo e gás brasileira:

- **Armadilha reducionista:** transferir toda a responsabilidade pela resiliência para a linha de frente (*sharp end*), esperando que suas capaci-

dades adaptativas garantam o funcionamento do sistema. É a armadilha mais comum em ambientes onde a pressão de eficiência é alta e as condições estruturais permanecem intocadas – a "resiliência apesar do sistema", não "graças ao sistema" (Bergström & Dekker, 2019).

- **Armadilha moral:** uso do conceito de resiliência para *responsabilização* de trabalhadores por condições sistêmicas que estão além de seu controle – uma versão refinada da Visão Tradicional.
- **Armadilha normativa:** tratamento da resiliência como propriedade sempre positiva, silenciando a questão sobre se certos riscos deveriam ser aceitos em primeiro lugar.

O reconhecimento destas armadilhas tem implicação direta para o framework: o Movimento V (Resiliência e Capacidade Adaptativa) só é genuíno quando ancorado nos Movimentos I (governança que prioriza investimentos estruturais) e IV (alinhamento de sistemas que ampliam – não restringem – a margem de manobra organizacional). Resiliência delegada ao *sharp end* sem suporte estrutural não é resiliência: é exposição.



4.4 Ênfase na Prevenção de Eventos com Potencial de Gravidade: Segurança de Processo e Segurança Pessoal

A indústria de óleo e gás opera sistemas sociotécnicos de alto risco, onde a interação entre operadores humanos, tecnologia avançada e estruturas organizacionais pode determinar a diferença entre operações bem-sucedidas e falhas catastróficas (Hopkins, 2012). Um princípio fundamental do framework integrador é o foco na **Segurança de Processo** e na prevenção de eventos que podem levar a cenários de grandes emergências – acidentes com potencial de múltiplas fatalidades, danos ambientais severos ou perdas catastróficas de ativos. Essa ênfase, porém, não coloca a **Segurança Pessoal** em segundo plano. Os dois ramos têm o mesmo objetivo final – **evitar eventos que tiram ou mudam vidas** – e diferem apenas nos precursores e nas barreiras de cada um (Seção 4.4.1). A proposta, então, é dar **ênfase ao potencial de gravidade das consequências**, **e não apenas à frequência dos eventos**. No campo pessoal, isso significa conduzir a gestão com base em indicadores de severidade e de potencial (SIF/Potencial SIF, Seção 4.4.2). Assim, mantém-se o cuidado preventivo com lesões graves e fatais, sem cair nos problemas de dar peso excessivo a eventos de baixa severidade. Os fundamentos conceituais e ferramentais desta abordagem (MAH, HAZOP, bow-tie, Conjuntos Solidários de Barreiras - CSB, LOPA, HSE Case) estão consolidados na Seção 3.6 deste compêndio. Esta seção foca em *como* o framework integrador endereça a prevenção de eventos de alta gravidade, nos eixos de processo e pessoal, por meio dos cinco movimentos.

4.4.1 A Distinção Crítica: Segurança Pessoal versus Segurança de Processo

Em coerência com a opção terminológica registrada na Seção 3.6.1 (nota [^2]) – que adota "segurança pessoal" como termo primário, reservando "segurança ocupacional" à sua acepção brasileira consagrada –, conforme demonstrado pelo SINTEF (Rosness et al., 2010), acidentes pessoais menores e acidentes organizacionais maiores frequentemente surgem de padrões diferentes de problemas de segurança. Uma organização que exibe excelentes indicadores de LTI (*Lost Time Injuries*) pode estar caminhando para um desastre, já que alguns dos fatores que contribuem para o risco de acidentes maiores têm pouco impacto na frequência de LTIs. Os desastres de Texas City (2005) e Macondo (2010) – que resultaram em 15 e 11 fatalidades, respectivamente – ilustram tragicamente esta falácia: em ambos os casos, indicadores de segurança pessoal aparentemente satisfatórios coexistiam com falhas sistêmicas em Segurança de Processo (U.S. CSB, 2007; Hopkins, 2008, 2012).

Esta distinção tem implicações profundas para a jornada de Fatores Humanos: estratégias preventivas que funcionam bem para acidentes menores podem ser insuficientes para controlar riscos de acidentes maiores. Programas de cultura de segurança direcionados exclusivamente à prevenção de acidentes pessoais não substituem barreiras adequadas contra acidentes de processo (CSB, 2007).

Os efeitos adversos da ênfase excessiva em eventos de baixa severidade

A distinção entre os dois ramos tem, ainda, uma consequência prática frequentemente subestimada: **priorizar métricas de frequência de eventos menores (TRIR, LTIR) não é apenas insuficiente – pode ser contraproducente**. Quando esses indicadores se tornam o principal foco de gestão e de incentivo, três efeitos adversos tendem a emergir:

- **Distorção do foco ("formiga e elefante").** Recursos, atenção gerencial e esforço de observação migram para os eventos frequentes e de baixa consequência, que inflam o TRIR, em detrimento das exposições raras e de alto potencial. Análises de centenas de milhões de observações com-

portamentais mostram foco cerca de cinco vezes maior em itens de baixa consequência (p. Ex., EPI) do que em atividades de alto potencial (trabalho em altura, espaços confinados, energia elétrica) (Busch et al., 2019).

- **Silêncio organizacional (subnotificação defensiva)**. Quando o desempenho é julgado pela contagem de lesões menores, cria-se o receio de "estragar o indicador", o que desencoraja o registro de eventos e quase-acidentes e mascara a exposição real. Estima-se que mais da metade das lesões graves não fatais não seja reportada, ao passo que fatalidades são muito mais difíceis de omitir (Michaels, 2016; Busch et al., 2019).
- **Comprometimento da capacidade de enxergar o risco estrutural**. O foco em eventos de baixa severidade consome a capacidade organizacional de detectar e tratar riscos estruturais e potencialmente fatais, deteriorando justamente a vigilância sobre as barreiras que previnem SIF e acidentes de processo.

Em conjunto, esses efeitos explicam por que a mera redução do TRIR/LTIR pode conviver com, ou até anteceder, a estabilidade ou o aumento das fatalidades, reforçando a necessidade de indicadores orientados à severidade e ao potencial (SIFR e PSIFR), abordados na Seção 4.4.2.

4.4.2 Eventos SIF e Potencial SIF: foco no Potencial de Gravidade

Os conceitos de **SIF (Serious Injury or Fatality)** e **Potencial SIF** representam uma evolução importante na gestão de segurança. Enquanto a pirâmide tradicional de Heinrich sugere uma relação proporcional entre incidentes menores e maiores, evidências empíricas demonstram que eventos com potencial de consequências catastróficas frequentemente apresentam precursores distintos. O framework integrador enfatiza:

- **Identificação de precursores SIF:** eventos que, sob circunstâncias ligeiramente diferentes, poderiam ter resultado em fatalidades ou lesões graves.
- **Análise de exposição a energias perigosas:** hidrocarbonetos sob pressão, cargas suspensas, trabalho em altura, espaços confinados, energias acumuladas.

- **Investigação diferenciada:** eventos com Potenciais SIF devem receber o mesmo rigor investigativo que eventos SIF reais.

Definição entre SIF real e Potencial SIF; indicadores SIFR e PSFR

A gestão de SIF distingue dois estados mutuamente exclusivos de um mesmo evento. O **SIF real** (SIFa – actual) designa o evento em que a lesão grave ou a fatalidade efetivamente ocorreu. O **Potencial SIF** (SIFp – potential) designa o evento que, sob circunstâncias apenas ligeiramente diferentes, teria resultado em lesão grave ou morte, ainda que o desfecho real tenha sido leve ou nulo. Por serem mutuamente exclusivos, um mesmo evento é classificado como SIFa ou SIFp, não como ambos, o que permite que suas taxas sejam lidas conjuntamente, sem dupla contagem, como medida da exposição total a consequências severas (IADC, 2026; IOGP, 2022).

Definem-se, correspondentemente, dois indicadores de taxa, análogos em construção ao TRIR: o **SIFR** (*Serious Injury and Fatality Rate*), que mede a frequência de SIF reais, e o **PSIFR** (*Potential Serious Injury and Fatality Rate*), que mede a frequência de eventos com potencial SIF. Ambos são normalizados por horas-homem expostas (tipicamente por 200.000 ou 1.000.000 de horas). O SIFR é um indicador reativo de baixa frequência e alta severidade; o PSIFR, por capturar também os quase-acidentes de alto potencial, comporta-se como indicador mais sensível e antecipatório do estado das defesas contra eventos severos (Martin & Black, 2015; Campbell Institute, 2019).

Estudos empíricos estabelecem um limiar operacional de alta energia da ordem de 500 ft-lb (≈ 680 J): acima desse patamar, a probabilidade de que um evento resulte em SIF torna-se preponderante (Hallowell et al., 2017; EEI, 2024). As formas de energia usualmente consideradas incluem gravidade e altura, movimento e linha de fogo, energia mecânica, elétrica, pressão, temperatura, energia química, radiação, som e agentes biológicos (Alexander, Hallowell & Gambatese, 2017; EEI, 2024).

Essa lógica é convergente com a perspectiva de barreiras adotada na Seção 3.6: o Potencial SIF é, em essência, um evento de alta energia no qual as barreiras de prevenção estavam ausentes, foram transgredidas ou mostraram-se inadequadas. A diferença de natureza dos precursores – pessoais (por exemplo, objeto suspenso sobre um trabalhador) versus de processo (perda de contenção primária) – recomenda manter indicadores distintos para cada eixo, evitando que a soma de precursores heterogêneos dilua o sinal específico de cada um (Rosness et al., 2010; Hopkins, 2008).

Evidência empírica: o descolamento entre frequência e severidade

A justificativa empírica para tratar SIF/Potencial SIF como objeto próprio é o descolamento sistemático entre a queda das taxas de frequência (TRIR/LTIR) e a persistência – ou o aumento – das lesões graves e fatais. Três conjuntos de dados independentes ilustram o fenômeno.

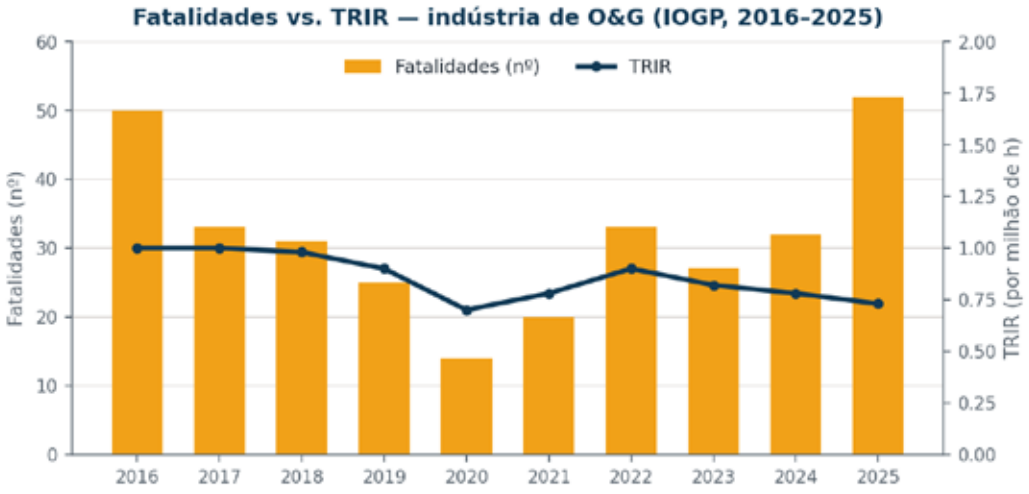


Figura 4.4.1. Fatalidades (n) vs. TRIR na indústria de óleo e gás. Em 2025 registraram-se 52 fatalidades (a maior série desde 2016), com a FAR subindo cerca de 75% frente a 2024, ainda que o TRIR tenha recuado ~6%. **Fonte:** IOGP, Safety performance indicators 2024 data (2025).

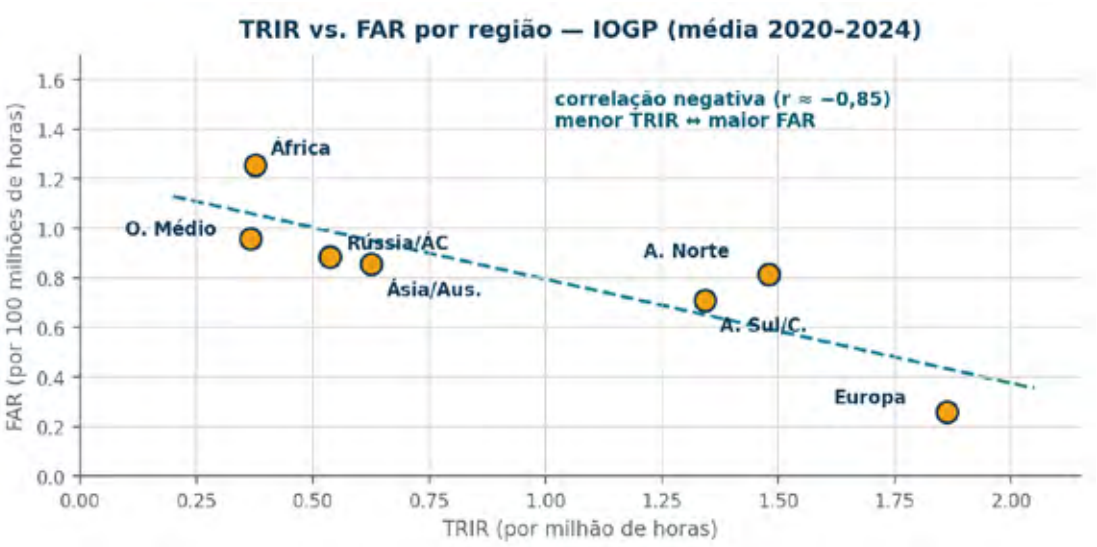


Figura 4.4.2. TRIR vs. FAR por região (média 2020 – 2024). Regiões com menor TRIR tendem a apresentar maior FAR (correlação negativa, r= -0,85): a Europa reporta o maior TRIR e a menor FAR, enquanto África, Rússia e Oriente Médio combinam baixo TRIR e alta FAR. **Fonte:** elaborado a partir de IOGP, *Safety performance indicators* 2024 data (2025).

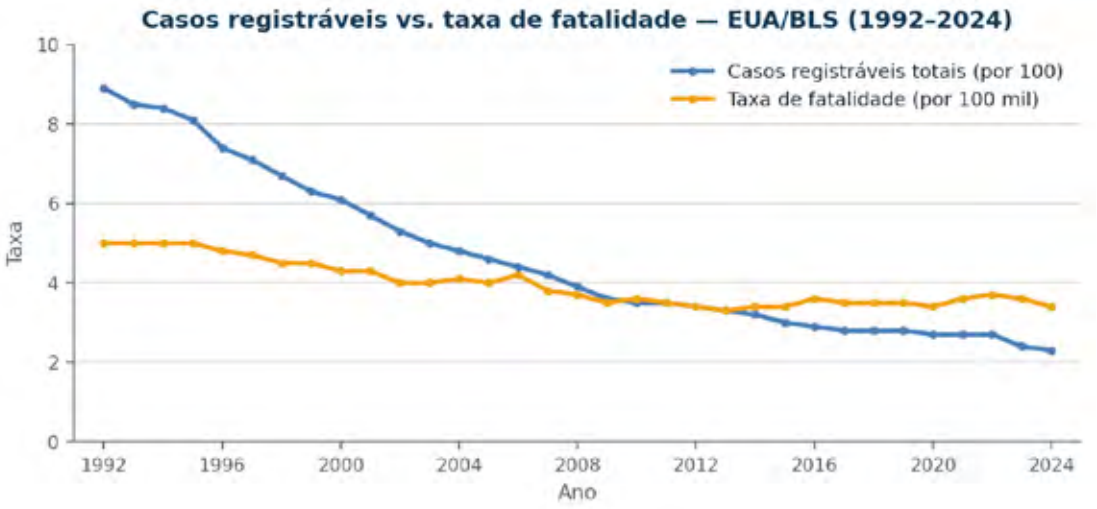


Figura 4.4.3. Casos registráveis vs. taxa de fatalidade nos EUA (BLS, 1992 – 2024). Os casos registráveis caíram de forma acentuada, enquanto a taxa de fatalidade permaneceu essencialmente estável por mais de uma década. Nota: quebra metodológica na série de registráveis em 2002 (*recordkeeping* OSHA). Fontes: BLS/SOII e BLS/CFOI; leitura do paradoxo conforme Busch et al. (2019).

Como sintetizou Terrie Norris (então presidente da ASSP, 2011), "um platô estatístico de fatalidades não é uma conquista, mas evidência de que os esforços para proteger trabalhadores estão estagnados" (apud Busch et al., 2019). Em termos

de indicadores: reduzir o TRIR e o LTIR não é o mesmo que reduzir os eventos que tiram ou alteram vidas – o TRIR não prediz a fatalidade (Hallowell et al., 2021).

Recomendação de Indicadores Combinados: SIFR e PSIFR

Recomenda-se, portanto, que o eixo de Segurança Pessoal seja monitorado por SIFR (dano real) e PSIFR (dano potencial), ao lado dos indicadores de Segurança de Processo (Seção 3.6.5). Para fins de leitura de tendência, SIFR e PSIFR podem ser somados como exposição total a SIF, dada a exclusividade mútua entre SIFa e SIFp; para fins de incentivo, contudo, recomenda-se preservar o SIFR como condição de barreira (gate) de modo que um SIF real não seja compensado por bom desempenho no PSIFR, mantendo o PSIFR como métrica contínua de melhoria (Martin & Black, 2015; IOGP, 2022).

4.4.3 Monitoramento de Elementos Críticos e Sinais de Alerta (Warning Signals)

Em sistemas de alto risco com grandes energias, a saúde e integridade de **elementos críticos de segurança operacional** – conforme definido pela NT 10/2023 ANP – deve ser continuamente monitorada. Isto inclui equipamentos críticos, sistemas críticos e procedimentos críticos essenciais para prevenção ou mitigação de acidentes associados a grandes emergências.

A perspectiva de barreiras (Reason, 1997; Hollnagel, 2004) enfatiza que funções de barreira precisam ser monitoradas e mantidas. Elementos de barreira podem deteriorar-se e interdependências entre barreiras podem surgir ou aumentar. O monitoramento de risco deve investigar atributos de cada função de barreira individual e das relações entre elas – como uma função pode falhar, se existem interdependências (falhas de causa comum), como funções podem deteriorar-se ao longo do tempo, e quais indicadores podem medir disponibilidade e eficiência.

Warning signals (sinais de alerta) são manifestações precoces de deterioração de barreiras ou condições latentes que podem preceder acidentes organizacionais.

A capacidade de detectar, interpretar e responder a estes sinais é característica distintiva de Organizações de Alta Confiabilidade (Weick & Sutcliffe, 2015).

4.4.4 Contribuição dos Cinco Movimentos para a Segurança de Processo e Pessoal (SIF/Potencial SIF)

A Tabela 4.4.1 sintetiza como cada movimento do framework integrador contribui especificamente para a gestão da Segurança de Processo e da Segurança Pessoal – esta, no sentido de prevenção de lesões graves e fatais (SIF/Potencial SIF). A leitura recomendada é horizontal e vertical: horizontal, para compreender a contribuição de cada movimento isoladamente; vertical, para reconhecer que tanto a Segurança de Processo, quanto a Segurança Pessoal são **propriedades emergentes da integração** dos cinco movimentos, não responsabilidade exclusiva de qualquer um deles.



Tabela 4.4.1: Contribuição dos cinco movimentos para a Segurança de Processo e Pessoal (SIF/Potencial SIF)

Movimento	Contribuição para Segurança de Processo	Contribuição para Segurança Pessoal
I. Governança	Priorização estratégica da gestão de barreiras; visibilidade dos indicadores de processo (Tier 1–4) em fóruns executivos; legitimidade para deliberar sobre revisão de práticas que erodem defesas; alocação de recursos para manutenção e verificação de Elementos Críticos de Segurança Operacional (ECSO).	Elevação do SIFR e do PSIFR em indicadores de primeiro nível (Level 1) nos fóruns executivos; adoção do SIFR como gate de tolerância zero a SIF real e do PSIFR como métrica contínua de melhoria; alocação de recursos para controles diretos de energias perigosas de alto potencial, em vez de foco na frequência de eventos menores (TRIR/LTIR).
II. Fluência	Capacitação de lideranças e linha gerencial em conceitos de Major Accident Hazards (MAH), Conjuntos Solidários de Barreiras (CSB), bow-tie, deriva prática e degradação de barreiras; superação da falácia LTI-como-proxy-da-Segurança de Processo.	Capacitação em precursores de SIF baseados em energia (limiar de alta energia da ordem de 500 ft-lb / 680 J) e nas formas de energia perigosa (gravidade e altura, linha de fogo, mecânica, elétrica, pressão, temperatura, química); compreensão do descolamento entre frequência (TRIR) e severidade e dos efeitos adversos da ênfase excessiva em eventos de baixa severidade.
III. Aprendizagem	Detecção precoce de adaptações cotidianas que sinalizam degradação de barreiras; Learning Teams aplicados a tarefas críticas de segurança operacional; warning signals visíveis através da Aprendizagem Operacional, antes que se materializem como eventos SIF.	Investigação de eventos com Potencial SIF com o mesmo rigor dos SIF reais; Learning Teams aplicados a exposições de alta energia com controles ausentes ou ineficazes; identificação de *warning signals* no eixo pessoal e combate à subnotificação defensiva (silêncio organizacional).

Movimento	Contribuição para Segurança de Processo	Contribuição para Segurança Pessoal
IV. Alinhamento	Revisão dos sistemas de indicadores para incluir métricas específicas de processo (Tier 1–4); investigação diferenciada para eventos Potencial SIF; integração de Análise de Confiabilidade Humana (HRA) nas tarefas críticas; alinhamento entre HSE Case e práticas operacionais reais.	Monitoramento do eixo pessoal por SIFR (dano real) e PSIFR (dano potencial), mantidos distintos dos indicadores de processo para não diluir o sinal de cada eixo; classificação por severidade real e potencial (classes 4 - 5); integração de HRA em tarefas de alta energia.
V. Resiliência	Capacidade de antecipar combinações inéditas de degradação de barreiras (falhas de causa comum, interdependências emergentes); HSE Case como instrumento vivo de aprendizagem, revisado a cada modificação significativa; monitoramento dinâmico que vai além da verificação periódica isolada.	Antecipação de exposições inéditas de alta energia e de combinações de controles ausentes; monitoramento dinâmico da presença e eficácia dos controles diretos (leading indicators), em vez da contagem reativa de lesões; adaptação dos controles a condições operacionais variáveis.

Quando a Segurança de Processo e a Segurança Pessoal são tratadas como tarefa exclusiva de uma disciplina técnica – a engenharia de segurança, a engenharia de perfuração ou de processo da planta, ou o departamento de saúde e segurança –, sem integração com a jornada de Fatores Humanos, o resultado tende a ser previsível: barreiras tecnicamente bem desenhadas, mas progressivamente erodidas por adaptações operacionais não monitoradas; sistemas de gestão desconectados do trabalho real; e indicadores que medem o que é fácil de medir, e não o que importa. O framework integrador busca responder a essa lacuna.

4.5 Matriz de Aplicação por Perspectiva Teórica

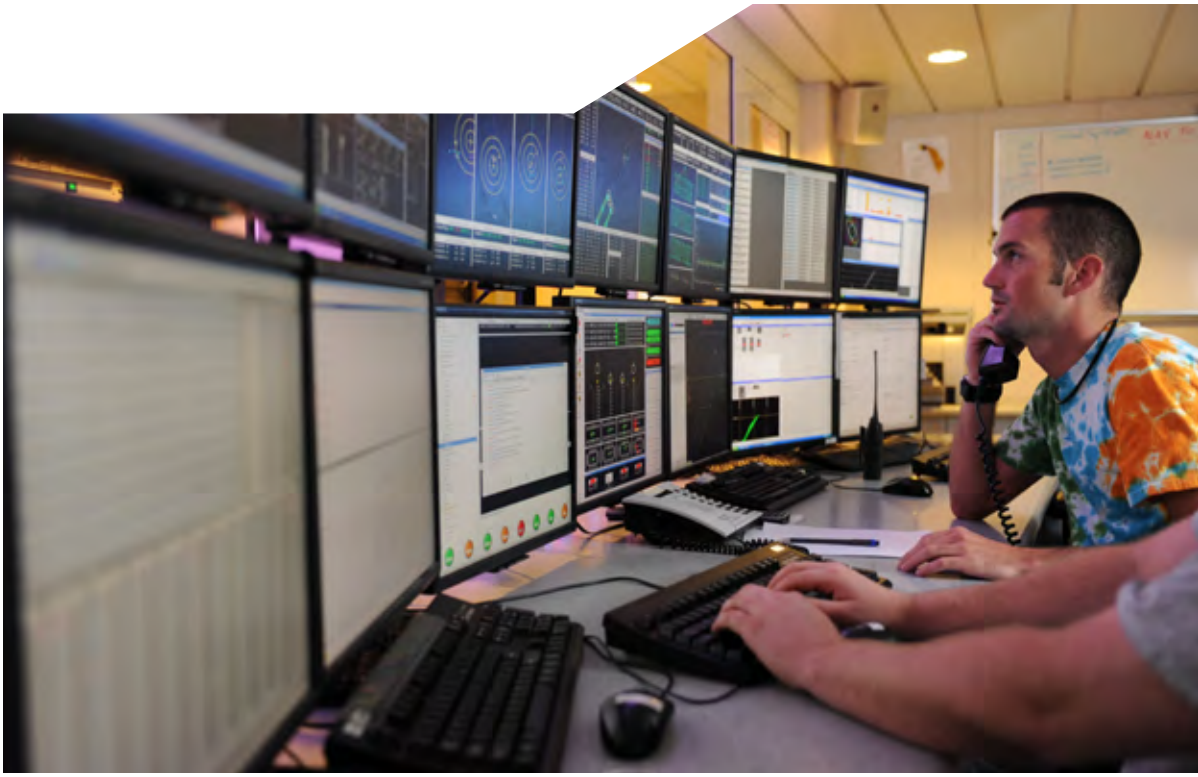
Cada perspectiva teórica apresentada na Parte II oferece contribuições específicas que podem ser mobilizadas em diferentes contextos e para diferentes propósitos. A Tabela 4.5.1 sintetiza as aplicações recomendadas de cada escola, orientando organizações na seleção de lentes analíticas adequadas aos seus desafios específicos.

Tabela 4.5.1: Matriz de aplicação por perspectiva teórica

Perspectiva	Contribuição Central	Aplicações Recomendadas
NAT / Acidentes Normais	Riscos estruturais de complexidade e acoplamento forte; limites inerentes de sistemas	Avaliação de riscos sistêmicos; design de sistemas; decisões sobre automação; análise de limites estruturais de segurança
HRO / Alta Confiabilidade	Mindfulness organizacional; processos cognitivos coletivos; preocupação crônica com falhas potenciais	Desenvolvimento de cultura; governança de segurança; decisões em ambientes dinâmicos; gestão de operações de alto risco
Perspectiva Rasmusseniana	Migração para fronteiras; gradientes de pressão; análise multinível (micro-macro)	Investigação de acidentes (AcciMap); análise de pressões organizacionais; gestão de trade-offs segurança-produção-eficiência
Engenharia de Resiliência	Capacidades adaptativas (responder, monitorar, antecipar, aprender); variabilidade como recurso	Análise funcional (FRAM); desenvolvimento de capacidades adaptativas; Safety-II; compreensão de sucesso operacional
Dependência de Trajetória	Dimensão temporal; normalização do desvio; incubação de desastres; segredo estrutural	Detecção de deriva organizacional; análise histórica de decisões; prevenção de erosão de margens de segurança; warning signals

Esta matriz é instrumento de seleção, não hierarquia de valor: nenhuma pers-

pectiva esgota o fenômeno, e a escolha da lente apropriada depende do recorte analítico (a pergunta que se busca responder) e do nível do sistema sob exame (micro, meso ou macro). O pluralismo teórico declarado em 4.1.1 manifesta-se aqui como prática: organizações maduras transitam entre perspectivas conforme o problema, evitando tanto a captura dogmática por uma única escola quanto o ecletismo superficial que diluiria a contribuição de cada uma



4.6 A Expansão do Olhar: Do Micro ao Macro

O princípio orientador da expansão do olhar do micro para o macro – desenvolvido em detalhe na Síntese da Seção 4.2.6 – perpassa todos os cinco movimentos e merece registro próprio como diretriz transversal. Embora a ênfase em indivíduos, decisões e adaptações nas linhas de frente seja necessária, por si só não é suficiente. Uma jornada transformadora examina também estruturas de poder, projetos e recursos existentes, pressões de produção e dinâmicas organizacionais que moldam comportamento e desempenho (Rasmussen, 1997). Sem esta compreensão multinível, intervenções tratam sintomas enquanto causas estruturais permanecem intocadas. Para a operacionalização deste princípio, ver a subseção "Expansão micro → macro" no Movimento II (4.2.2) e a síntese em 4.2.6.

4.7 Integração do Ecossistema Setorial: Contratantes, Contratadas e Regulador

A transformação em Fatores Humanos não pode se limitar às fronteiras de uma única organização. Na indústria de óleo e gás, operações envolvem ecossistemas complexos de contratantes, prestadores de serviços, fornecedores e agências regulatórias – todos interconectados e mutuamente influentes. Como destacado pela experiência da Constellation, a jornada de transformação deve envolver "as lideranças e a força de trabalho, própria e terceirizada, parceiros e todos os demais públicos de interesse" (Almeida et al., 2025).

4.7.1 Parceria ao longo da Cadeia de Contratação

A **relação entre contratantes e contratadas é um dos pontos mais críticos na gestão de Fatores Humanos** – e um dos que mais se beneficiam da mudança de modelo mental discutida em 4.1.2. Esta relação assume configurações distintas ao longo da cadeia produtiva do setor: entre operadoras e prestadoras de serviço; entre contratistas de perfuração (*drilling contractors*) e suas próprias contratadas e subcontratadas; e em modelos integrados (EPC, contratos guarda-chuva, integrated services), nos quais uma mesma empresa acumula papéis de contratante e contratada em diferentes frentes do mesmo empreendimento. Independentemente da configuração específica, os mesmos riscos estruturais se manifestam sempre que uma organização depende de mão de obra ou de serviços fornecidos por outra pessoa jurídica, razão pela qual as recomendações desta seção devem ser lidas como aplicáveis a qualquer par contratante-contratada da cadeia, e não apenas ao par operadora-prestadora de serviço. Como já demonstrado pelo IOGP Report 453 (Seção 1.2), o desenho de contratos e as interfaces entre organizações figuram entre os fatores sistêmicos que explicam a maior parte dos eventos rotulados superficialmente como "descumprimento de regra", o que desloca a per-

gunta de "como fiscalizar melhor a contratada" para "como o desenho da relação contratual cria ou remove condições para o trabalho seguro". Modelos contratuais tradicionais podem, inadvertidamente, criar pressões que minam os princípios de FH. As barreiras identificadas incluem (Almeida et al., 2025): a interface cliente/contratada, com demandas e expectativas concorrentes; o foco na conformidade regulatória, que pode conflitar com a construção de capacidade adaptativa; e a ciclicidade dos negócios, que desvia a atenção sob pressões econômicas. A esses riscos soma-se uma dimensão relacional: como observam Rosness et al. (2000; cf. Seção 2.2), a terceirização pode minar a confiança e a abertura mútuas necessárias à dimensão cultural da redundância organizacional, e a subordinação hierárquica da força de trabalho terceirizada tende a inibir a intervenção entre pares justamente nos momentos em que ela mais protege o sistema. Por isso, o framework integrador trata esta relação, em qualquer ponto da cadeia em que ocorra, não como interface cliente-fornecedor a ser gerenciada, mas como **parceria a ser construída**, coerente com a citação que abre a Seção 4.7, que inclui explicitamente "força de trabalho, própria e terceirizada, parceiros e todos os demais públicos de interesse" (Almeida et al., 2025) no escopo da jornada.

Condições de contorno ao longo do contrato. O contrato fixa as condições de contorno do trabalho de quem opera pelo contratante (escopo, prazos, efetivo, recursos e indicadores) à luz do ambiente existente na assinatura (Rasmussen, 1997; cf. Seção 2.3). Ao longo da vigência, esse ambiente muda; as cláusulas, não. Sem monitoramento, a diferença é absorvida pelos ajustes da linha de frente, o que empurra o risco para baixo na cadeia. E, como a confiabilidade de uma operação em rede é da rede e não de um elo, o risco transferido retorna ao contratante. Daí uma pergunta que os indicadores contratuais raramente respondem: a que custo os resultados estão sendo entregues?

Práticas de integração recomendadas: inclusão de lideranças de contratados-chave nos Laboratórios de Fatores Humanos; programas conjuntos de capacitação; sistemas compartilhados de aprendizagem operacional; revisão conjunta de cláusulas contratuais para alinhamento aos princípios e fundamentos de Fatores Humanos; métricas de desempenho que incentivem transparência e aprendizagem; revisão periódica, ao longo da vigência do contrato, da adequação das condições de contorno ao trabalho real, com participação da contratada; indicadores que revelem também as condições que produzem os resultados (por exemplo, horas

extras, backlog e soluções de contorno), não utilizados como gatilho automático de penalidade; e, em arranjos com múltiplos elos contratuais (ex.: operadora → *drilling contractor* → prestadoras especializadas), estendendo essas mesmas práticas a cada elo da cadeia, evitando que princípios e fundamentos de Fatores Humanos se apliquem apenas ao primeiro nível de contratação e se diluam nos elos subsequentes.

4.7.2 Parceria com a Agência Regulatória

A NT 10/2023 da ANP representa um avanço significativo ao estabelecer requisitos para a integração de Fatores Humanos no ciclo de vida das instalações. Contudo, a relação entre indústria e regulador pode ir além da mera conformidade para constituir parceria genuína no avanço do campo: diálogo técnico através de participação conjunta em fóruns e workshops; mecanismos de compartilhamento de lições aprendidas; codesenvolvimento de guias de boas práticas; e contribuição técnico-científica para aprimoramento contínuo do framework regulatório.

O próprio Grupo de Trabalho de Fatores Humanos da ABESPetro – sob cuja iniciativa este compêndio foi produzido – constitui exemplo concreto deste modo de relação: um espaço setorial onde empresas associadas, especialistas acadêmicos e referências regulatórias convergem para coconstruir vocabulário comum, repertório técnico e diretrizes alinhadas aos requisitos da NT 10/2023. A obra é, ela própria, instância do que recomenda – a transformação setorial é trabalho coletivo, não soma de iniciativas isoladas.



4.8 Articulação com a NT 10/2023 da ANP

O framework integrador oferece fundamentação conceitual para atendimento qualificado aos requisitos da NT 10/2023, transcendendo a mera conformidade documental para desenvolver capacidades organizacionais genuínas. A articulação entre movimentos da jornada e requisitos regulatórios permite que organizações desenvolvam competências reais enquanto demonstram conformidade.



4.9 A Jornada como Compromisso Contínuo

O framework integrador apresentado nesta Parte IV não é prescrição definitiva, mas convite ao engajamento crítico. Como toda jornada genuína, não possui ponto de chegada final – apenas horizontes que se expandem à medida que avançamos. A experiência da Constellation demonstra que a aplicação sistemática de princípios de Engenharia de Resiliência pode promover uma transformação organizacional significativa em indústrias de alto risco e complexas, movendo-se além de abordagens orientadas à conformidade, em direção à construção de capacidade adaptativa e de sistemas de aprendizagem contínua (Almeida et al., 2025).

Três lembretes finais para organizações que iniciam ou dão continuidade a sua jornada:

1. **Começar pelo entendimento, não pela solução.** Investir tempo em compreender como o trabalho realmente acontece – suas pressões, adaptações e racionalidades locais – é pré-requisito para intervenções efetivas.
2. **Privilegiar aprendizagem sobre conformidade.** O objetivo não é provar que fazemos as coisas certas, mas sim descobrir continuamente como fazer melhor.
3. **Reconhecer que mudança é gradual.** Um ciclo completo de transformação organizacional demanda tempo – estimativas conservadoras apontam para períodos de dois anos ou mais.

É nesse ponto que a Parte IV se fecha sobre si mesma – não com uma resposta, mas com o lembrete que Woods e colegas deixam à comunidade da segurança:

> *"Organizações de alta confiabilidade não tomam o sucesso passado como razão para confiança; em vez disso, continuam investindo na antecipação do potencial mutável de falha" — Woods et al., 2010.*

Referências da Parte IV

Alexander, D., Hallowell, M., & Gambatese, J. (2017). Precursors of construction fatalities. II: Predictive modeling and empirical validation. Journal of Construction Engineering and Management, 143(7), 04017024.

Almeida, R. C., Bruno, J. C. S., & Capaverde, C. B. (2025). A learning journey toward more resilient systems: The case of a Brazilian oil and gas company. In Proceedings of the Joint 11th Biennial Symposium of the Resilience Engineering Association and 14th Annual Resilient Health Care Society Meeting (pp. 47–54). REA/RHCS.

Bergström, J., & Dekker, S. W. A. (2019). The 2010s and onward: Resilience engineering. In S. W. A. Dekker, Foundations of safety science: A century of understanding accidents and disasters (pp. 391–426). CRC Press.

Bergström, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. Reliability Engineering & System Safety, 141, 131–141. https://doi.org/10.1016/j.ress.2015.03.008

Bruno, J. C. S. (2020). Human factors in deepwater drilling: A new approach to safety and operational excellence [Dissertação de mestrado, Lund University]. Lund University Publications.

Busch, C., Usrey, C., Loud, J., Goodell, N., & Carrillo, R. A. (2019). Serious injuries and fatalities: Why do they remain constant while injury rates decline? [White paper].

Campbell Institute. (2019). Serious injury and fatality prevention: Perspectives and practices. National Safety Council.

Chemical Safety and Hazard Investigation Board. (2007). Investigation report: Refinery explosion and fire (BP Texas City) (Report No. 2005-04-I-TX). CSB.

Conklin, T. (2019). The 5 principles of human performance: A contemporary update of the building blocks of human performance for the new view of safety. PreAccident Media.

Deal, T. E., & Kennedy, A. A. (1982). Corporate cultures: The rites and rituals of corporate life. Addison-Wesley.

Dekker, S. W. A. (2012). Just culture: Balancing safety and accountability (2ª ed.). Ashgate.

Dekker, S. W. A. (2017). Just culture: Restoring trust and accountability in your organization (3ª ed.). CRC Press.

Dekker, S. W. A. (2019). Foundations of safety science: A century of understanding accidents and disasters. CRC Press. https://doi.org/10.4324/9781351059794

Dekker, S. W. A., Rafferty, J., & Oates, A. (Eds.). (2022). Restorative just culture in practice: Implementation and evaluation. Routledge/Productivity Press. https://doi.org/10.4324/9781003162582.

Edison Electric Institute. (2024). High-energy hazards and controls inventory. EEI.

Edmondson, A. C. (2019). The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth. Wiley.

Hallowell, M. R., Alexander, D., & Gambatese, J. A. (2017). Energy-based safety risk assessment: Does magnitude and intensity of energy predict injury severity? Construction Management and Economics, 35(1–2), 64–77.

Hallowell, M. R., Quashne, M., Salas, R., Jones, M., MacLean, B., & Quinn, E. (2021). The statistical invalidity of TRIR as a measure of safety performance. Construction Safety Research Alliance, University of Colorado Boulder.

Henriqson, E. (2023). Nova visão de segurança: Princípios, práticas, cultura e gestão da mudança [Palestra]. Nova Visão de Segurança Brasil, 30 set. 2023.

Hofstede, G. (2001). Culture's consequences (2ª ed.). Sage.

Hollnagel, E. (2004). Barriers and accident prevention. Ashgate.

Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate.

Hollnagel, E. (2018). Safety-II in practice: Developing the resilience potentials. Routledge.

Hopkins, A. (2008). Failure to learn: The BP Texas City refinery disaster. CCH Australia.

Hopkins, A. (2012). Disastrous decisions: The human and organisational causes of the Gulf of Mexico blowout. CCH Australia.

International Association of Drilling Contractors. (2026). Definition of a serious injury and fatality (SIF). IADC.

International Association of Oil & Gas Producers. (2022). Fatal and process safety incident (FPI) definitions [Flyer]. IOGP.

International Association of Oil & Gas Producers. (2025). Safety performance indicators – 2024 data. IOGP.

Martin, D. K., & Black, A. N. (2015). Preventing serious injuries and fatalities. Professional Safety, 60(9), 35–43.

Rae, A. J., Weber, D. E., & Dekker, S. W. A. (2018). Safety clutter: The accumulation and persistence of 'safety' work that does not contribute to operational safety. Policy and Practice in Health and Safety, 16(2), 194–211. https://doi.org/10.1080/14773996.2018.1491147

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Reason, J. (1997). Managing the risks of organizational accidents. Ashgate.

Rosness, R., Grøtan, T. O., Guttormsen, G., Herrera, I. A., Steiro, T., Størseth, F., Tinmannsvik, R. K., & Wærø, I. (2010). Organisational accidents and resilient organisations: Six perspectives (Report SINTEF A17034, Revisão 2). SINTEF Technology and Society.

U.S. Bureau of Labor Statistics. (2020). Injuries, illnesses, and fatalities (IIF). U.S. Department of Labor. https://www.bls.gov/iif/

Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3ª ed.). John Wiley & Sons.

Woods, D. D., Dekker, S. W. A., Cook, R., Johannesen, L., & Sarter, N. (2010). Behind human error (2ª ed.). Ashgate.

Glossário Técnico Unificado

Este glossário apresenta definições padronizadas dos principais termos utilizados no campo de Fatores Humanos e segurança, incorporando terminologia das principais referências internacionais. As definições foram compiladas a partir das fontes originais citadas ao longo do Compêndio, buscando preservar a precisão conceitual de cada termo.

Total de termos: 140 entradas

A

Accountability

Capacidade de prestar contas sobre ações e suas consequências. O termo deriva de account (relatar, descrever eventos passados) e é mantido em inglês por não haver tradução direta adequada em português (Pellegrino, 2019). Distingue-se de dois construtos vizinhos: da **responsabilidade** (*responsibility*) a obrigação de executar uma tarefa ("*responsibility involves doing; accountability involves reporting*", Ieraci, 2007) e da **responsabilização legal** (*liability*), que implica sujeição a consequências legais. *Accountability* ultrapassa a responsabilidade porque se estende por fronteiras hierárquicas e organizacionais e abrange situações não previstas antecipadamente (Hoskin, 1996). Não é construto único, mas uma **família de práticas** com efeitos distintos sobre a aprendizagem: as formas tradicionais (hierárquica, *backward, outcome*) focam nas consequências de ações individuais, sustentam a lógica de culpa individual (IBL) e favorecem comportamentos defensivos; as formas orientadas ao processo e à melhoria (process, forward) deslocam a atenção para a qualidade da decisão e para os fatores sistêmicos (OFL); as formas relacionais (socializing, lateral) constroem confiança entre pares e favorecem o relato. Sharpe (2003) distingue a *accountability* **retrospectiva** - voltada a eventos passados e à atribuição de culpa - da **prospectiva** - orientada à deliberação sobre os processos e papéis necessários para alcançar a segurança, tratando os profissionais como parte da solução, e não apenas como problema a ser controlado (Dekker & Breakey, 2016). Seus efeitos dependem da **legitimidade percebida**: quando vivenciada como ilegítima, produz polarização de atitudes, queda de motivação intrínseca e estresse (Lerner & Tetlock, 1999). No

arranjo conceitual deste compêndio, **cultura justa é o sistema, *accountability* são as práticas e a aprendizagem organizacional é o resultado**. Ver Seção 3.3.

Ver também: Cultura Justa; Justiça Substantiva; Justiça Processual; Justiça Restaurativa; Justiça Retributiva; Captura Punitiva do Sistema de Accountability; Aprendizagem Organizacional; Teste de Substituição; Segunda Vítima.

Fontes: Pellegrino, 2019; Ieraci, 2007; Hoskin, 1996; Sharpe, 2003; Dekker & Breakey, 2016; Roberts, 1991, 1996; Lerner & Tetlock, 1999; Tetlock, 1985; Parris, 2025.

AcciMap

Ferramenta analítica desenvolvida por Rasmussen para mapear a contribuição de múltiplos níveis organizacionais para acidentes. Representa graficamente como decisões em diferentes níveis (governo, reguladores, empresa, gestão, operações) interagem e contribuem para eventos adversos.

Ver também: Migração para os Limites; Gradiente de Pressão; STAMP.

Fonte: Rasmussen & Svedung, 2000.

Acidente Normal (*Normal Accident*)

Também denominado *acidente de sistema* (*system accident*). Categoria proposta por Charles Perrow (1984/1999) para acidentes caracterizados por múltiplas interações inesperadas entre falhas, onde o "tamanho" da falha não é proporcional ao seu resultado. Emergem das propriedades estruturais do sistema – complexidade interativa e acoplamento estreito –, não de falhas específicas de componentes. Argumento central da Normal Accident Theory (NAT).

Ver também: Complexidade Interativa; Acoplamento Estreito; STAMP.

Fonte: Perrow, 1984, 1999.

Acoplamento Estreito (*Tight Coupling*)

Característica de sistemas onde processos são fortemente interdependentes, com pouca folga ou amortecimento entre eles, permitindo que falhas se propaguem rapidamente. Em sistemas fortemente acoplados: processos são dependentes do tempo, sequências são invariantes, há apenas um caminho para atingir objetivos, e há pouca folga possível em suprimentos e equipamentos.

Ver também: Acoplamento Frouxo; Complexidade Interativa; Acidente Normal.

Fonte: Perrow, 1984, 1999.

Acoplamento Frouxo (*Loose Coupling*)

Característica de sistemas onde processos são relativamente independentes, com folgas e

amortecimentos que permitem absorver perturbações sem propagação rápida de falhas. Sistemas com acoplamento frouxo permitem maior flexibilidade e improvisação.
Ver também: Acoplamento Estreito; Capacidade de Amortecimento.
Fonte: Perrow, 1984.

Adaptabilidade Sustentada (*Sustained Adaptability*)

Um dos quatro modelos de resiliência de Woods: capacidade de um sistema de manter sua adaptabilidade ao longo do tempo, evitando a exaustão de suas capacidades adaptativas.
Ver também: Extensibilidade Graciosa; Capacidade Adaptativa; Engenharia de Resiliência.
Fonte: Woods, 2015.

ALARP (*As Low As Reasonably Practicable*)

Princípio que estabelece que riscos devem ser reduzidos ao nível tão baixo quanto razoavelmente praticável, considerando o equilíbrio entre custos e benefícios das medidas de redução de risco. Estrutura-se em três zonas de tolerabilidade: (1) **intolerável** – risco acima do limite superior, que deve ser reduzido independentemente do custo; (2) **tolerável ou ALARP** – risco entre os limites superior e inferior, que deve ser reduzido até o ponto em que o custo adicional de redução seja desproporcionalmente alto em relação ao benefício obtido em segurança; (3) **aceitável** – risco abaixo do limite inferior, sem necessidade de ações adicionais. Na indústria offshore, os limites tipicamente adotados são 10^{-3} e 10^{-5} fatalidades por pessoa exposta por ano. O critério ALARP não é estático: o risco residual deve ser reavaliado sempre que barreiras se degradam, modificações são realizadas ou novos dados de frequência alteram as premissas da análise.
Ver também: Risco Residual; LOPA; PFD; HSE Case.
Fontes: HSE UK; ISO 17776, 2016; IOGP 544, 2016.

Análise de Confiabilidade Humana (HRA – *Human Reliability Analysis*)

Abordagem sistemática para identificar e quantificar a contribuição humana para o risco em sistemas complexos. Busca responder: quais erros humanos são possíveis? Qual sua probabilidade? Quais fatores influenciam essa probabilidade? Como podem ser prevenidos ou mitigados? Ver seção 3.4.
Ver também: HEP; PSF; PetroHRA; SPAR-H; CREAM; THERP; HEART; Tarefa Crítica de Segurança Operacional.
Fontes: Kirwan, 1994; Energy Institute, 2020; NT 10/2023 ANP.

Análise Hierárquica de Tarefas (HTA – *Hierarchical Task Analysis*)

Método estruturado para decompor tarefas complexas em subtarefas e operações elementares, representadas em formato hierárquico (diagrama em árvore). Utilizado como base para análise de confiabilidade humana e identificação de tarefas críticas.

Fontes: Øie & Fernander, 2022; IFE

Antítese (Princípio de)

Princípio orientador segundo o qual a formalização de novos princípios em uma organização é frequentemente motivada pelo reconhecimento de que sua antítese prevalece na prática. Se uma empresa precisa declarar formalmente que "errar é humano e sistêmico", é porque, no cotidiano, erros continuam sendo tratados como falhas individuais. Tem implicação direta para a leitura crítica de programas de cultura, segurança psicológica e Cultura Justa: o anúncio formal não substitui o reconhecimento honesto do estado atual – verdadeiro ponto de partida da transformação.

Ver também: Coerência entre o Dizer e o Fazer; Movimentos da Jornada; Princípios de Fatores Humanos (PFH).

Fonte: Henriqson, 2023.

APOA (*Analysis of Pre-Accident Operator Actions*)

Método qualitativo de análise de confiabilidade humana desenvolvido para capturar e reduzir riscos associados a erros pré-iniciadores e iniciadores, que geralmente ocorrem no lado esquerdo do diagrama Bow-tie. Foca em operações críticas onde erros podem desencadear eventos ou degradar barreiras.

Fonte: Øie & Fernander, 2022; IFE

Aprendizagem Operacional (*Operational Learning*)

Aprendizagem gerada a partir das operações cotidianas e dos sucessos, e não apenas das falhas. Parte do reconhecimento de que compreender como o trabalho normalmente dá certo é tão importante quanto analisar quando dá errado. Para isso, recorre a ferramentas como *Learning Teams* e investigações pré-acidente para identificar oportunidades de melhoria de forma proativa (Conklin, 2019; Hollnagel, 2014). Alinha-se à abordagem "*Aprendendo com o Trabalho Normal*" (*Learning from Normal Work*), consolidada pelo IOGP 642 (2022) e incorporada às diretrizes de desempenho humano do IOGP 810 (2026). Na abordagem baseada na prática (*practice-based approach*), a aprendizagem operacional vai além da extração de lições aprendidas. O conhecimento operacional não é uma posse cognitiva

a ser armazenada, mas o saber na prática (*knowing-in-practice*): uma competência coletiva que vive nas adaptações situadas, na expertise incorporada e nos ajustes contínuos que praticantes realizam para criar segurança face às demandas reais do trabalho (Gherardi, 2006, 2012; Gherardi & Nicolini, 2002). No plano organizacional, é uma das fontes que alimentam a Aprendizagem Organizacional, fornecendo o saber situado que a organização precisa traduzir e não apenas registrar, para transformar suas práticas e evoluir.

Ver também: Aprendizagem Organizacional; Safety-II; Lacuna WAI-WAD; Learning Teams; Movimentos da Jornada; Racionalidade Local.

Fontes: Conklin, 2019; Gherardi, 2006, 2012; Gherardi & Nicolini, 2002b; Hollnagel, 2014; IOGP 810, 2026.

Aprendizagem Organizacional (*Organizational Learning*)

Processo pelo qual a experiência, de falhas e de sucessos, se converte em mudança efetiva nas práticas, estruturas e entendimentos compartilhados de uma organização. Distingue-se do simples acúmulo de relatórios de incidentes por exigir mudança efetiva na forma como a organização trabalha. Requer condições estruturais (canais de reporte, sistemas de análise, fóruns de discussão) e culturais (segurança psicológica, Cultura Justa, tempo dedicado) (Edmondson, 2019).

O conceito é lido por duas tradições complementares. Na **tradição cognitivo-reflexiva**, o conhecimento é tratado como posse cognitiva a ser adquirida, codificada, armazenada e transferida entre níveis organizacionais. Aprender é detectar e corrigir desvios, ou rever as premissas que os produzem, e institucionalizar conhecimento-como-conteúdo (Argyris & Schön, 1978; Senge, 1990). Na **abordagem baseada na prática**, a aprendizagem é a reprodução e a transformação contínuas das práticas organizacionais. Aprender não é adquirir informação, mas participar competentemente de práticas compartilhadas, articulando o saber situado em comunidades de prática (Gherardi, 2006, 2012; Gherardi & Nicolini, 2000a, 2002a).

A aprendizagem pode ser reativa, quando parte de eventos indesejados, ou proativa, quando estuda como o trabalho cotidiano produz sucesso e segurança. Organizações resilientes não tomam o sucesso passado como razão para confiança: continuam investindo em antecipar como o potencial de falha se transforma (Woods et al., 2010).

Ver também: Aprendizagem Operacional; Learning Teams; Distanciamento por Diferenças; Histórias Primárias e Secundárias; Segurança Psicológica; HRO.

Fontes: Argyris & Schön, 1978; Edmondson, 2019; Gherardi, 2006, 2012; Gherardi & Nicolini, 2000a, 2002a; Senge, 1990; Woods et al., 2010.

Armadilhas Analíticas (Reducionista, Moral, Normativa)

Três riscos na aplicação da Engenharia de Resiliência, sistematizados por Bergström e Dekker (2019) a partir da crítica seminal de Bergström, van Winsen e Henriqson (2015): **(1) Reducionista** - localizar as capacidades adaptativas exclusivamente na linha de frente (*sharp end*), esperando que a adaptação dos operadores garanta o funcionamento do sistema sem alterar as condições estruturais ("resiliência apesar do sistema", não "graças ao sistema"); **(2) Moral** - responsabilizar (*responsibilization*) os operadores por condições sistêmicas fora de seu controle, convertendo a resiliência em categoria de *accountability* moral do indivíduo *accountability downward* disfarçado de empoderamento; **(3) Normativa** - tratar a resiliência como propriedade sempre positiva, silenciando a questão perroviana sobre se certos riscos deveriam ser aceitos em primeiro lugar. Ver Seção 2.4.6.
Ver também: Engenharia de Resiliência; Capacidade Adaptativa; Extremidades Afiada e Cega; Visão Tradicional.
Fonte: Bergström, van Winsen & Henriqson, 2015; Bergström & Dekker, 2019..

Avaliação Crítica de Práticas

Processo deliberativo conduzido por estrutura de governança (Comitê de Fatores Humanos ou equivalente) para examinar criticamente práticas organizacionais existentes – procedimentos, controles, indicadores, formulários – quanto ao seu propósito original, valor operacional efetivo e coerência com princípios de Fatores Humanos declarados. Pode resultar em manutenção, ressignificação, simplificação ou descontinuação. Ataque direto ao acúmulo de *safety clutter*. Manifestação prática do Movimento I (Engajamento das Lideranças & Governança).
Ver também: Safety Clutter; Comitê de Fatores Humanos; Movimentos da Jornada.
Fontes: Rae, Weber & Dekker, 2018; Compêndio de Fatores Humanos, Parte IV, 2026

B

Barreira

Meio físico ou funcional que impede uma ação ou ocorrência indesejada, ou que protege contra as consequências de tais eventos (Hollnagel, 2004). Na gestão de Segurança de Processo, barreiras são interpostas entre fontes de energia perigosa e alvos vulneráveis. A taxonomia de Sklet (2006), amplamente adotada na indústria de óleo e gás, classifica barreiras em quatro tipos: (1) **Físicas passivas** – estruturas e dispositivos que atuam sem necessitar de ativação (diques de contenção, estruturas antifogo, válvulas de alívio); (2)

Ativas – sistemas que detectam condições anormais e intervêm automaticamente (sistemas de intertravamento, detecção e supressão de incêndio, SDI/ESD); (3) **Procedurais** – ações humanas especificadas em procedimentos, cuja eficácia depende de clareza procedimental, treinamento e condições de execução; (4) **Competência dos Guardiões** – requisitos de capacitação e certificação das pessoas responsáveis por operar e manter as barreiras. Barreiras raramente são elementos isolados; em geral constituem Conjuntos Solidários de Barreiras (CSB), nos quais a degradação de qualquer elemento compromete a funcionalidade do conjunto.

Ver também: Conjunto Solidário de Barreiras (CSB); Defesa em Profundidade; Guardião da Barreira; VECSO; PFD.

Fontes: Hollnagel, 2004; Sklet, 2006; IOGP 544, 2016; Reason, 1997.

Bow-tie

Método de análise e gestão de risco que representa graficamente as relações entre ameaças (causas), evento central (*top event* – perda de contenção do perigo), consequências e barreiras de prevenção e mitigação. A forma de "gravata borboleta" resulta da representação das barreiras nos dois lados do evento central: à esquerda, barreiras de prevenção que impedem o *top event*; à direita, barreiras de mitigação que limitam as consequências após o *top event*. O bow-tie conecta visualmente os cenários de *Major Accident Hazard* (MAH) às barreiras específicas que os controlam e às pessoas e sistemas responsáveis por mantê-las. Na sua forma dinâmica – atualizado em tempo real conforme o estado das barreiras muda – transforma-se de documento estático de análise em instrumento vivo de gerenciamento de risco. Alimenta a identificação dos Elementos Críticos de Segurança Operacional (ECSO) exigidos pela NT 10/2023 da ANP.

Ver também: LOPA; MAH; MAH Scenarios; Conjunto Solidário de Barreiras (CSB); HAZOP.

Fontes: IOGP 544, 2016; CCPS/Energy Institute, 2018.

C

Capacidade Adaptativa (*Adaptive Capacity*)

Prontidão ou potencial de um sistema sociotécnico para ajustar seu funcionamento – seus modelos, planos, processos e comportamentos – antes, durante ou após perturbações, variações, surpresas e oportunidades, mantendo operações seguras e efetivas. Não é atributo fixo: pode ser construída, sustentada, degradada e perdida, razão pela qual precisa ser monitorada (ver Seção 3.2.7). Conceito central da Engenharia de Resiliência.

Ver também: Engenharia de Resiliência; Potenciais da Resiliência; Adaptabilidade Sustentada; Extensibilidade Graciosa.
Fontes: Woods, 2006; Hollnagel et al., 2006.

Capacidade de Amortecimento (*Buffering Capacity*)

Propriedade de resiliência que se refere ao tamanho ou tipos de perturbações que o sistema pode absorver ou adaptar-se sem um colapso fundamental no desempenho.
Ver também: Capacidade Adaptativa; Engenharia de Resiliência; Acoplamento Frouxo.
Fonte: Woods et al., 2010.

Captura do Pesquisador

Limitação metodológica identificada por Perrow (1994), citado por Hopkins (2014), pela qual pesquisadores em estudos etnográficos prolongados de organizações de alto risco podem perder objetividade crítica, sendo "capturados" pelo impacto sensorial e simbólico das operações complexas. Cautela relevante para a tradição HRO, cujos achados originam-se de imersão de longo prazo em organizações como porta-aviões e centrais nucleares.
Ver também: HRO.
Fontes: Perrow, 1994; Hopkins, 2014.

Captura Punitiva do Sistema de *Accountability*

Fenômeno organizacional pelo qual investigações de acidentes – conduzidas por reguladores, comissões internas ou gestores – são percebidas por trabalhadores como processos orientados à identificação de culpados e à conformidade legal, e não à aprendizagem sistêmica. Esvazia mecanismos formais de Cultura Justa, mesmo quando estes existem em política. Está associado a silêncio organizacional, multiplicação de procedimentos sem ganho de segurança e recorrência de eventos. Discutido em detalhe na Seção 3.3.8.
Ver também: Cultura Justa; Accountability; Segunda Vítima; Justiça Retributiva.
Fontes: Catino, 2008; Parris, 2025.

Coerência entre o Dizer e o Fazer

Métrica qualitativa fundamental da jornada de Fatores Humanos: alinhamento entre os princípios declarados pela organização e suas práticas efetivas em investigação de acidentes, sistemas disciplinares, alocação de recursos e comunicação cotidiana. A construção de incoerência – declarar que "errar é normal" e investigar buscando culpados – gera desconfiança e silêncio organizacional, frequentemente mais danosos do que a ausência da declaração inicial. Atenção constante da estrutura de governança.

Ver também: Antítese (Princípio de); Cultura Justa; Movimentos da Jornada.
Fonte: Henriqson, 2023.

Colapso Abrupto (*Brittleness*)

Tendência de um sistema a falhar de forma abrupta, quando eventos e demandas o levam além dos seus limites de competência, em vez de se degradar ou se estender gradualmente. Opõe-se à extensibilidade graciosa. Sistemas podem ser confiáveis nas condições previstas e, ainda assim, frágeis diante do inesperado, razão pela qual confiabilidade e resiliência não se confundem. Ver Seções 2.4.3 e 3.2.7.
Ver também: Extensibilidade Graciosa; Descompensação; Robustez; Resiliência.
Fonte: Woods, 2015, 2018.

Comitê de Fatores Humanos

Estrutura de governança organizacional, específica ou atribuída a comitês estratégicos já constituídos, responsável por deliberar sobre a jornada de Fatores Humanos, incluindo: aprovação de revisões de práticas e políticas; acompanhamento de ações acordadas; priorização de investimentos; e monitoramento de progresso nos cinco movimentos.
Ver também: Movimentos da Jornada; Avaliação Crítica de Práticas; Princípios de Fatores Humanos (PFH).
Fonte: Compêndio de Fatores Humanos, Parte IV, 2026.

Complexidade Interativa (*Interactive Complexity*)

Característica de sistemas onde componentes interagem de maneiras não antecipadas pelos projetistas. Sistemas interativamente complexos apresentam: proximidade física de componentes, subsistemas interconectados, múltiplas funções de componentes, e informação indireta sobre o estado do sistema.
Ver também: Acidente Normal; Acoplamento Estreito.
Fonte: Perrow, 1984, 1999.

Compromisso com a Resiliência (*Commitment to Resilience*)

Um dos cinco processos de *mindful organizing*: capacidade de detectar, conter e recuperar de erros antes que causem danos. Processo de contenção que permite às organizações responder efetivamente quando eventos inesperados ocorrem.

Ver também: Mindful Organizing; Mindfulness Organizacional; HRO.
Fontes: Weick & Sutcliffe, 2007, 2015.

Conceptual Slack (Folga Conceitual)

Conceito desenvolvido por Schulman (1993) para descrever a presença, em uma organização, de múltiplas interpretações divergentes – não consensuais – sobre como o sistema funciona e quais riscos ele apresenta. Em vez de problema a eliminar, a folga conceitual é recurso de confiabilidade: a ausência de consenso impede a complacência de uma "visão dominante única" e mantém a organização atenta a sinais que seriam descartados por uma interpretação hegemônica. Característica das HROs.
Ver também: HRO; Relutância em Simplificar; Hero-embracing / Hero-avoiding.
Fonte: Schulman, 1993.

Condições de Contorno (*Boundary Conditions*)

Conjunto de restrições e recursos definidos fora da atividade, por contratos, regulamentos, orçamentos, metas, efetivo e decisões de projeto, dentro dos quais as equipes ajustam seu desempenho. Delimitam o espaço de trabalho descrito por Rasmussen, cujas fronteiras econômicas, de carga de trabalho e de desempenho aceitável orientam a migração das atividades. Por serem fixadas em um dado momento, tendem a envelhecer à medida que o ambiente operacional muda. Sem monitoramento, a diferença é absorvida pelos ajustes da linha de frente, deslocando o risco para a ponta. Em operações em rede, como na cadeia operadora - contratada - subcontratada, são estabelecidas em grande parte por contratos e pela regulação. Ver seções 2.3, 2.4.3 e 4.7.1.
Ver também: Fronteira de Desempenho Aceitável; Migração para os Limites; Gradiente de Pressão; Adaptabilidade Sustentada; Deriva para Falha.
Fontes: Rasmussen, 1997; Henriqueson, 2026.

Condição Latente (*Latent Condition*)

Condição preexistente no sistema que pode permanecer dormente por longos períodos e contribuir para acidentes quando combinada com falhas ativas e gatilhos locais. Resultado de decisões tomadas em níveis mais altos da organização (reguladores, designers, gestores).
Ver também: Modelo do Queijo Suíço; Falha Ativa; Extremidades Afiada e Cega.
Fontes: Reason, 1990, 1997.

Conjunto Solidário de Barreiras (CSB)

Conjunto integrado de elementos interdependentes – hardware, sistemas instrumenta-

dos, procedimentos e competências – que, atuando solidariamente, executam a função de uma barreira de segurança. O conceito reconhece que barreiras complexas raramente são compostas por um único elemento: a degradação ou perda de qualquer componente compromete a funcionalidade do conjunto como um todo, independentemente do estado dos demais. Cada CSB tipicamente desdobra-se em quatro categorias de elementos: (1) integridade de equipamentos e sistemas (hardware e instrumentação); (2) Tarefas Críticas de Segurança Operacional (TCSO) – ações humanas necessárias para que a barreira cumpra sua função; (3) Verificações de Elementos Críticos (VECSO) – inspeções e testes regulares que confirmam a prontidão das barreiras; e (4) competência dos guardiões – capacitação e certificação das pessoas responsáveis pelas barreiras. Em cenários de poço, os CSBs são representados como camadas independentes de proteção (IPLs) capazes de prevenir ou mitigar eventos de topo, com a distinção entre CSB primário (mais próximo do intervalo isolado, diretamente exposto à pressão da formação) e CSB secundário (exposto em caso de perda de integridade do primário). O conceito é particularmente operacionalizado em diretrizes setoriais brasileiras de projeto e construção de poços marítimos.

Ver também: Barreira; IPL; Guardião da Barreira; TCSO; VECSO; PFD; Risco Residual; Bow-tie.

Fontes: IBP, 2022 (diretrizes para projeto e construção de poços marítimos); NORSOK D-010, 2013; IOGP 544, 2016; NT 10/2023 ANP.

CREAM
(*Cognitive Reliability and Error Analysis Method*)

Método de Análise de Confiabilidade Humana (HRA) fundamentado no Modelo de Controle Contextual (Contextual Control Model COCOM), que trata o desempenho humano como função do modo de controle cognitivo adotado pelo operador diante das condições do contexto de trabalho, e não de uma taxonomia fixa de tipos de erro. Distingue quatro modos de controle estratégico, tático, oportunista e *scrambled* (caótico) cuja combinação com os Fatores Modeladores de Desempenho (PSF) determina a probabilidade de erro (HEP). Apresenta duas versões: a básica, retrospectiva e qualitativa, voltada à investigação de eventos já ocorridos; e a estendida, prospectiva e quantitativa, voltada à estimativa de probabilidades de erro em tarefas críticas ainda não realizadas. Reconhecido pela NT 10/2023 ANP como um dos métodos aceitos de HRA para a indústria de óleo e gás (Seção 3.4.4 deste compêndio).

Ver também: HRA; PSF; HEP; SPAR-H; THERP; HEART; PetroHRA.

Fonte: Hollnagel, 1998.

Cultura de Segurança (*Safety Culture*)

Padrão emergente de pressupostos, valores, atitudes, competências e comportamentos compartilhados pelo qual uma organização e seus grupos respondem aos desafios da segurança em seu contexto sociotécnico. Inclui os elementos de cultura justa, cultura de relato, cultura flexível e cultura de aprendizagem (Reason, 1997), expressando-se na qualidade dos fluxos autênticos de informação – particularmente nas condições para que más notícias circulem das frentes operacionais para os centros de decisão – e na confiança como moeda da liderança (Lloyd, 2020). É importante distinguir culturas de segurança construídas sobre conformidade – nas quais a segurança é gerida como cumprimento de regras e burocracia, frequentemente sustentadas por assimetrias de poder que blindam decisões estruturais do escrutínio crítico – daquelas baseadas em aprendizagem genuína, nas quais a segurança é tratada como valor crônico que infunde a prática cotidiana (Dekker, 2014). Culturas de conformidade tendem a produzir silêncio organizacional e acúmulo de safety clutter; culturas de aprendizagem investem continuamente em compreender como o trabalho realmente acontece (Safety-II). Ressalva conceitual e crítica: cultura é construto, não objeto físico, e propriedade emergente de grupos enquanto sistemas complexos – não pode ser "implantada" pela gestão (Busch, 2021). Toda definição e avaliação de cultura de segurança envolve relações de poder: define o que conta como "maduro", quem detém o critério e a quem se atribui responsabilidade pelos resultados – com risco permanente de responsibilization da linha de frente em nome da cultura (Silbey, 2009; Antonsen, 2009; Henriqson et al., 2014). A pergunta-guia que sustenta o uso responsável do termo é: quem se beneficia desta cultura e desta leitura?.

Ver também: Cultura Justa; Safety-II; Safety Clutter; Maturidade da Cultura; Poder Organizacional; Responsibilization; Princípios de Fatores Humanos (PFH).

Fontes: IAEA, 1991; Reason, 1997; Silbey, 2009; Antonsen, 2009; Dekker, 2014; Henriqson et al., 2014; Hollnagel, 2014; Lloyd, 2020; Busch, 2021.

Cultura Justa (*Just Culture*)

Paradigma e sistema organizacional que busca equilibrar a necessidade de aprender com erros e a de manter *accountability*, evitando tanto a cultura de culpa que inibe o relato - quanto a cultura sem culpa - que comprometeria a credibilidade e toleraria comportamentos deliberadamente inseguros (Reason, 1997; Dekker, 2017). Em sua formulação de referência, é a cultura na qual operadores de linha de frente não são punidos por ações, omissões ou decisões proporcionais à sua experiência e treinamento, mas na qual negligência grave, violações deliberadas e atos destrutivos não são tolerados (Pellegrino, 2019). Constitui o conjunto de regras, processos e disposições institucionais

que regulam as respostas a desvios e erros - **o sistema dentro do qual as práticas de *accountability* operam** (ver verbete) e do qual depende a aprendizagem organizacional. Estrutura-se em três dimensões de justiça (Dekker & Breakey, 2016): substantiva (legitimidade e equidade das próprias regras), **processual** (legitimidade dos processos que determinam violações, com garantias como julgamento por pares e direito a recurso) e **restaurativa** (reparação do dano e reintegração, em contraste com a lógica retributiva). Sua distinção operacional central opõe a vertente **retributiva** - organizada em torno de "*qual regra foi descumprida, quem o fez e qual sanção cabe*" à **restaurativa** organizada em torno de "*quem foi impactado, do que precisa e de quem é a obrigação de atender*" (Dekker, 2017; Dekker, Rafferty & Oates, 2022). Ressalva crítica: a própria consolidação legal e organizacional do conceito é objeto de crítica contemporânea, por poder deslocar a autoridade de "*traçar a linha*" para o aparato judicial-regulatório e por operar sobre assimetrias de poder entre quem categoriza e quem é categorizado (Bergström, 2019; Henriqson et al., 2014; cf. 3.3.9). Ver Seção 3.3.

Ver também: Accountability; Justiça Substantiva; Justiça Processual; Justiça Restaurativa; Justiça Retributiva; Captura Punitiva do Sistema de Accountability; Segunda Vítima; Teste de Substituição; Segurança Psicológica; Aprendizagem Organizacional.

Fontes: Reason, 1997; Pellegrino, 2019; Dekker & Breakey, 2016; Dekker, 2017; Dekker, Rafferty & Oates, 2022; Bergström, 2019; Henriqson et al., 2014.

D

Deferência à Expertise (*Deference to Expertise*)

Um dos cinco processos de *mindful organizing*: tomada de decisão direcionada para quem tem maior conhecimento sobre a situação, independentemente de posição hierárquica formal. Durante crises, decisões fluem para quem tem maior expertise.

Ver também: Mindful Organizing; HRO; Hero-embracing / Hero-avoiding.

Fontes: Weick & Sutcliffe, 2007, 2015.

Defesa em Profundidade (*Defense in Depth*)

Estratégia de segurança que emprega múltiplas camadas de proteção redundantes, de modo que a falha de uma não comprometa imediatamente as demais. A independência entre camadas é condição necessária para a validade do modelo. Na perspectiva Rasmusseniana, estas defesas tendem a degradar-se sistematicamente ao longo do tempo quando a pressão por custo-efetividade domina, pois a violação local de uma defesa não produz efeito imediato visível.

Ver também: Barreira; Conjunto Solidário de Barreiras (CSB); LOPA; Redundância.
Fontes: Reason, 1997; Rasmussen, 1997; IEC 61511, 2016.

Deriva para Falha (*Drift into Failure*)

Processo pelo qual sistemas sociotécnicos migram gradualmente em direção a falhas catastróficas através de pequenas decisões e adaptações que parecem individualmente razoáveis. Dekker (2011) sintetizou as perspectivas de Turner, Vaughan, Snook e Rasmussen identificando cinco características: escassez e competição, decrementalismo (cada passo parece marginal), sensibilidade a condições iniciais, tecnologia indócil (que resiste ao controle) e contribuição da estrutura protetiva (as próprias redundâncias podem obscurecer vulnerabilidades). Distingue-se de "acidente" por seu caráter processual e incremental – não há uma causa-raiz discreta, mas uma trajetória.
Ver também: Deriva Prática; Normalização do Desvio; Migração para os Limites; Incubação; Fine-Tuning; Desastre Fabricado.
Fonte: Dekker, 2011.

Deriva Prática (*Practical Drift*)

Processo pelo qual práticas localmente eficientes substituem gradualmente procedimentos formais através de um desacoplamento incremental não documentado. Diferente da normalização do desvio, permanece invisível para a liderança, emergindo como *workarounds* (adaptações/ajustes) locais que preenchem lacunas onde regras e procedimentos não alcançam a complexidade do trabalho real.
Ver também: Normalização do Desvio; Lacuna WAI-WAD; Deriva para Falha; Racionalidade Local.
Fonte: Snook, 2000.

Desastre Fabricado (*Man-Made Disaster*)

Conceito introduzido por Barry Turner em sua obra seminal de 1978, redigida após análise de 84 relatórios de inquéritos britânicos. Refere-se a desastres que emergem de processos sociotécnicos prolongados – não de acidentes súbitos –, marcados por períodos extensos de incubação durante os quais sinais de perigo se acumulam mas não são reconhecidos pelas crenças vigentes na organização. Fundamento histórico da tradição de Dependência de Trajetória.
Ver também: Incubação; Normalização do Desvio; Deriva Prática; Deriva para Falha; Segredo Estrutural.
Fontes: Turner, 1978; Turner & Pidgeon, 1997.

Desempenho Humano (*Human Performance* – HP)

Designa, a um só tempo, (i) o que as pessoas fazem e como fazem no trabalho a contribuição de indivíduos e equipes para os resultados do sistema e (ii) a abordagem aplicada, voltada à liderança e à operação, que mobiliza conceitos de Fatores Humanos e da ciência da segurança para qualificar essa contribuição. O Relatório IOGP 810 define a HP como a capacidade de indivíduos executarem tarefas com sucesso, eficiência e segurança, contribuindo para o desempenho global do sistema. O relatório organiza a abordagem em cinco princípios: (1) erro é normal; (2) culpa não resolve nada; (3) contexto dirige comportamento; (4) aprender é vital; (5) como os líderes respondem importa. Neste compêndio, HP é compreendido como objeto e expressão aplicada de Fatores Humanos: seu escopo se inscreve no campo, que estuda os fatores do trabalho, indivíduos e organizações que influenciam o desempenho. Tem como variantes o HOP (*Human and Organizational Performance*), associado a Todd Conklin, e o HPI (*Human Performance Improvement*), originado no setor nuclear. Ver Seção 1.2.6. (A relação entre Fatores Humanos e Desempenho Humano).

Ver também: Fatores Humanos; HOP; Engenharia de Fatores Humanos (HFE); Nova Visão; Cultura Justa; Aprendizagem Operacional.

Fontes: Shorrock, 2019; DOE, 2009; Conklin, 2019; IOGP 810, 2026.

Distanciamento por Diferenças (*Distancing through Differencing*)

Mecanismo cognitivo e organizacional pelo qual uma organização rejeita a relevância de lições de acidentes ocorridos em outras organizações, apontando diferenças (de setor, contexto, tecnologia, escala) que justificariam "isso não pode acontecer aqui". Identificado por Woods e colegas como um dos principais obstáculos à aprendizagem interorganizacional. Particularmente relevante na indústria de óleo e gás, onde lições de Texas City, Macondo e outros desastres correm o risco de ser localizadas em vez de generalizadas.

Ver também: Aprendizagem Organizacional; Histórias Primárias e Secundárias.

Fonte: Woods et al., 2010.

E

Ecossistema de Fatores Humanos

Metáfora integradora que representa as disciplinas e abordagens do campo de Fatores Humanos como um sistema dinâmico, interdependente e em constante adaptação. Assim como em ecossistema biológico, cada disciplina é um "bioma" que se conecta aos demais por raízes conceituais e práticas. "Eco" representa características distintivas de cada disciplina; "system" representa suas convergências e sobreposições. Ver seção 3.1.

Ver também: Zonas de Contato.

Fonte: França, 2024.

Efetivo Mínimo

Quantidade mínima necessária de mão de obra para operar uma instalação com segurança. Calculado considerando análise temporal de tarefas contidas nos procedimentos críticos operacionais e no plano de resposta a emergência. O maior entre os valores calculados para operações normais e para o Plano de Resposta a Emergência deve ser adotado.

Ver também: Procedimento Crítico; Tarefa Crítica de Segurança Operacional.

Fontes: NT 10/2023 ANP; Guia IADC Brasil, 2025.

Elemento Crítico de Segurança Operacional (ECSO)

Elemento essencial para prevenção ou mitigação de acidente operacional associado a grandes emergências, ou que em caso de falha, falta ou degradação possa provocar tal acidente. Inclui três categorias: equipamentos críticos, sistemas críticos e procedimentos críticos.

Ver também: Equipamento Crítico; Sistema Crítico; Procedimento Crítico; VECSO; Guardião da Barreira.

Fonte: NT 10/2023 ANP.

Engenharia de Fatores Humanos (HFE – *Human Factors Engineering*)

Disciplina aplicada que integra conhecimentos sobre capacidades e limitações humanas no design de sistemas, equipamentos, interfaces e ambientes de trabalho. Visa otimizar o desempenho humano e reduzir erros através de design centrado no usuário. Ver seção 3.5.

Ver também: Interface Humano-Máquina (IHM); Erro Humano.

Fontes: IOGP 454, 2020; Lee et al., 201.

Engenharia de Resiliência

(*Resilience Engineering*)

Abordagem que estuda o projeto, o desempenho e a gestão de sistemas sociotécnicos diante de incertezas, variabilidades e riscos residuais. Conceba a segurança como capacidade de ter sucesso sob condições variadas, esperadas e inesperadas (Safety-II), e não apenas como ausência de falhas. Sua unidade de análise é sempre o sistema sociotécnico, nunca o indivíduo, o equipamento ou o procedimento isolado. "Resiliência" designa a capacidade adaptativa desse sistema, expressa nos quatro potenciais: responder, monitorar, antecipar e aprender. "Engenharia" não indica uma nova disciplina técnica, mas uma dimensão de projeto e gestão das condições que sustentam essas adaptações, da linha de frente às decisões organizacionais e regulatórias. Complementa, e não substitui, a confiabilidade e a robustez. Ver Seção 2.4.

Ver também: Segurança-II; Potenciais da Resiliência; FRAM; RAG; Princípio ETTO; Variabilidade de Desempenho; Armadilhas Analíticas (Reducionista, Moral, Normativa).

Fonte: Hollnagel, Woods & Leveson, 2006; Bergström, van Winsen & Henriqson, 2015.

Equipamento Crítico

Qualquer equipamento, componente ou elemento estrutural da instalação essencial para prevenção ou mitigação de acidente operacional, ou que em caso de falha possa provocar acidente associado a grandes emergências.

Ver também: ECSO; Sistema Crítico; Procedimento Crítico.

Fonte: NT 10/2023 ANP.

EERA
(*Escape, Evacuation and Rescue Analysis*)

Análise de fuga, evacuação e resgate. Estudo de risco estruturado que avalia, em cenários de emergência (incêndio, explosão, abandono), a adequação das rotas de fuga, dos meios de evacuação e dos mecanismos de resgate disponíveis em uma instalação – particularmente em unidades offshore, onde a evacuação tem desafios específicos relacionados ao isolamento geográfico, condições marítimas e capacidade limitada de embarcações e helicópteros de resgate. O EERA dimensiona tempos de escape, capacidade das rotas, redundância de meios e tempos de resposta de organizações externas. Em conjunto com FERA e QRA, integra o pacote analítico padrão para a elaboração do HSE Case de instalações offshore (ISO 17776, 2016; IADC, 2015).

Ver também FERA; QRA; HSE Case; MAH; ISO 17776.

Fontes: ISO 17776, 2016; IADC, 2015; IOGP 544, 2016.

Erro Humano (*Human Error*)

Na Visão Tradicional: causa primária de acidentes, problema a ser controlado. Na Nova Visão: sintoma de condições sistêmicas mais profundas, ponto de partida para investigação (não ponto de chegada). O rótulo "erro humano" é um julgamento feito em retrospectiva, não uma explicação. Na perspectiva Rasmusseniana, a ação humana opera em zona de variabilidade onde a tentativa adaptativa frente à incerteza é constitutiva – o que retrospectivamente é classificado como "erro" é, no momento da decisão, parte do espaço normal de atuação sob restrições.

Ver também: Visão Tradicional; Nova Visão; Racionalidade Local; Viés de Retrospectiva; Teste de Substituição.

Fontes: Reason, 1990; Dekker, 2014; Rasmussen, 1997.

Extensibilidade Graciosa (*Graceful Extensibility*)

Um dos quatro modelos de resiliência de Woods: capacidade de um sistema de estender seu desempenho além do envelope de design quando surpresas ocorrem. A pergunta central é "como sistemas se esticam (adaptam) para lidar com surpresas?". Seu oposto é o colapso abrupto (brittleness). A teoria da extensibilidade graciosa descreve como a capacidade adaptativa é construída, sustentada, degradada e perdida em sistemas complexos.

Ver também: Adaptabilidade Sustentada; Capacidade Adaptativa; Engenharia de Resiliência; colapso abrupto.

Fontes: Woods, 2015, 2018.

Extremidades Afiada e Cega (*Sharp End / Blunt End*)

Distinção proposta por Reason e desenvolvida por Woods et al. para localizar os diferentes níveis nos quais decisões e ações contribuem para a segurança ou para acidentes. A *extremidade afiada* (*sharp end*) refere-se aos operadores em contato direto com o processo – onde as ações finais ocorrem; a *extremidade cega* (*blunt end*) refere-se aos níveis organizacionais distantes do processo – gestores, projetistas, reguladores – que criam as condições, recursos e pressões sob as quais os operadores na *sharp end* atuam. Acidentes raramente são causados pela *sharp end* isoladamente; refletem decisões e condições da *blunt end*.

Ver também: Condição Latente; Falha Ativa; Modelo do Queijo Suíço; Migração para os Limites; Gradiente de Pressão; Armadilhas Analíticas.

Fontes: Reason, 1997; Woods et al., 2010.

F

Falácia do Indicador Ocupacional (Falácia LTI/TRI)

Uso indevido de indicadores de segurança pessoal (ocupacional) – Lost Time Injury (LTI) e Total Recordable Injury / Total Recordable Injury Rate (TRI/TRIR) – como proxy (indicador indireto) do estado das barreiras de Segurança de Processos. Empiricamente demonstrada por Hopkins (2008, 2012) nos casos da refinaria de Texas City (BP, 2005) e do blowout de Macondo (Deepwater Horizon, 2010), nos quais indicadores ocupacionais aparentemente excelentes – celebrados internamente como evidência de maturidade em segurança – coexistiam com erosão progressiva das defesas de processo que conduziu aos acidentes catastróficos. Decorre de uma confusão categorial: indicadores ocupacionais medem a frequência de eventos pessoais frequentes e de baixa severidade (quedas, cortes, esforços), enquanto a integridade das barreiras de processo se refere a eventos raros e de alta severidade (perdas de contenção, explosões, blowouts), cuja dinâmica não está estatisticamente correlacionada à dos primeiros. Sustenta a necessidade de indicadores específicos de Segurança de Processos, organizados em frameworks dedicados (API RP 754). A falácia manifesta-se em duas dimensões: (i) entre eixos – indicadores de frequência pessoais não predizem o estado das barreiras de Segurança de Processo (Hopkins, 2008, 2012); e (ii) dentro do próprio eixo pessoal – a queda do TRIR/LTIR não implica redução de fatalidades e lesões graves (SIF), como evidenciam as séries da IOGP e do BLS, o que motiva a adoção dos indicadores SIFR e PSIFR (Hallowell et al., 2021; IOGP, 2025).

Ver também: Segurança de Processos; SIF e Potencial SIF; SIFR e PSIFR; Indicadores Antecipadores; Indicadores Reativos; MAH.

Fontes: Hopkins, 2008, 2012; CSB, 2007 (Texas City); BOEMRE/CG, 2011 (Macondo); API RP 754, 2021; IOGP, 2025; Rosness et al., 2010.

Falha Ativa (*Active Failure*)

Erros ou violações cometidos pelos operadores na *extremidade afiada* do sistema, cujas consequências são imediatamente visíveis. Diferenciam-se das condições latentes por sua proximidade temporal e causal com o evento adverso.

Ver também: Condição Latente; Extremidades Afiada e Cega; Modelo do Queijo Suíço.

Fontes: Reason, 1990, 1997.

Fatores Humanos (*Human Factors*)

Campo de conhecimento científico interdisciplinar que, a partir de uma perspectiva sistêmica, estuda a influência mútua entre os seres humanos e o sistema de trabalho do

qual fazem parte – em suas dimensões organizacionais, tecnológicas, ambientais e individuais, entre outras –, compreendendo tanto como esse sistema depende da contribuição humana para operar quanto como condiciona o desempenho de quem nele atua (com base em Henriqson, 2026). Reconhece que os resultados do trabalho emergem dessa interação e não da atuação isolada de indivíduos ou componentes do sistema – e tem por propósito compreender essas relações e intervir sobre as condições que as moldam, sobretudo por meio do projeto do trabalho, visando otimizar, de forma integrada, a segurança, o bem-estar humano e o desempenho dos sistemas sociotécnicos complexos. Equivalente a Ergonomia na definição da IEA (2000), combina contribuições de psicologia, fisiologia, engenharia, design, sociologia organizacional e ciências cognitivas, entre outras. Grafado com iniciais maiúsculas, sem artigo e com verbo no singular, o termo designa o campo; com artigo, em minúsculas e no plural – *os fatores humanos,* designa os fatores que influenciam o comportamento no trabalho, acepção adotada na NT n.° 10/2023 da ANP. Ver Seção 1.1.1, incluindo a definição adotada, as definições normativas e a Nota terminológica.

Ver também: Desempenho Humano (HP); Ecossistema de Fatores Humanos; Engenharia de Fatores Humanos (HFE); Sistema Sociotécnico; Princípios de Fatores Humanos (PFH).

Fontes: IEA, 2000; Henriqson, 2026; NT 10/2023 ANP; CCPS, 2019; HSE, 1999; Shorrock, 2017d, 2019b; IOGP 454, 2020; IOGP 810, 2026.

Fatores Humanos como Jornada de Aprendizagem Organizacional

Conceito que enquadra a implementação de Fatores Humanos não como projeto pontual ou conjunto de ferramentas, mas como processo contínuo de transformação organizacional – experimentação, descoberta, desconstrução e construção de conhecimento de forma iterativa e participativa, envolvendo lideranças, força de trabalho própria e terceirizada, parceiros e demais públicos de interesse.

Ver também: Movimentos da Jornada; Princípios de Fatores Humanos (PFH); Laboratórios de Fatores Humanos.

Fontes: Bruno, 2020; Almeida, Bruno & Capaverde, 2025.

Fatores Modeladores de Desempenho (PSF – *Performance Shaping Factors*)

Fatores contextuais que influenciam a probabilidade de erro humano em uma tarefa. Incluem complexidade da tarefa, tempo disponível, qualidade dos procedimentos, treinamento, fadiga, estresse, ergonomia da interface, ambiente físico e suporte organizacional.

São o mecanismo pelo qual métodos de HRA (PetroHRA, SPAR-H, CREAM) ajustam a HEP base para refletir o contexto específico.
Ver também: HRA; HEP; PetroHRA; SPAR-H; CREAM.
Fontes: Kirwan, 1994; IFE, 2022.

Fenômeno do Engodo (*Decoy Phenomenon*)

Mecanismo cognitivo descrito por Turner (1978) no qual a organização concentra atenção em um perigo familiar (o "engodo") enquanto perigos genuínos, frequentemente novos ou menos visíveis, incubam-se sem reconhecimento. Componente característico do período de incubação que precede desastres.
Ver também: Incubação; Desastre Fabricado; Relutância em Simplificar.
Fontes: Turner, 1978; Turner & Pidgeon, 1997.

FERA (*Fire and Explosion Risk Analysis*)

Análise de risco de incêndio e explosão. Estudo quantitativo dos riscos decorrentes de cenários de liberação de hidrocarbonetos com potencial de ignição, dimensionando dispersão de gases, radiação térmica, sobrepressões e impacto em estruturas, áreas habitadas e barreiras de segurança. O FERA fornece base técnica para a definição de distâncias seguras, dimensionamento de sistemas de proteção (parede contra fogo, sistemas de detecção e supressão, evacuação) e planejamento de resposta a emergências. Conduzido tipicamente em conjunto com EERA e QRA, integra o pacote analítico de avaliação de *Major Accident Hazards* (MAH) em instalações de óleo e gás.
Ver também: EERA; QRA; FMEA/FMECA; HSE Case; MAH; Segurança de Processo.
Fontes: ISO 17776, 2016; CCPS, 2007; Lees, 2012.

Fine-Tuning

Mecanismo identificado por Starbuck e Milliken (1988) pelo qual organizações realizam ajustes incrementais bem-sucedidos que progressivamente reduzem margens de segurança. Cada ajuste é localmente justificável; o efeito cumulativo é a erosão das defesas. O sucesso passado retroalimenta o processo: cada operação bem-sucedida reforça a crença de que o sistema é confiável, justificando novos ajustes. O caso Challenger ilustra o fenômeno: ao longo de 24 lançamentos bem-sucedidos, ajustes sucessivos nas avaliações de risco dos O-rings produziram condições que jamais teriam sido aceitas no primeiro lançamento.
Ver também: Normalização do Desvio; Incubação; Deriva para Falha; Migração para os Limites.
Fonte: Starbuck & Milliken, 1988.

FMEA / FMECA (*Failure Mode and Effects Analysis / Criticality Analysis*)

Técnica sistemática de análise de modos de falha. O FMEA (Failure Mode and Effects Analysis) examina, para cada componente ou subsistema, quais são os modos pelos quais ele pode falhar, quais os efeitos dessas falhas no sistema como um todo e quais as causas e mecanismos subjacentes. A extensão FMECA (Criticality Analysis) acrescenta uma análise quantitativa ou semiquantitativa da criticidade de cada modo de falha, considerando probabilidade de ocorrência, severidade das consequências e detectabilidade. Aplicado tipicamente a equipamentos e sistemas críticos, o FMEA/FMECA alimenta a priorização de inspeções, manutenções preventivas e o dimensionamento de redundâncias. Diferentemente do HAZOP – que examina desvios de parâmetros de processo –, o FMEA centra-se em modos de falha de componentes individuais; as duas técnicas são complementares no portfólio de análise de risco.

Ver também: HAZOP; HAZID; LOPA; QRA; Equipamento Crítico; Sistema Crítico.

Fontes: Lees, 2012; CCPS, 2007; IEC 60812.

FRAM (*Functional Resonance Analysis Method*)

Metodologia para modelar sistemas sociotécnicos complexos em termos de funções e suas variabilidades, em contraste com métodos tradicionais que buscam causas de falhas. Modela como funções interagem e como suas variabilidades podem se combinar – "ressonar" – para produzir tanto resultados desejados quanto indesejados. Pode ser empregado retrospectivamente, para compreender como um evento ocorreu, ou prospectivamente, para antecipar como variabilidades podem se combinar. Ver seção 2.4.

Ver também: Ressonância Funcional; Variabilidade de Desempenho; Princípio ETTO; Engenharia de Resiliência; RAG.

Fonte: Hollnagel, 2012.

Fronteira de Desempenho Aceitável

Conceito central da perspectiva Rasmusseniana: cada atividade em um sistema sociotécnico opera dentro de um envelope de desempenho aceitável, delimitado por três fronteiras – econômica, de carga de trabalho aceitável e de desempenho aceitável (segurança). Pressões de eficiência e menor esforço empurram continuamente a atividade em direção à fronteira de segurança; sem mecanismos contrários (incluindo Fatores Humanos), o sistema migra para os limites.

Ver também: Migração para os Limites; Gradiente de Pressão; AcciMap.

Fonte: Rasmussen, 1997.

G

Gestão de Mudança (MOC – *Management of Change*)

Processo sistemático para assegurar que modificações em equipamentos, sistemas, procedimentos, operações ou condições de trabalho sejam adequadamente analisadas, aprovadas e implementadas sem introduzir novos riscos não controlados. A MOC é um dos elementos mais críticos na prevenção de acidentes de processo: investigações de desastres como Flixborough (1974), Texas City (2005) e inúmeros outros revelaram modificações implementadas sem análise adequada de segurança como fator contribuinte central. Na prática de Segurança de Processo, toda modificação significativa deve passar por análise de risco – tipicamente incluindo HAZOP de modificação – antes de ser implementada. A NT 10/2023 da ANP e a Resolução 43/2007 (SGSO) estabelecem requisitos específicos para processos de MOC em instalações de óleo e gás.

Ver também: HAZOP; Segurança de Processo.

Fontes: CCPS, 2007; Hopkins, 2008; NT 10/2023 ANP.

Gradiente de Pressão

Pressões sistêmicas que empurram atividades em direção às fronteiras de segurança. Incluem o gradiente em direção ao menor esforço (tendência individual) e o gradiente em direção à maior eficiência/menor custo (pressão gerencial). Analogamente a gradientes termodinâmicos que dirigem o fluxo de calor.

Ver também: Migração para os Limites; Fronteira de Desempenho Aceitável; AcciMap; Extremidades Afiada e Cega.

Fonte: Rasmussen, 1997.

Guardião da Barreira

Indivíduo ou função organizacional formalmente responsável pela manutenção, verificação e operação de um conjunto específico de elementos de barreira de segurança, assegurando que estes se encontrem prontos para cumprir sua função quando demandados. O conceito de guardião é central nos sistemas de gerenciamento dinâmico de barreiras: cada elemento de um Conjunto Solidário de Barreiras (CSB) deve ter um guardião identificado, com competência verificada e treinamento vigente. A competência do guardião é um dos quatro elementos constitutivos de um CSB – sua degradação (por treinamento vencido, ausência, substituição sem capacitação adequada) torna o CSB incompleto, elevando o risco residual do cenário associado.

Ver também: Conjunto Solidário de Barreiras (CSB); VECSO; Barreira; Risco Residual.
Fontes: IOGP 544, 2016; NT 10/2023 ANP; Guia IADC Brasil, 2025.

H

HAZID (*Hazard Identification*)

Técnica qualitativa e estruturada de identificação de perigos, conduzida por equipe multidisciplinar em reuniões facilitadas. Diferentemente do HAZOP – que examina desvios de parâmetros de processo sobre P&IDs já projetados –, o HAZID opera em granularidade mais ampla: divide a instalação em atividades ou áreas e revisa sistematicamente cada uma para identificar perigos, cenários acidentais, causas, consequências e salvaguardas existentes. Emprega classificação em duas etapas – risco inicial (sem barreiras) e risco residual (com barreiras existentes) –, e cenários classificados como principais no risco residual são tipicamente promovidos a Major Accident Hazards (MAHs) da unidade. Em instalações offshore, particularmente em unidades móveis de perfuração (MODUs), o HAZID ancorado no Anexo F da ISO 17776:2016 constitui a técnica de referência para identificação de MAHs e elaboração do HSE Case, alimentando o eixo metodológico HAZID → Bow-tie → HSE Case adotado por drilling contractors.
Ver também: Bow-tie; HAZOP; MAH; HSE Case; ECSO; TCSO; HRA; LOPA.
Fontes: ISO 17776, 2016 (Anexo F); IADC, 2015; IOGP 544, 2016; NT 10/2023 ANP.

HAZOP (*Hazard and Operability Study*)

Técnica estruturada de identificação de perigos e análise de operabilidade, desenvolvida na ICI (Imperial Chemical Industries, Reino Unido) no início dos anos 1960 (Lawley, 1974) e amplamente disseminada por Trevor Kletz e colaboradores. Examina sistematicamente como desvios das condições de projeto pretendidas podem gerar situações perigosas ou falhas operacionais. Conduzido por equipe multidisciplinar, o HAZOP analisa cada trecho do sistema (*node*) aplicando palavras-guia (*guide words*) — Nenhum/Não, Mais, Menos, Bem como, Parte de, Reverso, Outro que — a parâmetros de processo (vazão, pressão, temperatura, nível, composição), identificando causas, consequências, salvaguardas e recomendações de melhoria. Os resultados alimentam a construção de bow-ties, a identificação de Elementos Críticos de Segurança Operacional (ECSO) e o HSE Case. Em unidades móveis de perfuração (MODUs), é tipicamente aplicado na fase de projeto, sendo o HAZID a técnica primária ao longo da operação. Deve ser revisado periodicamente (tipicamente quinquenal) e a cada modificação significativa (integrado ao MOC).

Ver também: HAZID; Human HAZOP; Bow-tie; LOPA; MAH; Gestão de Mudança (MOC); HSE Case.
Fontes: Lawley, 1974; Kletz, 2006; IEC 61882, 2016; CCPS, 2008; NT 10/2023 ANP.

HEART (*Human Error Assessment and Reduction Technique*)

Método de Análise de Confiabilidade Humana (HRA) baseado em Fatores de Condição de Erro (Error Producing Conditions EPCs). Parte de uma probabilidade nominal de erro humano associada ao tipo geral de tarefa e a ajusta multiplicativamente conforme a presença e a intensidade de condições que degradam o desempenho por exemplo, inexperiência do operador, tempo insuficiente para a ação, ambiguidade de informação ou incompatibilidade de interface. Reconhecido por sua simplicidade de aplicação e transparência de cálculo em relação a métodos mais complexos, ainda que a atribuição dos EPCs e de seus pesos dependa fortemente do julgamento do analista. Sua versão estendida, HEART+, refina a ponderação desses fatores para reduzir a variabilidade entre analistas. Reconhecido pela NT 10/2023 ANP como um dos métodos aceitos de HRA para a indústria de óleo e gás (Seção 3.4.4 deste compêndio).
Ver também: HRA; PSF; HEP; SPAR-H; CREAM; THERP.
Fontes: Williams, 1986.

Hero-embracing / Hero-avoiding

Tipologia organizacional proposta por Schulman para distinguir dois padrões de relação com expertise e responsabilidade individual. Organizações *hero-embracing* constroem narrativas em torno de indivíduos excepcionais que "salvam o dia"; organizações *hero-avoiding* institucionalizam a expertise em equipes, procedimentos e estruturas, evitando que o desempenho dependa de heroísmo individual. HROs tendem ao segundo padrão. Implicação para jornadas de Fatores Humanos: a transformação personalizada (dependente de "campeões" carismáticos) é frágil; a transformação institucionalizada é sustentável.
Ver também: HRO; Antítese (Princípio de); Conceptual Slack.
Fontes: Schulman, 1993, 1996.

Histórias Primárias e Secundárias (*First Stories / Second Stories*)

Distinção proposta por Woods e colegas. **Histórias primárias** são relatos simplificados de acidentes, enviesados pelo conhecimento do resultado, que atribuem a causa a fatores proximais (geralmente "erro humano"). Aparecem na imprensa e dirigem reações públi-

cas, legais e regulatórias. **Histórias secundárias** revelam múltiplos contribuintes sistêmicos que criaram condições para os erros, permitindo ver como o sistema se move em direção a acidentes – através destas percepções mais profundas, a aprendizagem ocorre e o processo de melhoria começa.
Ver também: Viés de Retrospectiva; Racionalidade Local; Raciocínio Contrafactual; Erro Humano.
Fonte: Woods et al., 2010.

HOP (*Human and Organizational Performance*)

Traduzido como **Desempenho Humano e Organizacional,** HOP é uma abordagem prática que traduz conceitos da Nova Visão para aplicação operacional, fundamentada em cinco princípios: (1) erro é normal e esperado; (2) culpa não resolve nada; (3) contexto dirige comportamento; (4) aprender é vital; (5) como respondemos às falhas importa. Ferramentas principais: Learning Teams, Aprendizagem Operacional e investigações pré-acidente. Integra insights de múltiplas perspectivas teóricas em framework aplicável.
Ver também: Desempenho Humano; Nova Visão; Safety Differently; Learning Teams; Princípios de Fatores Humanos (PFH); Cultura Justa.
Fontes: Conklin, 2012, 2019.

HRO (*High Reliability Organization*)

Traduzido como **organização de alta confiabilidade.** Organização que opera tecnologias de alto risco com potencial catastrófico, mas que mantém registros extraordinários de segurança durante longos períodos. Caracteriza-se por *mindful organizing*, redundância técnica e social, deferência à expertise e cultura de confiabilidade. Estudadas empiricamente pelo grupo de Berkeley (La Porte, Roberts, Rochlin) em porta-aviões, controle de tráfego aéreo e redes elétricas. Ver seção 2.2.
Ver também: Mindful Organizing; Mindfulness Organizacional; Preocupação com Falhas; Relutância em Simplificar; Sensibilidade às Operações; Compromisso com a Resiliência; Deferência à Expertise; Redundância; Conceptual Slack; Process Auditing; Hero-embracing / Hero-avoiding; Captura do Pesquisador.
Fontes: Roberts, 1990; Rochlin et al., 1987; Weick & Sutcliffe, 2007, 2015.

HSE Case (*Safety Case*)

Documento de segurança desenvolvido especificamente para cada instalação que demonstra, de forma integrada, como os riscos associados às suas operações são identificados, avaliados e controlados a um nível ALARP. Reúne evidências de engenharia, análises de risco (incluindo resultados de HAZOP, HAZID, FERA, QRA), descrição de sistemas

de gestão, planos de resposta a emergências e demonstração de que as barreiras críticas são mantidas em conformidade com padrões de desempenho rigorosos. O conceito originou-se no Reino Unido após o desastre de Piper Alpha (1988), quando a investigação de Lord Cullen concluiu que o regime regulatório prescritivo então vigente era insuficiente para garantir a segurança de instalações complexas. O HSE Case não é documento estático – deve refletir continuamente o estado atual da instalação, sendo atualizado a cada modificação significativa, mudança operacional ou novo dado de risco. No Brasil, o arcabouço regulatório do SGSO (Resolução ANP 43/2007) e a NT 10/2023 estabelecem requisitos funcionalmente equivalentes.

Ver também: ALARP; Bow-tie; HAZOP; MAH; Risco Residual.

Fontes: ISO 17776, 2016; Hopkins, 2000; IOGP 544, 2016; NT 10/2023 ANP.

Incubação (Período de)

Período que precede desastres durante o qual sinais de perigo se acumulam sem serem reconhecidos, em desacordo com as crenças estabelecidas sobre os perigos. Pode variar de semanas a décadas. Caracterizado por rigidez de crenças, fenômeno do engodo e relutância em temer o pior resultado. Turner identificou seis estágios: normalidade inicial → incubação → evento precipitante → manifestação do desastre → resgate → ajuste cultural.

Ver também: Desastre Fabricado; Fenômeno do Engodo; Normalização do Desvio; Deriva para Falha.

Fontes: Turner, 1978; Turner & Pidgeon, 1997.

Indicadores Antecipadores (*Leading Indicators*)

Métricas que monitoram o estado de saúde das barreiras, processos e capacidades organizacionais antes que ocorram eventos adversos – disponibilidade de sistemas de proteção, atrasos em manutenções críticas, treinamentos vencidos, desvios de procedimentos, resultados de inspeções de integridade. No framework Indicadores de Segurança de Processos (Tier 1-4) (API RP 754), correspondem ao Nível 4. São os mais sensíveis e valiosos para prevenção, pois permitem intervenção antes da materialização do evento.

Ver também: Indicadores de Segurança de Processos (Tier 1-4); Indicadores Reativos; Segurança de Processo; Falácia LTI.

Fontes: API RP 754, 2021; Hollnagel, 2014; Hopkins, 2008.

Indicadores Reativos (*Lagging Indicators*)

Métricas que mensuram eventos adversos já ocorridos – taxas de frequência de acidentes, lesões com afastamento (LTI), liberações de hidrocarbonetos, ativações de sistemas de proteção. Indispensáveis, mas insuficientes: organizações que monitoram apenas eventos passados aprendem tarde demais. No framework Indicadores de Segurança de Processos (Tier 1-4), correspondem aos Níveis 1 e 2. Devem ser combinados com indicadores antecipadores.

Ver também: Indicadores Antecipadores; Indicadores de Segurança de Processos (Tier 1-4); Falácia LTI; SIF e Potencial SIF.

Fontes: API RP 754, 2016; Hollnagel, 2014.

Interface Humano-Máquina (IHM / HMI)

Ponto de interação entre operador humano e sistema técnico, incluindo displays, controles, alarmes e dispositivos de entrada de dados. O design adequado de IHM é fundamental para prevenir erros e apoiar a consciência situacional. Ver seção 3.5.

Ver também: Engenharia de Fatores Humanos (HFE); Erro Humano.

Fontes: ISO 11064; IOGP 454, 2020.

J

Justiça Processual (*Procedural Justice*)

Uma das três dimensões da justiça organizacional: estabelece processos legítimos para determinar violações de regras, oferece proteções ao acusado, e governa quem deve fazer tais determinações. Inclui presunção de inocência, direito a representação e possibilidade de recurso.

Ver também: Cultura Justa; Justiça Substantiva; Justiça Restaurativa; Justiça Retributiva.

Fonte: Dekker & Breakey, 2016.

Justiça Restaurativa (*Restorative Justice*)

Abordagem que visa restaurar o status do indivíduo envolvido e curar relacionamentos e danos após uma falha, em contraste com justiça retributiva. Se o erro causou dano, a resposta deve curar, não causar mais dano. Reconhece múltiplas vítimas em um incidente, incluindo as segundas vítimas (profissionais envolvidos).

Ver também: Cultura Justa; Justiça Retributiva; Segunda Vítima.

Fontes: Dekker & Breakey, 2016; Dekker, 2017.

Justiça Retributiva (*Retributive Justice*)

Abordagem que foca na correspondência entre tipos de ação humana e respostas gerenciais proporcionais, utilizando algoritmos e árvores de decisão para categorizar comportamentos em graus de culpabilidade. É a abordagem predominante nas implementações organizacionais atuais.

Ver também: Cultura Justa; Justiça Restaurativa; Captura Punitiva do Sistema de Accountability.

Fontes: Reason, 1997; Marx, 2001.

Justiça Substantiva (*Substantive Justice*)

Uma das três dimensões da justiça organizacional: refere-se à legitimidade e equidade das próprias regras, regulamentos e procedimentos. Procedimentos percebidos como injustos ou desconectados da realidade operacional minam a base moral para responsabilização.

Ver também: Cultura Justa; Justiça Processual; Lacuna WAI-WAD.

Fonte: Dekker & Breakey, 2016.

L

Laboratórios de Fatores Humanos

Espaços organizacionais estruturados voltados à construção conjunta de conhecimento em Fatores Humanos entre lideranças e profissionais. Diferem de palestras ou treinamentos por seu caráter experimental e dialógico: princípios são testados, ressignificados e negociados contra a realidade operacional da organização. A escolha do termo "laboratório", segundo Henriqson, captura a noção de "espaço de experimentação de ideias". Constituem manifestação prática do Movimento I (Engajamento das Lideranças & Governança).

Ver também: Movimentos da Jornada; Princípios de Fatores Humanos (PFH); Fatores Humanos como Jornada.

Fontes: Bruno, 2020; Henriqson, 2023; Almeida, Bruno & Capaverde, 2025.

Lacuna WAI-WAD

Diferença estrutural e inevitável entre o Trabalho como Imaginado (WAI) – como gestores, designers e reguladores pressupõem que o trabalho acontece – e o Trabalho como Realizado (WAD) – como o trabalho efetivamente acontece na prática. Não é um defeito a ser eliminado: resulta da variabilidade, incerteza e complexidade inerentes a sistemas sociotécnicos. Compreender esta lacuna – em vez de tentar eliminá-la pela multiplicação de procedimentos – permite identificar onde adaptações cotidianas criam segurança e

onde podem introduzir riscos não reconhecidos.
Ver também: Trabalho como Imaginado (WAI); Trabalho como Realizado (WAD); Deriva Prática; Racionalidade Local; Safety-II.
Fontes: Hollnagel, 2014, 2017.

Learning Teams (Times de Aprendizagem / LIT)

Dispositivo organizacional dedicado à observação do trabalho como prática regular, e não como auditoria ou evento extraordinário. Em uma sessão LIT, facilitadores treinados, supervisão de linha e trabalhadores da linha de frente observam conjuntamente a operação diária com foco em compreensão – não em fiscalização – para tornar visível o saber-na-prática que vive nas operações cotidianas (Gherardi, 2012). A distinção em relação às auditorias comportamentais clássicas é ontológica antes de ser metodológica: a LIT não compara o desempenho a um padrão prescrito (Trabalho como Imaginado) para identificar desvios, mas observa o Trabalho como Realizado para aprender com ele – incluindo, em particular, as variações benéficas que normalmente permanecem invisíveis ao sistema de gestão (Hollnagel, 2018). A expressão circulou inicialmente na tradição Human and Organizational Performance (HOP) e em experiências aplicadas em aviação, notadamente na American Airlines (FSF, 2021). Aplicações no setor de óleo e gás têm sido documentadas em diferentes empresas, incluindo a variante denominada **LIT** (***Learning and Improvement Teams***) implementada na Constellation Serviços de Petróleo, que integra aprendizado e ação de melhoria em um mesmo ciclo (Almeida, Bruno & Capaverde, 2025). Condição necessária para o funcionamento de uma LIT é a segurança psicológica do diálogo: sem ela, o saber situado da linha de frente não emerge. Ver Seção 3.2.6.
Ver também: Aprendizagem Operacional; Aprendizagem Organizacional; HOP; Safety-II; Trabalho como Realizado (WAD); Lacuna WAI-WAD; Segurança Psicológica.
Fontes: Gherardi, 2012; Conklin, 2019; Hollnagel, 2018; FSF, 2021; Almeida, Bruno & Capaverde, 2025.

LOPA (Análise de Camadas de Proteção – *Layers of Protection Analysis*)

Metodologia semiquantitativa que avalia se as camadas de proteção independentes (IPL – *Independent Protection Layer*) existentes para um cenário de risco reduzem o risco residual a um nível aceitável (ALARP). Para cada IPL, o LOPA estima uma Probabilidade de Falha na Demanda (PFD), que representa a probabilidade de que a barreira falhe em prevenir ou mitigar o evento quando acionada. O risco residual de um cenário é calculado multiplicando a frequência do evento iniciador pelas PFDs de todas as IPLs associadas. A condição

de independência entre as IPLs é fundamental: barreiras que compartilham componentes, dependem do mesmo operador ou falham por causas comuns não podem ser contabilizadas como camadas independentes – violação frequentemente identificada em investigações de acidentes de processo. O LOPA é conduzido após o HAZOP e alimenta a definição de requisitos de integridade para Sistemas Instrumentados de Segurança (SIS/SIL).
Ver também: Bow-tie; HAZOP; ALARP; MAH; PFD; Risco Residual; Barreira.
Fontes: CCPS, 2001; IEC 61511, 2016; IEC 61882, 2016.

M

Major Accident Hazard (MAH – Perigo de Acidente Maior)

Situação com potencial para causar acidentes de grande magnitude, incluindo múltiplas fatalidades, danos ambientais severos ou perdas catastróficas de ativos, decorrentes de falhas em processos industriais. Na indústria de óleo e gás offshore, os MAHs típicos incluem: perda de controle de poço (blowout), explosão e incêndio na instalação, liberação de gás tóxico, colisão de embarcações e afundamento da unidade. A identificação sistemática de todos os MAH scenarios de uma instalação – e das barreiras que os controlam – é o ponto de partida de qualquer sistema de gestão de Segurança de Processo. Os MAH scenarios são formalmente capturados em bow-ties e quantificados via LOPA. A distinção entre MAH (risco de processo catastrófico) e riscos ocupacionais convencionais é fundamental: indicadores de segurança pessoal como LTI não refletem o estado das barreiras que previnem acidentes maiores.
Ver também: MAH Scenarios; Bow-tie; HAZOP; LOPA; HSE Case; Segurança de Processo; Falácia LTI.
Fontes: ISO 17776, 2016; CCPS, 2007; Hopkins, 2012; NT 10/2023 ANP.

MAH Scenarios

Representações estruturadas de como um perigo de acidente maior pode evoluir para um evento catastrófico, incluindo a cadeia de causas (ameaças), o evento central (*top event*) e as possíveis consequências. São o objeto formal de modelagem em bow-ties e quantificação em LOPA. Sua identificação sistemática é exigência regulatória (NT 10/2023 ANP, ISO 17776) e ponto de partida de qualquer sistema de gestão de Segurança de Processo.
Ver também: MAH; Bow-tie; LOPA; HAZID; HSE Case.
Fontes: ISO 17776, 2016; NT 10/2023 ANP.

Migração para os Limites (*Migration to the Boundaries*)

Processo sistemático pelo qual atividades em sistemas sociotécnicos movem-se gradualmente em direção às fronteiras de desempenho aceitável sob pressão de gradientes de eficiência e menor esforço. Conceito central da perspectiva Rasmusseniana. A migração é incremental, cada passo parece racional, e a estrutura de defesa em profundidade pode ocultar o processo até que um cruzamento irreversível de fronteira ocorra.

Ver também: Fronteira de Desempenho Aceitável; Gradiente de Pressão; Deriva para Falha; AcciMap.

Fonte: Rasmussen, 1997.

Mindful Organizing

Processo organizacional contínuo descrito por Weick e Sutcliffe como prática coletiva concreta que sustenta a alta confiabilidade. Distingue-se de *mindfulness organizacional* como estado mental: *mindful organizing* é o que a organização **faz** – através dos cinco processos (preocupação com falhas, relutância em simplificar, sensibilidade às operações, compromisso com a resiliência, deferência à expertise). Esta distinção, enfatizada na 3ª edição (2015) de *Managing the Unexpected*, é importante para evitar a leitura individualizante de "mindfulness" como atributo psicológico isolado.

Ver também: Mindfulness Organizacional; HRO; Process Auditing.

Fonte: Weick & Sutcliffe, 2015.

Mindfulness Organizacional (*Organizational Mindfulness*)

Estado de consciência atenta caracterizado por cinco processos cognitivos coletivos: (1) preocupação com falhas, (2) relutância em simplificar, (3) sensibilidade às operações, (4) compromisso com a resiliência e (5) deferência à expertise. Os três primeiros são processos de antecipação; os dois últimos, de contenção. Característica distintiva de HROs. **Nota de uso**: na 3ª edição (2015) de *Managing the Unexpected*, Weick e Sutcliffe enfatizaram a expressão *mindful organizing* (substantivo de ação) para evitar a leitura individualizante de "mindfulness" como atributo psicológico, deslocando o foco para o que a organização concretamente faz.

Ver também: Mindful Organizing; HRO; Preocupação com Falhas; Relutância em Simplificar; Sensibilidade às Operações; Compromisso com a Resiliência; Deferência à Expertise.

Fontes: Weick & Sutcliffe, 2007, 2015.

Movimentos da Jornada (de Fatores Humanos)

Arquitetura conceitual do framework integrador proposto na Parte IV deste compêndio para a transformação organizacional em Fatores Humanos. Organiza a jornada em cinco movimentos direções de desenvolvimento organizacional simultâneas, recursivas e interdependentes e não estágios sequenciais de um modelo de maturidade a serem "concluídos": (I) Engajamento das Lideranças & Governança mudança de modelo mental e estrutura de governança da jornada; (II) Fluência nos Fundamentos disseminação de linguagem e repertório conceitual comuns; (III) Aprendizagem Operacional conexão com o trabalho real (WAI WAD); (IV) Alinhamento e Integração revisão de sistemas, processos e políticas de consequência à luz dos princípios de Fatores Humanos; e (V) Resiliência e Capacidade Adaptativa desenvolvimento das capacidades de antecipar, monitorar, responder e aprender. Cada movimento fornece insumos aos demais e deles recebe insumos (ver Tabela 4.2.3), configurando um sistema dinâmico de aprendizagem contínua, e não um caminho linear com ponto de chegada definido. Um princípio transversal aos cinco movimentos é a expansão do olhar do micro para o macro (Seção 4.2.6). Ver Seção 4.2.

Ver também: Comitê de Fatores Humanos; Antítese (Princípio de); Aprendizagem Operacional; Coerência entre o Dizer e o Fazer; Princípios de Fatores Humanos (PFH).

Fontes: Almeida et al., 2025; Bruno, 2020; Henriqson, 2023.

Modelo do Queijo Suíço (*Swiss Cheese Model*)

Representação visual de como acidentes ocorrem quando múltiplas camadas de defesa falham simultaneamente, permitindo que uma trajetória de acidente atravesse todas as barreiras. Cada camada (fatia de queijo) tem buracos (vulnerabilidades) que podem se alinhar. Introduz a distinção crucial entre falhas ativas e condições latentes.

Ver também: Falha Ativa; Condição Latente; Defesa em Profundidade; Extremidades Afiada e Cega.

Fontes: Reason, 1990, 1997.

N

Normalização do Desvio (*Normalization of Deviance*)

Processo pelo qual comportamentos que violam procedimentos ou especificações tornam-se gradualmente aceitos como normais através de revisões formais que estabelecem precedentes institucionalizados. Diferente de deriva prática, é oficialmente reconhecido e incorporado às políticas. Sustentado pelo "segredo estrutural" – a forma como divisão de

trabalho e especialização segregam conhecimento sobre riscos.
Ver também: Deriva Prática; Segredo Estrutural; Incubação; Fine-Tuning; Desastre Fabricado.
Fonte: Vaughan, 1996.

Nova Segurança

Designação que reúne movimentos contemporâneos da segurança consolidados a partir dos anos 2000 – Novas Visões do erro humano, Engenharia de Resiliência, *Safety Differently*, *Safety-II*/Segurança Incremental e HOP. Apesar de vocabulários e autores próprios, compartilham uma raiz comum: a retomada dos princípios da organização sociotécnica do trabalho como lógica para compreender o desempenho de pessoas, equipes e organizações e tornar os sistemas mais seguros. Ver Seção 1.2.5.
Ver também: Nova Visão; Engenharia de Resiliência; *Safety Differently; Safety-II;* HOP.
Fontes: Dekker, 2014; Le Coze, 2022.

Nova Visão (*New View*)

Movimento que reconceitualizou o erro humano como sintoma de condições sistêmicas mais profundas, e não como causa primária de acidentes. Originou-se da Engenharia de Sistemas Cognitivos (Rasmussen, Hollnagel, Woods, anos 1970) e o termo foi cunhado por Dekker nos anos 2000. Reconhece que pessoas criam segurança dinamicamente, reconciliando demandas conflitantes e mantendo unidos sistemas inerentemente imperfeitos.
Ver também: Nova Segurança; Visão Tradicional; Safety Differently; HOP; Erro Humano; Racionalidade Local.
Fontes: Dekker, 2014; Le Coze, 2022.

P

PetroHRA

Método de análise de confiabilidade humana desenvolvido especificamente para a indústria de petróleo e gás pelo IFE (Institute for Energy Technology). Contém fatores modeladores de desempenho (PSF) específicos para contexto offshore, incluindo complexidade da tarefa, tempo disponível, qualidade dos procedimentos, ambiente de trabalho e suporte organizacional. Originalmente desenvolvido para análise de eventos pós-iniciadores em cenários de processo; mediante ajustes nos PSFs, pode ser adaptado para outros tipos de tarefa.

Ver também: HRA; PSF; HEP; SPAR-H; CREAM.
Fonte: IFE, 2022.

PFD (*Probability of Failure on Demand* — Probabilidade de Falha sob Demanda)

Probabilidade de que uma barreira ou camada de proteção, quando demandada, falhe em executar sua função de segurança. É a medida quantitativa central do desempenho de barreiras instrumentadas e de proteção, expressando a indisponibilidade média da função no intervalo entre testes – quanto menor a PFD, maior a confiabilidade da barreira. Relaciona-se ao nível de integridade de segurança (SIL), alimenta os cálculos de LOPA e a avaliação ALARP e integra o gerenciamento dinâmico de barreiras: a degradação de qualquer elemento eleva a PFD do conjunto e reduz a margem de risco residual.
Ver também: Barreira; Conjunto Solidário de Barreiras (CSB); LOPA; ALARP; Risco Residual; HSE Case.
Fonte: IEC 61508/61511; CCPS/Energy Institute, 2018; IOGP 544, 2016.

Potenciais da Resiliência (Quatro Capacidades)

Denominados sucessivamente quatro habilidades (abilities), pilares (cornerstones), capacidades e, mais recentemente, potenciais ou potenciais sistêmicos, termo que enfatiza algo que a organização exerce e precisa sustentar, e não um atributo que possui. Capacidades essenciais para organizações resilientes, identificadas por Hollnagel: (1) Responder – saber o que fazer diante de eventos regulares e irregulares; (2) Monitorar – saber o que observar para identificar ameaças; (3) Antecipar – saber o que esperar e preparar-se para surpresas; (4) Aprender – saber o que aconteceu e extrair lições de experiências passadas. Devem ser desenvolvidos de forma integrada, em equilíbrio apropriado ao tipo de atividade e da situação; o método RAG é o principal instrumento para acompanhá-los.
Ver também: Engenharia de Resiliência; RAG; FRAM; Adaptabilidade Sustentada; Capacidade Adaptativa.
Fontes: Hollnagel, 2008, 2009, 2011, 2018, 2025.

Preocupação com Falhas (*Preoccupation with Failure*)

Um dos cinco processos de *mindful organizing*: tratar quase-acidentes e anomalias como sintomas de vulnerabilidades sistêmicas, não como evidências de sucesso. Manter vigilância mesmo após longos períodos sem acidentes, resistindo à complacência que o sucesso engendra.
Ver também: Mindful Organizing; HRO; Relutância em Simplificar.
Fontes: Weick & Sutcliffe, 2007, 2015.

Princípio ETTO (*Efficiency-Thoroughness Trade-Off*)

Formalização do trade-off inevitável entre eficiência e completude. Em condições de recursos limitados, é impossível ser simultaneamente máximo em eficiência e em completude. Explica por que adaptações e "atalhos" são normais e necessários – e por que quanto mais regras existem, mais fácil se torna mostrar que pelo menos algumas não são cumpridas.

Ver também: FRAM; Variabilidade de Desempenho; Lacuna WAI-WAD; Safety Clutter.

Fonte: Hollnagel, 2009.

Princípios de Fatores Humanos (PFH)

Postulados ou axiomas que orientam uma organização sobre como pensar segurança, erro e desempenho humano. Funcionam como "políticas de governo das práticas" (Henriqson, 2023): criam o referencial comum a partir do qual as práticas organizacionais – procedimentos, indicadores, sistemas disciplinares, processos de aprendizado – são revisadas e ressignificadas. A formalização de PFH é tipicamente o produto do Movimento I (Engajamento das Lideranças). Petrobras e Constellation publicaram conjuntos próprios de PFH. Não há um conjunto universal: a literatura oferece referências (os cinco princípios do HOP de Conklin, por exemplo), mas a construção é organizacional e participativa.

Ver também: HOP; Laboratórios de Fatores Humanos; Movimentos da Jornada; Antítese (Princípio de); Coerência entre o Dizer e o Fazer.

Fontes: Conklin, 2019; Henriqson, 2023; Bruno, 2020.

Probabilidade de Erro Humano (HEP – *Human Error Probability*)

Medida quantitativa da probabilidade de que um erro humano específico ocorra durante a execução de uma tarefa. Valor central nas análises de confiabilidade humana (HRA), influenciado pelos fatores modeladores de desempenho (PSF). Valores típicos em sistemas de alto risco situam-se entre 10^{-1} (tarefas complexas sob pressão de tempo, baixa qualidade procedimental) e 10^{-5} (tarefas simples, bem treinadas, com verificações cruzadas independentes).

Ver também: HRA; PSF; PetroHRA; SPAR-H; THERP; CREAM.

Fontes: Kirwan, 2017; IFE, 2022.

Procedimento Crítico

Procedimento cuja falha ou ausência de execução possa causar ou contribuir para acidente operacional associado a grandes emergências. Identificado quando é salvaguarda em análise de risco, associado a incidente de alta severidade, relacionado a elementos críticos, ou criado como contingência a falha de elemento crítico.

Ver também: ECSO; Tarefa Crítica de Segurança Operacional; Equipamento Crítico; Sistema Crítico.
Fontes: NT 10/2023 ANP; Guia IADC Brasil, 2025.

Q

QRA (*Quantitative Risk Assessment*)

Análise quantitativa de risco. Estudo estruturado que estima, em termos numéricos, os riscos associados a uma instalação ou operação – tipicamente expressos como risco individual (probabilidade anual de fatalidade para um indivíduo) e risco coletivo (curva F-N, frequência acumulada de cenários com N ou mais fatalidades). O QRA integra resultados de análises antecedentes (HAZID, HAZOP, FERA, EERA, FMEA) com modelagem probabilística (árvores de eventos, árvores de falhas) e cálculos físicos (dispersão de gases, radiação térmica, sobrepressões) para produzir uma estimativa global de risco da instalação. É insumo central para a demonstração de conformidade ao critério ALARP e para a tomada de decisão sobre investimentos em redução de risco. Em instalações offshore, o QRA fundamenta a elaboração do HSE Case e responde a requisitos regulatórios da ANP (NT 10/2023) e de jurisdições internacionais.
Ver também: HAZID; HAZOP; FERA; EERA; FMEA/FMECA; ALARP; HSE Case; MAH; Risco Residual.
Fontes: ISO 17776, 2016; Lees, 2012; CCPS, 2007; NT 10/2023 ANP.

R

Raciocínio Contrafactual (*Counterfactual Reasoning*)

Na análise de acidentes, tentativa de explicar a diferença entre o evento em questão e algum caso contrastante ("se apenas..."). Pode ser problemático quando o caso contrastante é irreal ou ignora as restrições que os praticantes enfrentavam. Facilita o viés de retrospectiva ao fazer a decisão "correta" parecer óbvia em retrospecto.
Ver também: Viés de Retrospectiva; Racionalidade Local; Histórias Primárias e Secundárias.
Fontes: Hilton, 1990; Woods et al., 2010.

Racionalidade Local (*Local Rationality*)

Princípio segundo o qual ações das pessoas fazem sentido dado seu conhecimento, objetivos, ponto de vista e recursos limitados no momento da decisão. Não existem "decisões monumentalmente ruins" — há apenas pequenos passos incrementais que parecem razoá-

veis no contexto. Fundamental para análise sistêmica de acidentes sem viés de retrospectiva.
Ver também: Viés de Retrospectiva; Erro Humano; Histórias Primárias e Secundárias; Lacuna WAI-WAD.
Fontes: Dekker, 2014a.

RAG (*Resilience Assessment Grid*)

Grade de Análise de Resiliência. Ferramenta para avaliar as capacidades de resiliência de uma organização em relação aos Potenciais da Resiliência (responder, monitorar, antecipar, aprender), por meio de questões avaliadas em escala de seis níveis de "ausência" a "excelente". Gera diagrama em estrela que visualiza pontos fortes e fracos. Representa um instantâneo qualitativo do momento avaliado, não uma métrica objetiva e permanente; ao ser reaplicado com as mesmas perguntas e o mesmo grupo de respondentes, permite acompanhar a evolução dos potenciais. Não define limiar de "resiliência"; cabe à organização decidir o que aprimorar. Versões recentes ancoram a avaliação na observação do trabalho cotidiano e nas práticas que sustentam cada potencial. A variante *Resilience Assessment Grid* também circula na literatura. Ver Seções 2.4.3 e 3.2.7.
Ver também: Potenciais da Resiliência; FRAM; Engenharia de Resiliência; Capacidade Adaptativa.
Fonte: Hollnagel, 2011; Ljungberg & Lundh, 2013; Trancoso, Patriarca & Henriqson, 2024.

Redundância

Duplicação de componentes, funções ou processos críticos para garantir que a falha de um elemento não comprometa o sistema como um todo. Pode ser técnica (equipamentos backup), social (verificações cruzadas entre membros da equipe) ou procedimental (múltiplas aprovações). Característica central de HROs.
Ver também: HRO; Defesa em Profundidade; Conjunto Solidário de Barreiras (CSB).
Fontes: La Porte & Consolini, 1991; Reason, 1997.

Relutância em Simplificar (*Reluctance to Simplify*)

Um dos cinco processos de *mindful organizing*: resistir a explicações simplistas e buscar entendimento profundo das situações. Reconhecer que o mundo é complexo e que simplificações excessivas podem ocultar vulnerabilidades críticas.
Ver também: Mindful Organizing; HRO; Conceptual Slack.
Fontes: Weick & Sutcliffe, 2007, 2015.

Resiliência (*Resilience*)

Na Engenharia de Resiliência, a capacidade de um sistema de ajustar seu funcionamento antes, durante ou após mudanças, perturbações e oportunidades, de modo a sustentar as operações sob condições esperadas e inesperadas. Amplia a definição inicial de Hollnagel (2006), centrada em reagir e recuperar-se de perturbações. Descreve o que o sistema faz, e não o que ele é: tornar-se resiliente é um processo contínuo, não estado a ser atingido. Distingue-se da robustez e da confiabilidade e não deve ser tratado como traço individual (ver Armadilhas Analíticas). Ver Seção 2.4.

Ver também: Engenharia de Resiliência; Capacidade Adaptativa; Potenciais da Resiliência; Robustez; Colapso Abrupto; Compromisso com a Resiliência.

Fontes: Hollnagel, 2006, 2018; Nemeth & Hollnagel, 2022; Woods, 2006, 2015.

Ressonância Funcional (*Functional Resonance*)

Fenômeno pelo qual variabilidades de múltiplas funções em um sistema se combinam de forma inesperada, podendo produzir resultados que não poderiam ser previstos a partir da análise de funções individuais. Conceito central do método FRAM, substitui a noção de "causa-raiz" pela de emergência de padrões complexos.

Ver também: FRAM; Variabilidade de Desempenho; Princípio ETTO.

Fonte: Hollnagel, 2012.

Risco Residual

Risco efetivo de um cenário de acidente após o efeito mitigador de todas as barreiras (camadas de proteção independentes, IPLs) que o controlam. Calculado em LOPA pela combinação da frequência do evento iniciador com as probabilidades de falha na demanda (PFDs) de todas as IPLs associadas. Não é constante: aumenta quando barreiras se degradam (equipamento falhando, manutenção em atraso, guardião sem treinamento vigente, procedimento desatualizado). O monitoramento dinâmico das barreiras busca acompanhar essas variações em tempo real, evitando que a organização opere com o risco calculado na última análise estática.

Ver também: LOPA; Barreira; PFD; ALARP; MAH.

Fontes: CCPS, 2001; IEC 61511, 2016; Hopkins, 2012.

S

Safety Clutter

Acúmulo e persistência de trabalho rotulado como "segurança" que não contribui efetivamente para a segurança operacional, mas consome recursos e atenção que poderiam ser direcionados para riscos genuínos. Resulta frequentemente da adição cumulativa de procedimentos, formulários e controles em resposta a eventos, sem avaliação crítica de seu valor real. Em sistemas saturados de procedimentos, o *safety clutter* paradoxalmente aumenta a probabilidade de violações documentáveis — e, portanto, de mais regras.

Ver também: Avaliação Crítica de Práticas; Princípio ETTO; Lacuna WAI-WAD.

Fonte: Rae, Weber & Dekker, 2018.

Safety Differently

Abordagem desenvolvida por Dekker que enfatiza engajamento com a complexidade do trabalho real, valorização da expertise operacional e foco em criar condições para o sucesso. Parte do movimento das "Novas Visões" de segurança. Propõe honrar as pessoas como solucionadores de problemas, em vez de controlá-las como fontes de risco.

Ver também: Nova Visão; HOP; Safety-II; Cultura Justa.

Fonte: Dekker, 2014.

Safety-I (Segurança Decremental)

Abordagem tradicional de segurança que define segurança como ausência de eventos indesejados (acidentes, incidentes) e foca em prevenir que coisas deem errado. Investiga por que as coisas falham e intervém para eliminar ou mitigar causas de falha. Centrada em componentes e suas falhas.

Ver também: Safety-II; Visão Tradicional; Erro Humano.

Fonte: Hollnagel, 2014.

Safety-II (Segurança Incremental)

Abordagem que define segurança como a capacidade de ter sucesso sob condições variadas, esperadas e inesperadas. Foca em garantir que as coisas deem certo, compreendendo a variabilidade positiva do desempenho humano. Investiga como o sucesso é cotidianamente criado — não apenas como falhas ocasionalmente ocorrem.

Ver também: Safety-I; Engenharia de Resiliência; Variabilidade de Desempenho; Lacuna WAI-WAD; Indicadores Antecipadores.

Fonte: Hollnagel, 2014.

Segredo Estrutural (*Structural Secrecy*)

Forma como o conhecimento é organizado em uma organização – pela divisão de trabalho, hierarquia e especialização — que pode resultar em pessoas sabendo menos precisamente porque a organização tenta comunicar mais. A estrutura "proporciona uma forma de ver que é simultaneamente uma forma de não ver" (Vaughan, 1999).

Ver também: Normalização do Desvio; Desastre Fabricado; Incubação.

Fontes: Vaughan, 1996, 1999.

Segunda Vítima (*Second Victim*)

Profissional envolvido em um incidente ou acidente que sofre consequências psicológicas significativas como resultado de seu envolvimento — culpa, ansiedade, dúvida de competência. Reconhecimento de que incidentes produzem múltiplas vítimas além das vítimas primárias. Conceito relevante para o design de sistemas de cultura justa e de suporte organizacional.

Ver também: Cultura Justa; Justiça Restaurativa; Captura Punitiva do Sistema de Accountability.

Fonte: Dekker, 2013.

Segurança (*Safety*)

Propriedade emergente de sistemas sociotécnicos complexos (Leveson, 2002; Rasmussen, 1997), construída e reconstruída continuamente pela interação dinâmica entre pessoas, tecnologia, ambiente e organização. Não é estado inerente a ser preservado, mas realização coletiva sustentada por capacidades adaptativas – antecipar, monitorar, responder e aprender (Hollnagel, 2011) – e por práticas situadas que praticantes mobilizam para conciliar demandas reais do trabalho (Gherardi, 2006; Woods et al., 2010). A literatura contemporânea distingue Safety-I (segurança como ausência de eventos indesejados) de Safety-II (segurança como presença de capacidades que permitem o sucesso sob variabilidade) (Hollnagel, 2014). Em síntese, segurança é a presença viva de capacidades positivas que fazem as coisas darem certo, colhida das condições cultivadas cotidianamente em todos os níveis da organização. Ver seções 1.1.4 e 2.4.

Ver também: Sistema Sociotécnico; Capacidade Adaptativa; Engenharia de Resiliência; Safety-I; Safety-II; Potenciais da Resiliência; Aprendizagem Operacional; Variabilidade de Desempenho.

Fonte: Gherardi, 2006; Hollnagel, 2011, 2014; Leveson, 2002; Rasmussen, 1997; Reason, 1997; Woods et al., 2010.

Segurança de Processo (*Process Safety*)

Disciplina que busca prevenir e mitigar acidentes de grande magnitude (*Major Accident Hazards* – MAH) decorrentes de falhas em processos industriais: vazamentos de hidrocarbonetos, explosões, incêndios e emissões tóxicas – com potencial para múltiplas fatalidades, danos ambientais severos ou perdas catastróficas de ativos. Difere fundamentalmente da segurança pessoal (ocupacional; ver Seção 3.6.1, nota [^2]): esta trata de lesões individuais de trabalhadores; aquela trata de eventos catastróficos que afetam múltiplas pessoas, comunidades e o meio ambiente. Indicadores de segurança pessoal (LTI, taxa de frequência) não refletem o estado das barreiras de processo – como demonstraram tragicamente Texas City (2005) e Macondo (2010), onde bons indicadores ocupacionais coexistiam com erosão progressiva das defesas de processo (Hopkins, 2008, 2012). A gestão de Segurança de Processo estrutura-se em: (a) identificação sistemática de MAH scenarios (via HAZID, HAZOP, FERA, QRA); (b) modelagem e gerenciamento de barreiras (Bow-tie, LOPA, CSB); (c) monitoramento dinâmico do estado das barreiras e do risco residual; (d) indicadores específicos de processo (Indicadores de Segurança de Processos, níveis 1–4); e (e) demonstração integrada via HSE Case. No Brasil, a NT 10/2023 da ANP e a Resolução 43/2007 (SGSO) estabelecem os requisitos regulatórios para esta gestão. Ver seção 3.6.

Ver também: MAH; Bow-tie; LOPA; HSE Case; Indicadores de Segurança de Processos (Tier 1-4); Falácia LTI; Risco Residual; SIF e Potencial SIF.

Fontes: Hopkins, 2008, 2012; CCPS, 2007; ISO 17776, 2016; NT 10/2023 ANP; Rosness et al., 2010.

Segurança Psicológica (*Psychological Safety*)

Crença compartilhada pelos membros de uma equipe de que o ambiente é seguro para assumir riscos interpessoais — expressar dúvidas, admitir erros, propor ideias não convencionais ou relatar problemas sem medo de punição, humilhação ou retaliação. É condição estrutural para o funcionamento efetivo de sistemas de reporte, Learning Teams e aprendizagem organizacional. Sem segurança psicológica, os princípios de Cultura Justa e HOP permanecem nominais, pois as pessoas continuam a ocultar informações sobre falhas e vulnerabilidades.

Ver também: Cultura Justa; HOP; Learning Teams; Aprendizagem Organizacional.

Fonte: Edmondson, 2019.

Segurança Pessoal (*Personal Safety*)

Ramo da segurança voltado à prevenção de lesões que atingem o trabalhador individualmente (quedas, cortes, choques, esforços), em contraste com a Segurança de Processo, que trata de eventos catastróficos de perda de contenção e integridade. Adota-se neste

compêndio a expressão segurança pessoal, seguindo Hopkins (2008), por ser conceitualmente mais precisa que **"segurança ocupacional"** – termo consagrado no Brasil, mas que, em sentido amplo, abarca todos os perigos do ambiente de trabalho, inclusive os de processo. É o eixo medido por indicadores de frequência (TRIR, LTIR) e, para as consequências severas, por SIFR e PSIFR.
Ver também: Segurança de Processo; SIF e Potencial SIF; SIFR e PSIFR; Falácia LTI/TRI.
Fonte: Hopkins (2008).

Sensibilidade às Operações (*Sensitivity to Operations*)

Um dos cinco processos de *mindful organizing*: manter consciência situacional contínua do que está acontecendo na linha de frente, mantendo contato próximo com a realidade operacional. Líderes com alta sensibilidade às operações percebem sinais fracos que podem indicar deterioração de barreiras.
Ver também: Mindful Organizing; HRO; Indicadores Antecipadores.
Fontes: Weick & Sutcliffe, 2007, 2015.

SIF (*Serious Injury or Fatality*) e Potencial SIF

SIF: evento que resultou em fatalidade ou lesão grave (amputação, fratura exposta, dano permanente). **Potencial SIF**: evento que, sob circunstâncias ligeiramente diferentes, poderia ter resultado em SIF – mesmo que o desfecho real tenha sido leve. A distinção é fundamental porque eventos com potencial catastrófico frequentemente têm precursores distintos dos acidentes ocupacionais menores. Eventos Potencial SIF devem receber o mesmo rigor investigativo que eventos SIF reais. Distinguem-se dois estados mutuamente exclusivos de um mesmo evento: SIF real (SIFa), em que a lesão grave ou a fatalidade efetivamente ocorreu, e Potencial SIF (SIFp), em que o desfecho grave era plausível, mas não se concretizou – um mesmo evento é classificado como SIFa ou SIFp, não como ambos. A caracterização do potencial apoia-se no modelo de precursores baseado em energia: alta energia (limiar operacional da ordem de 680 J / 500 ft-lb) combinada à ausência de um controle direto capaz de mitigá-la (Hallowell et al., 2017; EEI, 2024). As taxas correspondentes – SIFR e PSIFR – constam de verbete próprio. Desambiguação: não confundir com SIF – *Safety Instrumented Function* (função instrumentada de segurança, classificada por SIL), termo homônimo empregado em segurança de processo (ver verbete Sistema Crítico e SIF/SIL).
Ver também: Falácia LTI; Indicadores de Segurança de Processos (Tier 1-4); Segurança de Processo; MAH; SIFR e PSIFR; Segurança Pessoal; Sistema Crítico (SIF/SIL).
Fontes: IOGP 456, 2018; CSB; Energy Institute; Hallowell et al., 2017; EEI, 2024.

SIFR e PSIFR (*Serious Injury and Fatality Rate / Potential Serious Injury and Fatality Rate*)

Taxas correspondentes aos eventos SIF e Potencial SIF, normalizadas por horas-homem expostas (tipicamente por 200.000 ou 1.000.000 de horas), à semelhança do TRIR. O SIFR mede a frequência de SIF reais indicador reativo, de baixa frequência e alta severidade; o PSIFR mede a frequência de eventos com potencial SIF, comportando-se como indicador mais sensível e antecipatório do estado das defesas contra consequências severas. Por SIFa e SIFp serem mutuamente exclusivos, SIFR + PSIFR podem ser lidos conjuntamente como exposição total a SIF, sem dupla contagem. Para fins de incentivo, recomenda-se tratar o SIFR como condição de barreira (gate) e o PSIFR como métrica contínua de melhoria (Martin & Black, 2015; Hallowell et al., 2021; IOGP, 2025).

Ver também: SIF e Potencial SIF; Falácia LTI/TRI; Indicadores Antecipadores; Indicadores Reativos; Segurança Pessoal.

Fontes: IOGP 456, 2018; CSB; Energy Institute; Hallowell et al., 2017; EEI, 2024.

Sistema Crítico

Conforme a NT 10/2023 da ANP, sistemas de controle, detecção, alarme ou intertravamento com função de segurança operacional – isto é, sistemas cuja função é prevenir, detectar ou mitigar acidentes operacionais associados a grandes emergências. Inclui, tipicamente: sistemas instrumentados de segurança (SIS, particularmente SIF-*Safety Instrumented Function* de SIL 2 ou superior), sistemas de detecção de fogo e gás, sistemas de controle distribuído (DCS) com funções de segurança, sistemas de combate a incêndio e proteção contra explosão, sistemas de alarme críticos. Constitui uma das três categorias de Elementos Críticos de Segurança Operacional (ECSO), ao lado de Equipamento Crítico e Procedimento Crítico. Os Sistemas Críticos são objeto de Verificações de Elementos Críticos (VECSO) periódicas que confirmam sua prontidão funcional.

Ver também: ECSO; Equipamento Crítico; Procedimento Crítico; VECSO; SIF/SIL; Barreira.

Fontes: NT 10/2023 ANP; Resolução ANP 43/2007 (SGSO); IEC 61511, 2016.

Sistema Sociotécnico (*Sociotechnical System*)

Conceito que articula a inseparabilidade entre componentes sociais (pessoas, equipes, organização, cultura) e técnicos (equipamentos, tecnologia, procedimentos) de um sistema produtivo. O desempenho — e a segurança — emerge da interação entre estes componentes, não da soma de suas partes isoladas. Fundamento teórico transversal das perspectivas apresentadas neste compêndio.

Ver também: Fatores Humanos; Ecossistema de Fatores Humanos; Variabilidade de Desempenho.

Fontes: Trist & Bamforth, 1951; Emery & Trist, 1965.

SPAR-H
(*Standardized Plant Analysis Risk – Human Reliability Analysis*)

Método simplificado de HRA desenvolvido pela NRC (U.S. Nuclear Regulatory Commission) para uso em análises probabilísticas de segurança. Serviu de base para o desenvolvimento do PetroHRA, adaptado para a indústria de petróleo e gás.

Ver também: HRA; PetroHRA; HEP; CREAM; THERP.

Fontes: NRC; IFE, 2022.

STAMP
(*Systems-Theoretic Accident Model and Processes*)

Modelo de acidentes baseado em teoria de sistemas desenvolvido por Nancy Leveson. Trata segurança como problema de controle, onde acidentes resultam de controle inadequado de restrições de segurança ao longo da hierarquia do sistema. Foi projetado diretamente sobre o modelo sociotécnico de Rasmussen.

Ver também: AcciMap; Migração para os Limites; Sistema Sociotécnico.

Fontes: Leveson, 2004, 2012.

T

Tarefa Crítica de Segurança Operacional

Tarefa cuja falha de execução ou omissão possa causar, contribuir ou deixar de reduzir os efeitos de um acidente associado a grandes emergências. Normalmente relacionada a interação humano-máquina com equipamento ou sistema crítico. Ver seção 3.4.

Ver também: ECSO; Procedimento Crítico; HRA; Análise de Confiabilidade Humana.

Fonte: NT 10/2023 ANP.

Teste de Substituição (*Substitution Test*)

Ferramenta para avaliar culpabilidade proposta por Neil Johnston: substituir mentalmente o indivíduo envolvido por outro com qualificações e experiência comparáveis e perguntar se, dado o contexto em que os eventos se desenrolaram, esse novo indivíduo teria se comportado diferentemente. Se "provavelmente não", atribuir culpa não tem papel material — serve apenas para obscurecer deficiências sistêmicas.

Ver também: Cultura Justa; Erro Humano; Racionalidade Local.

Fonte: Reason, 1997.

THERP (*Technique for Human Error Rate Prediction*)

Método pioneiro de análise de confiabilidade humana desenvolvido para a indústria nuclear nos anos 1980. Utiliza árvores de eventos e dados empíricos para estimar probabilidades de erro humano em tarefas específicas.

Ver também: HRA; HEP; CREAM; HEART; SPAR-H.

Fonte: Swain & Guttmann, 1983.

Trabalho como Imaginado (*WAI – Work-as-Imagined*)

Forma como gestores, designers e reguladores pressupõem que o trabalho é ou será realizado. Frequentemente representado em procedimentos, manuais e análises de risco. Difere sistematicamente do trabalho como realizado (WAD), pois não consegue capturar a variabilidade, complexidade e incerteza das operações reais.

Ver também: Trabalho como Realizado (WAD); Lacuna WAI-WAD; Safety-II; Racionalidade Local.

Fontes: Hollnagel, 2014, 2017.

Trabalho como Realizado (*WAD – Work-as-Done*)

Forma como o trabalho efetivamente acontece na prática, incluindo adaptações, ajustes e improvisações necessários para lidar com a variabilidade, incerteza e complexidade do mundo real. A lacuna entre WAI e WAD não é um defeito a ser eliminado, mas característica inerente de sistemas complexos. Compreendê-la é condição para intervenções efetivas.

Ver também: Trabalho como Imaginado (WAI); Lacuna WAI-WAD; Variabilidade de Desempenho; VCP.

Fontes: Hollnagel, 2014, 2017.

Trabalho como Relatado (*Work-as-Disclosed*)

Forma como as pessoas descrevem ou demonstram o próprio trabalho em relatos, relatórios, auditorias, investigações e conversas com quem está disponível. Pode diferir do trabalho realizado (WAD) conforme o contexto de controle, as consequências esperadas e a confiança entre as partes. Tende a se aproximar do que se presume ser esperado (WAI) quando falar das adaptações traz riscos para quem relata. Somando-se ao longo dos níveis hierárquicos, esse filtro produz uma "bolha de otimismo": quanto mais alto o nível, mais favorável tende a ser a leitura do que ocorre na ponta, justamente onde se decidem prioridades e recursos. A distância entre o relatado e o realizado indica, por isso, o nível de segurança psicológica e a qualidade das relações, inclusive entre contratante e contratada.

Ver também: Trabalho como Realizado (WAD); Trabalho como Imaginado (WAI); Lacuna WAI-WAD; Segurança Psicológica; Equipes de Aprendizagem (Tempos de Aprendizagem/LIT).

Fontes: Shorock, 2016; Henriqson, 2026.

V

Variabilidade de Desempenho (*Performance Variability*)

Ajustes que pessoas fazem continuamente para corresponder às condições de trabalho às demandas. Na perspectiva da Engenharia de Resiliência, é normal e necessária, não aberração a ser eliminada — sucesso e falha são produtos da mesma variabilidade. A gestão efetiva busca compreender e canalizar a variabilidade, não suprimi-la.

Ver também: FRAM; Ressonância Funcional; Princípio ETTO; Safety-II.

Fontes: Hollnagel, 2014; Patriarca et al., 2021.

VCP (Verificação de Conformidade com o Procedimento)

Ferramenta de gestão desenvolvida e adotada pela Petrobras para avaliar se procedimentos operacionais estão adequados à execução em campo. Diferentemente de auditorias punitivas, a VCP é dialógica: incorpora o conhecimento do executante, identifica variabilidades do processo e considera experiências do trabalhador para detectar pontos de melhoria no documento — não no trabalhador. Manifestação prática dos princípios de Aprendizagem Operacional e do princípio de que "pessoas não são o problema".

Ver também: Lacuna WAI-WAD; Trabalho como Realizado (WAD); Learning Teams; Aprendizagem Organizacional.

Fonte: Guia Petrobras de Fatores Humanos.

VECSO (Verificação de Elemento Crítico de Segurança Operacional)

Atividade programada para testar e confirmar, com base nos Padrões de Desempenho estabelecidos, se os Elementos Críticos de Segurança Operacional estão desempenhando ou desempenharão sua função requerida quando demandada.

Ver também: ECSO; Guardião da Barreira; Conjunto Solidário de Barreiras (CSB).

Fonte: NT 10/2023 ANP.

Viés de Retrospectiva (*Hindsight Bias*)

Tendência cognitiva pela qual, conhecendo o resultado, simplificamos os dilemas enfrentados pelos praticantes, fazendo parecer que falharam em considerar informações "óbvias" e que a escolha "correta" era cristalina. Distorce análises de acidentes ao fazer ações razoáveis

no contexto original parecerem inequivocamente erradas em retrospecto.
Ver também: Raciocínio Contrafactual; Racionalidade Local; Histórias Primárias e Secundárias; Erro Humano.
Fontes: Woods et al., 2010; Dekker, 2017.

Visão Tradicional (*Old View*)

Perspectiva que vê erro humano como causa primária de acidentes e pessoas como problemas a serem controlados. Baseia-se na premissa de que organizações seriam seguras sem as "falhas humanas". Fundamenta máximas como "segurança é escolha do indivíduo" e "todos os acidentes são evitáveis". Profundamente enraizada na cultura organizacional e no sistema jurídico, persiste mesmo após lições catastróficas de desastres como Macondo e Texas City. O termo *Old View* foi cunhado por Dekker para contrastar com a *Nova Visão* (*New View*).
Ver também: Nova Visão; Safety-I; Erro Humano.
Fontes: Dekker, 2014, 2019; Bruno, 2020.

Z

Zonas de Contato

Pontos de convergência e sinergia entre abordagens do Ecossistema de Fatores Humanos que, apesar de suas especificidades metodológicas, podem ser articuladas de forma complementar. O conceito rejeita a visão de diferentes abordagens como "ilhas" competindo por relevância. Exemplos: HRA com Nova Visão; Investigação de Acidentes com Dependência de Trajetória; HFE com Resiliência; HOP com Cultura Justa. Ver seção 3.1.
Ver também: Ecossistema de Fatores Humanos.
Fontes: Le Coze, 2024; França, 2024.

ABESPetro

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE BENS E SERVIÇOS DE PETRÓLEO

Esta publicação é parte da coleção desenvolvida pelo
GT Fatores Humanos da ABESPetro

Próximos volumes:
Volume 2 – Métodos Analíticos e Ferramentas (novembro 2027)
Volume 3 – Implementação e Casos Práticos (novembro 2028)

www.abespetro.org.br