

Safety Culture, Safety Management, and Resilience Engineering

2009年11月20日ATEC航空安全
フォーラムでの講演スライド和訳版

Erik Hollnagel
エリック・ホルナゲル

E-mail: erik.hollnagel@crc.ensmp.fr

何かうまく行かないことがあると・・・

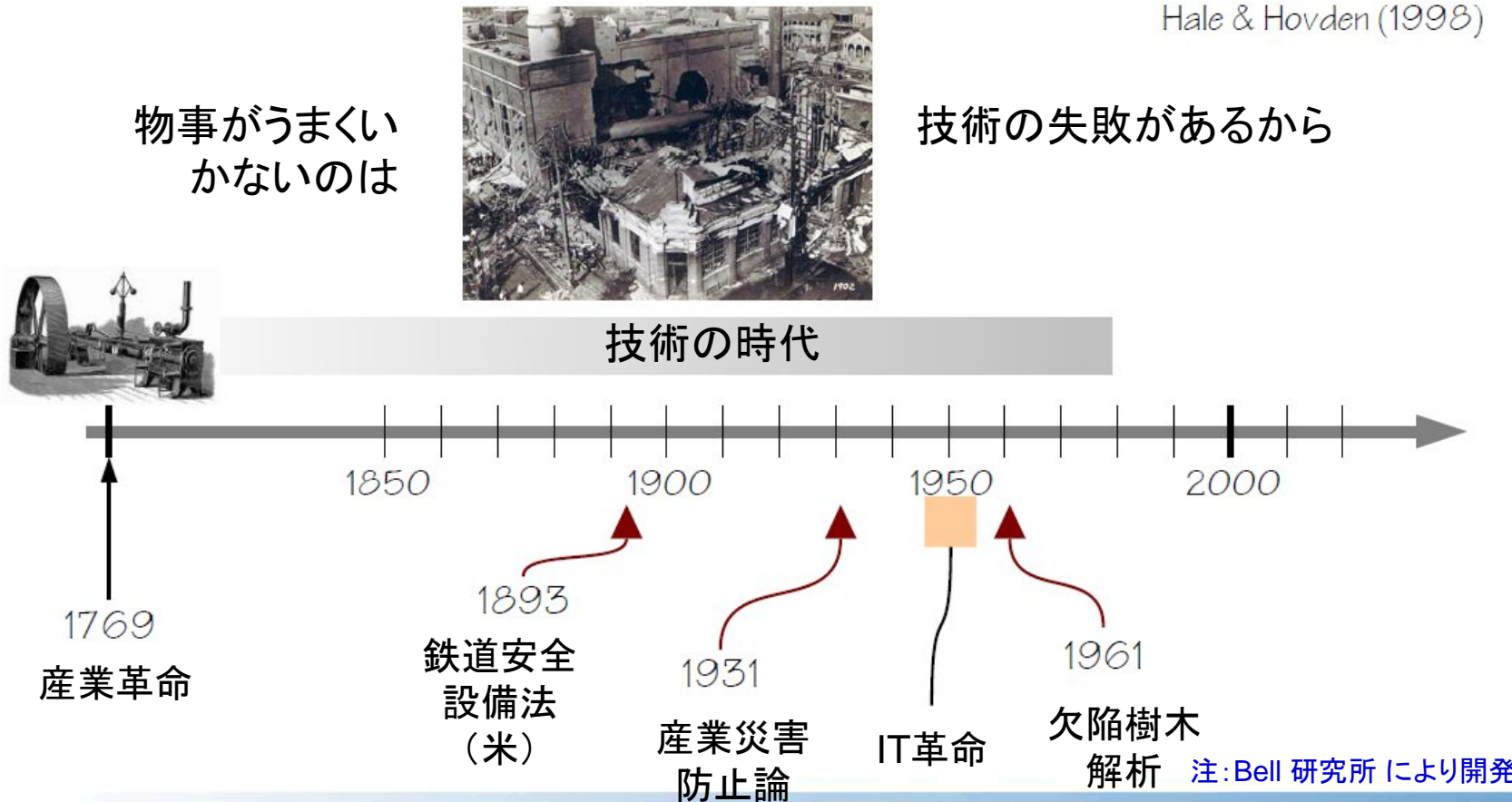
.. 私たちは、原因を見つけようとする・・・時には、まさに「根本原因」を。



産業安全の三つの時代

注: "Perspectives on safety management and change" (Oxford/Peramon 出版 Safety Management 1998年 所収第1章)による

Hale & Hovden (1998)



注: ハインリッヒ Herbert William Heinrich の著 Erik Hollnagel, 2009 年 著 "Industrial Accident Prevention - A Scientific Approach" 初版 1931年発行を指す

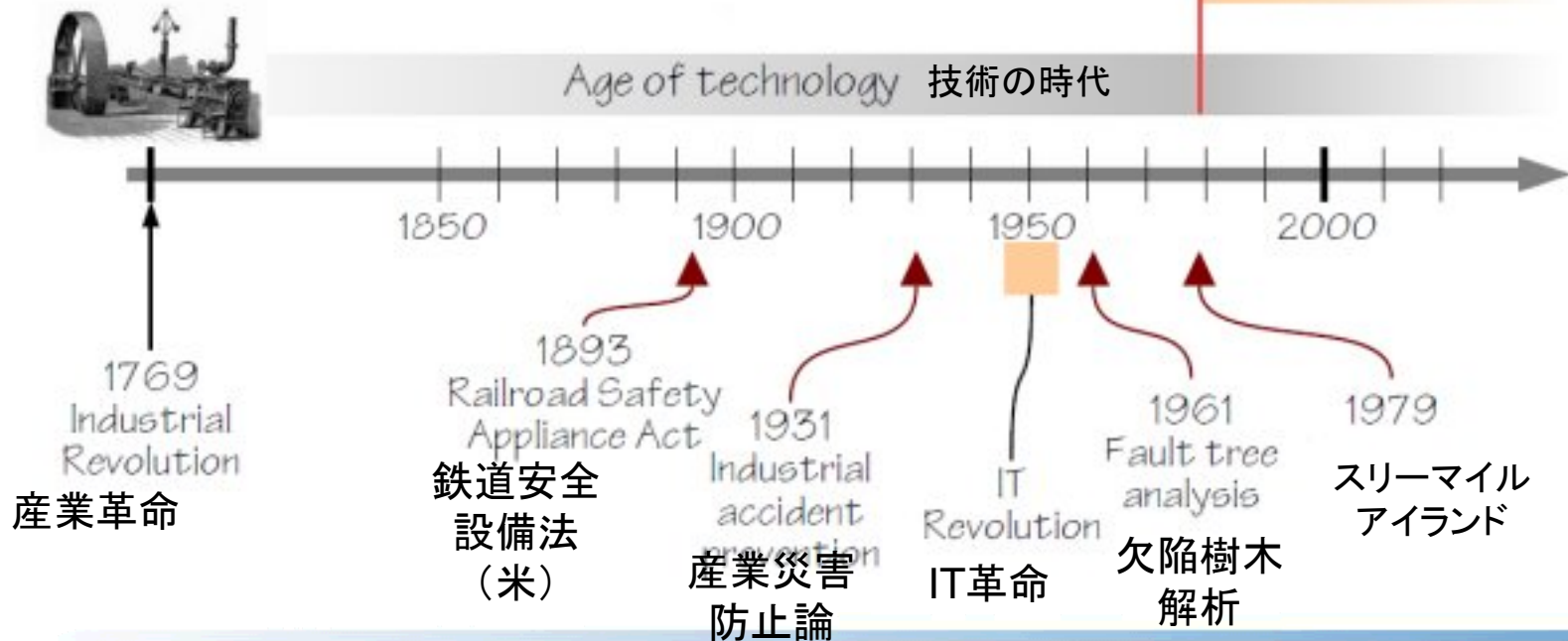
産業安全の三つの時代

物事がうまく行かないのは、
人的要素に問題があるから



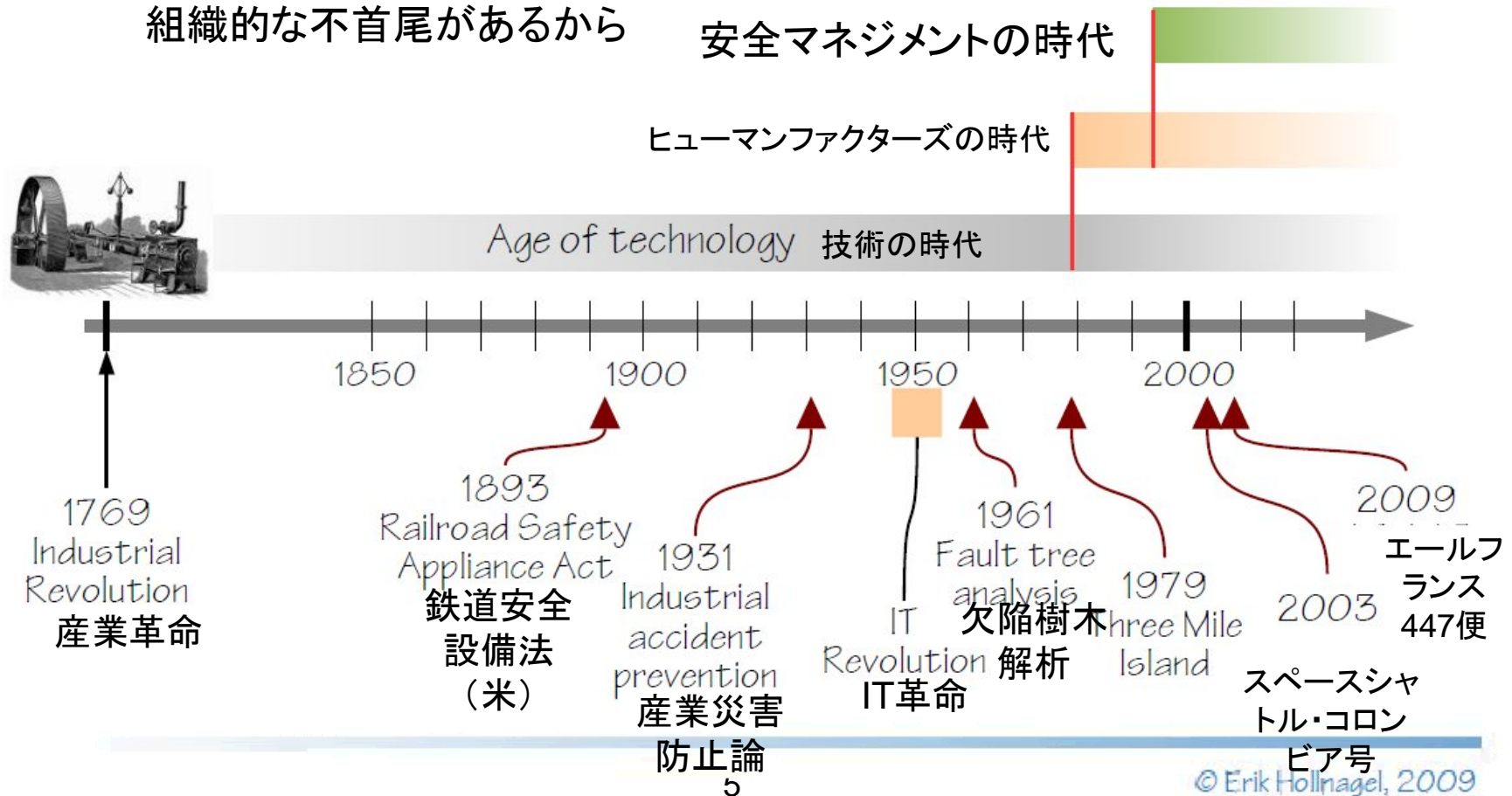
ヒューマンファクターズの時代

Age of technology 技術の時代



産業安全 三つの時代

物事がうまく行かないのは、
組織的な不首尾があるから



安全マネジメントの時代

ヒューマンファクターズの時代

Age of technology 技術の時代

1850

1900

1950

2000

1769
Industrial
Revolution
産業革命

1893
Railroad Safety
Appliance Act
鉄道安全
設備法
(米)

1931
Industrial
accident
prevention
産業災害
防止論

1950
IT
Revolution
IT革命

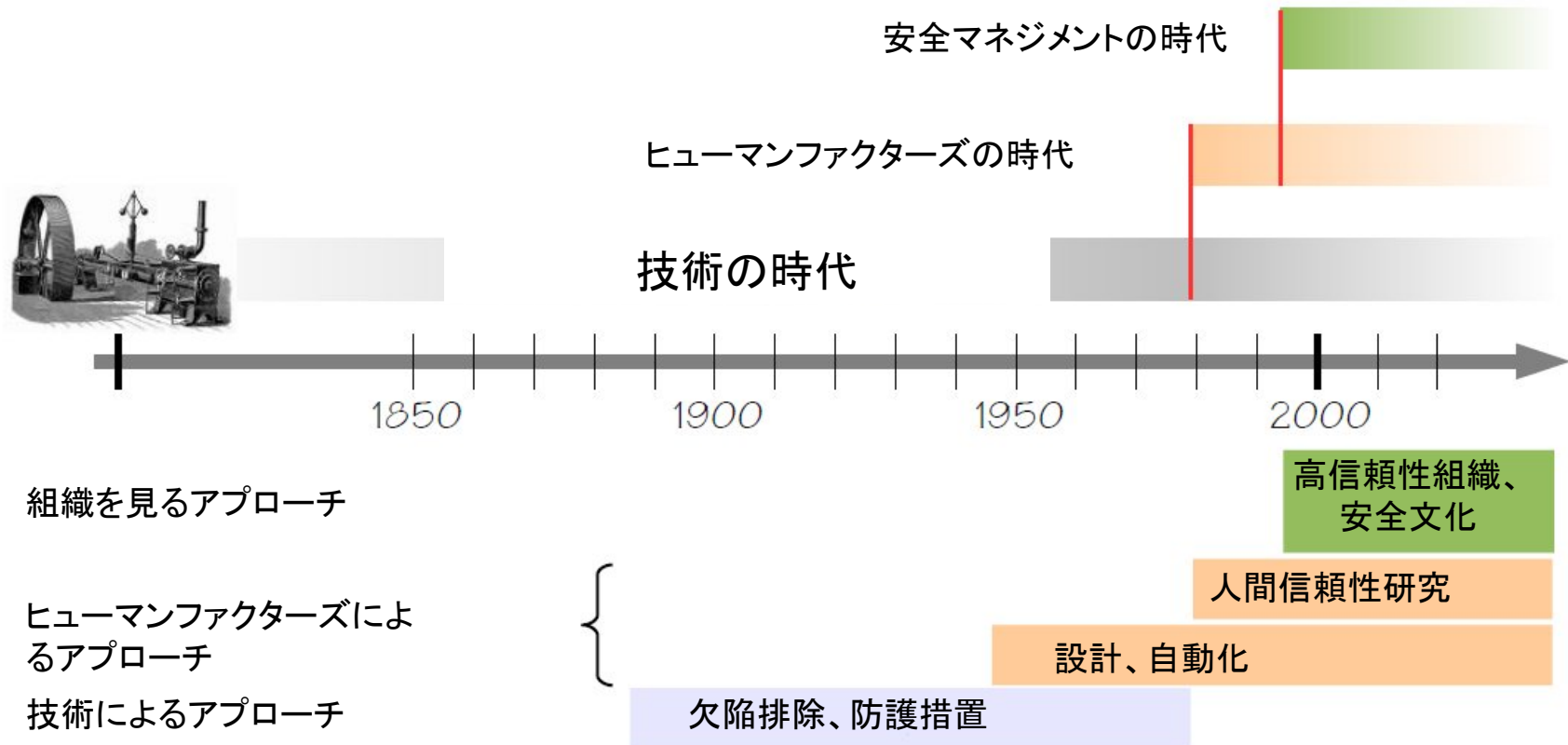
1961
Fault tree
analysis
欠陥樹木
解析

1979
Three Mile
Island

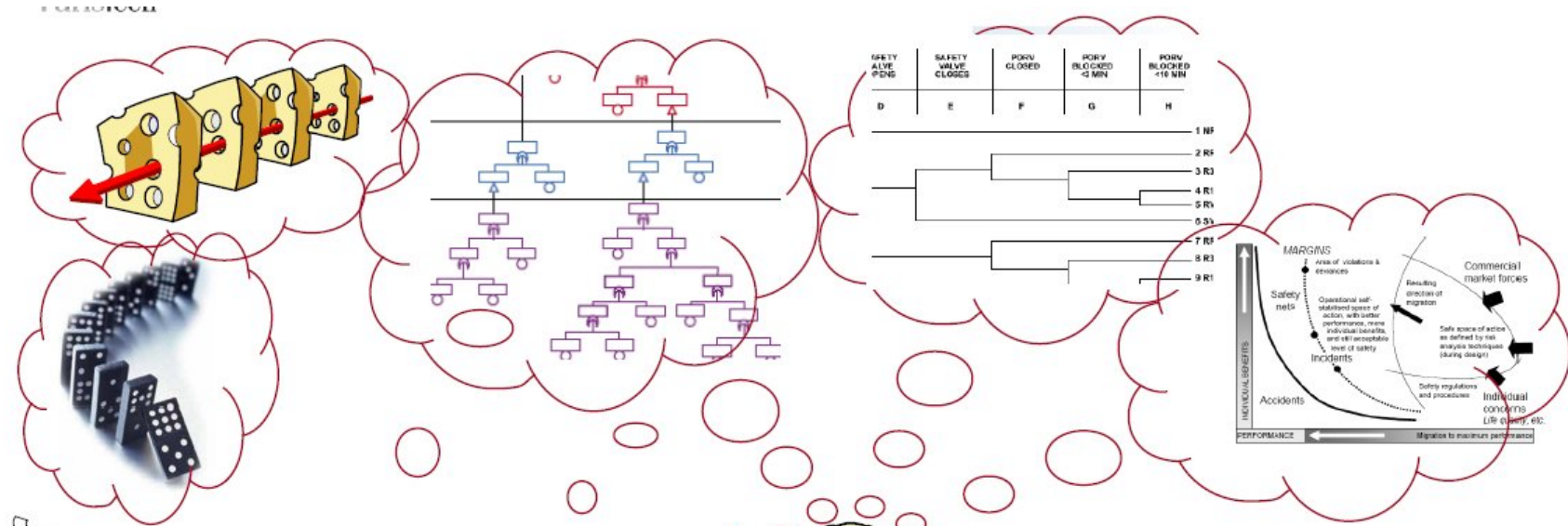
2003
スペースシャ
トル・コロ
ンビア号

2009
エールフ
ランス
447便

人々は一つの原因を求めたがる



何が物事をおかしくするのか、注目の対象



Error

事故の原因は人間。不注意、経験不足、就労態度による。

エラー

故障

Malfunction

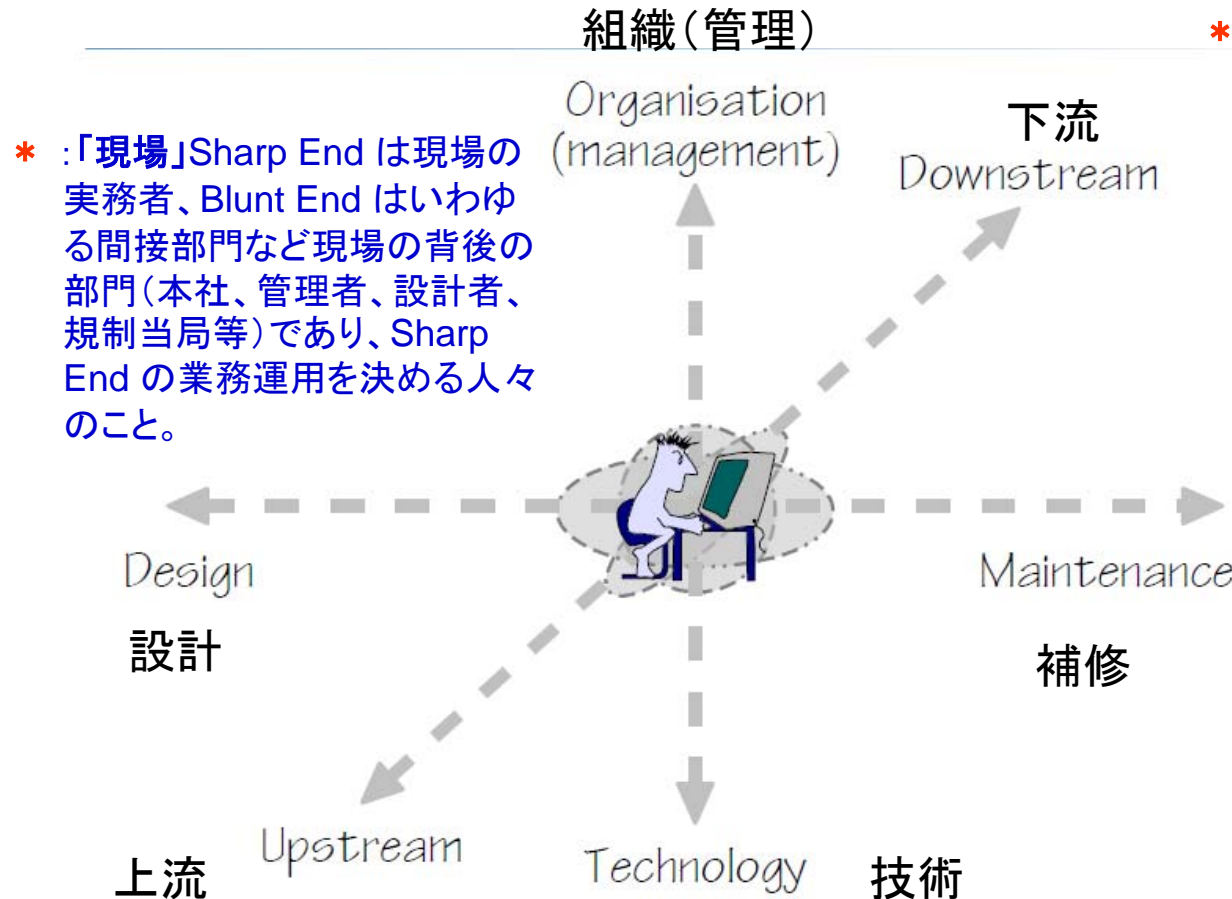
技術と材料が不完全なので故障・破損は不可避



Culture 文化

組織は複雑だが脆弱。組織の記憶は長続きせず、権限委譲の体系が不明確

注目はオペレータに (現場*の実務者、1984**)



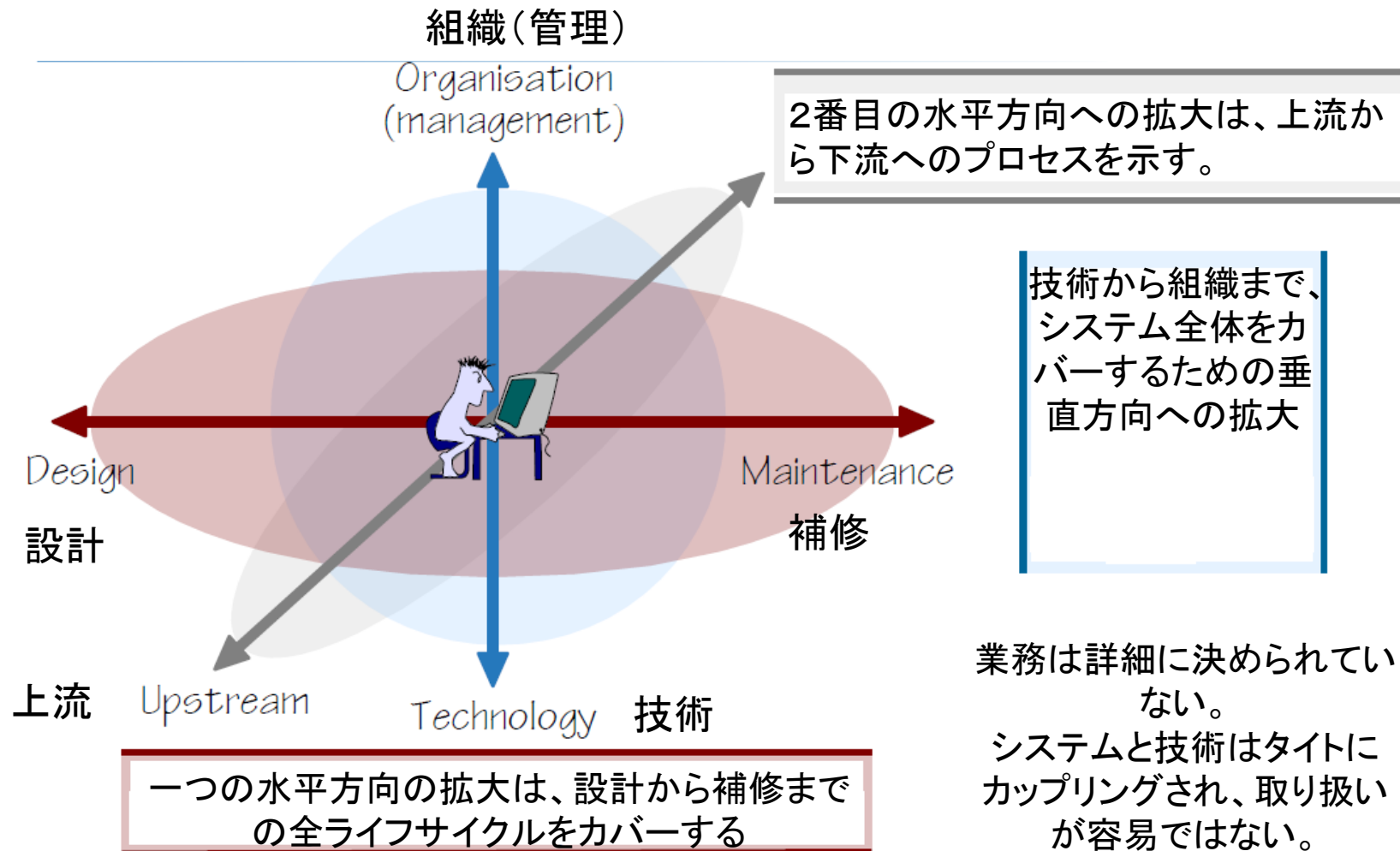
* :「現場」Sharp End は現場の実務者、Blunt End はいわゆる間接部門など現場の背後の部門(本社、管理者、設計者、規制当局等)であり、Sharp End の業務運用を決める人々のこと。

** :年号の1984は、Charles Perrow が “Normal Accident” (「当然の事故」、和訳版なし)の出版年

業務は明確な目的を持ち、細部まで明確に定義のなされた状況で実行された。システムと技術はゆるやかに関係付けられ、束縛関係(カップリング***)が少なく、取り扱いやすい。

*** : Tightly Coupled / Loosely Coupled は、システム基準と運用の幅・余裕、相互の関連性、反応速度によって区分するもの。複雑さと組み合わせてリスクを分類する。Charles Perrow “Normal Accident” 参照。

垂直・水平への拡大 (2009)



安全文化 / 組織の失敗



Chernobyl, 1986

その他の訳:

原子力プラントの安全問題には、その重要性にふさわしい注意が最優先で払われなければならない。そうした組織や個人の特性と姿勢を集約したものである

原子力プラントの安全問題が、最優先でその重要性に応じた注意が払われることを定着させる組織と個人の特性と姿勢の集合

いくつかの甚大な事故により、技術問題、ヒューマンファクター問題に単独で取り組むだけでは安全を保証できないことが明らかになった。

**SAFETY
CULTURE**

安全文化とは



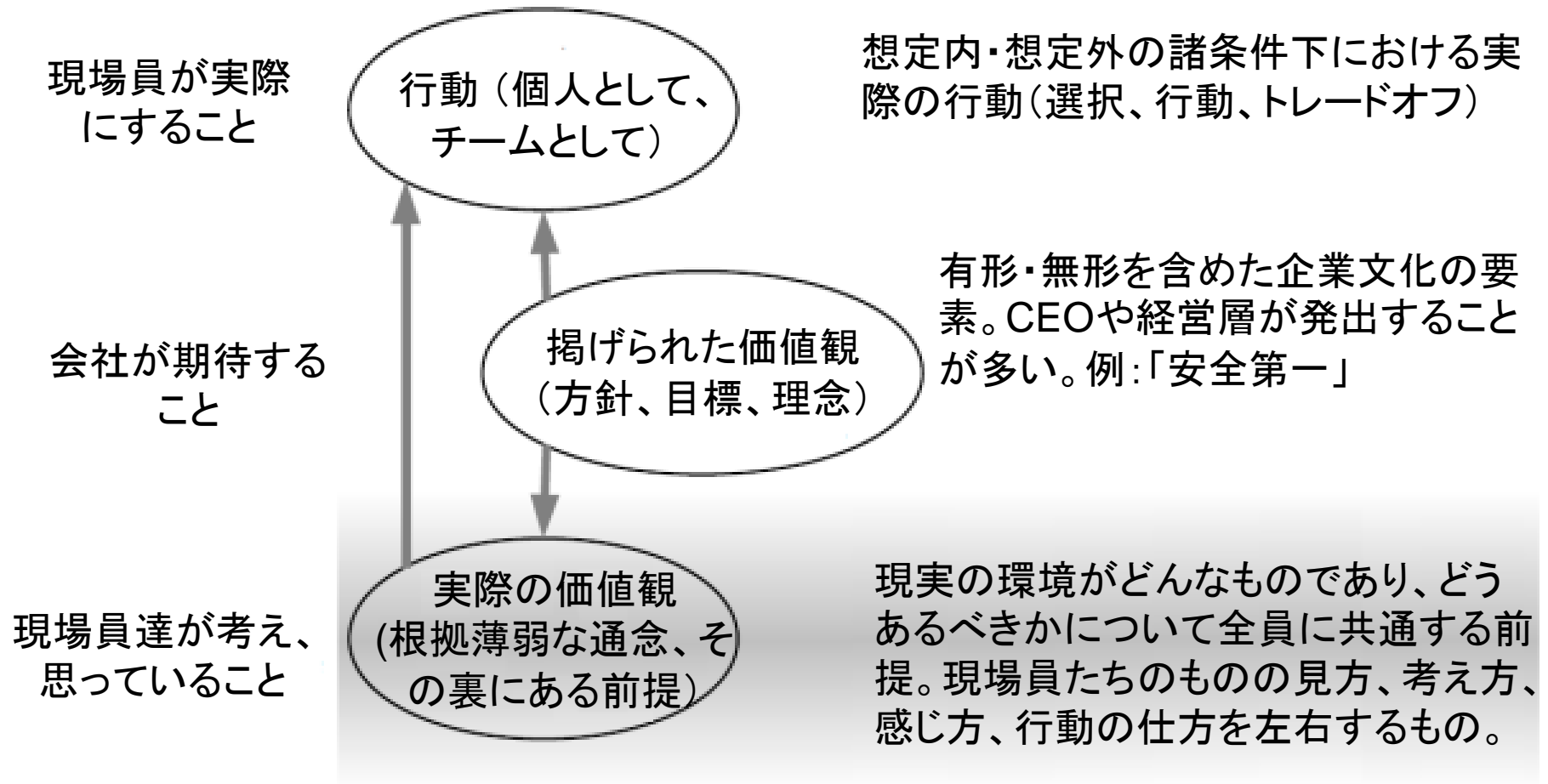
Challenger, 1986

“組織と構成員の特性および姿勢の集合であり、原子力プラントの安全問題が最優先され、その重要性にふさわしい注意を払われることを定着させるもの。”

国際原子力機関・国際原子力安全諮問グループ (INSAG)
報告書INSAG-1 (1986)

安全文化とは何か？

After Schein (1996)



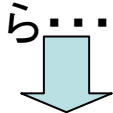
安全文化の段階 (Westrum)

注: Westrum, R による3段階分類 (Pathological, Bureaucratic, Generative) を、ライデン大学 Patrick Hudson が Westrum と共同して5段階に発展させたもの。

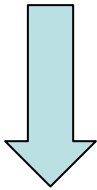
重症	知ったことか。規制当局にばれたり、ひどい事故でも起したりしないうちはね。	勝手気ままに
後追い型	安全について真剣に心配はしているんですけどねー(何もしていませんが)	経営管理層の資源配分ジレンマ
計算づく	前回の事故経験から、発生確率を計算して判断しています。	合理的、経済性を考えて
先取り・予防型	(経営者の姿勢) 良いことは先だってどんどんやれ。結果が出たら教えてくれ。	権限委譲 専門家育成
成長型	安全には全員が取り組んでいます。安全は我が社と我々の誇りです。	あたりまえ 責任

安全性、安全指標、安全文化

安全が、何かおかしくなっていることを、現場員が報告してくれることに依存しているのなら...



...報告する人々が非難を受けないで済むように保護することが必要。



だから、正義の文化が必要とされるのだ。

...安全の実態を測れる手段は、幅広いインシデント報告とその分析プロセスである。インシデントは、イギリス民間航空行政法人CAAの安全規制グループ SRG が運用する義務報告制度 MOR を通じて報告され、報告された事象はNATSが適宜 SRT とともに共同で調査してリスク評価を行う。

NATS (イギリス航空管制公社)は公正な「報告する文化」を守って、安全にかかわるインシデントが引き続き報告され調査できるようにする覚悟である。

NATSは、安全にかかわるインシデントや、現場の気がかり事項が、自由に率直に報告されることを奨励する「正義ある安全文化」の確立に取り組む...

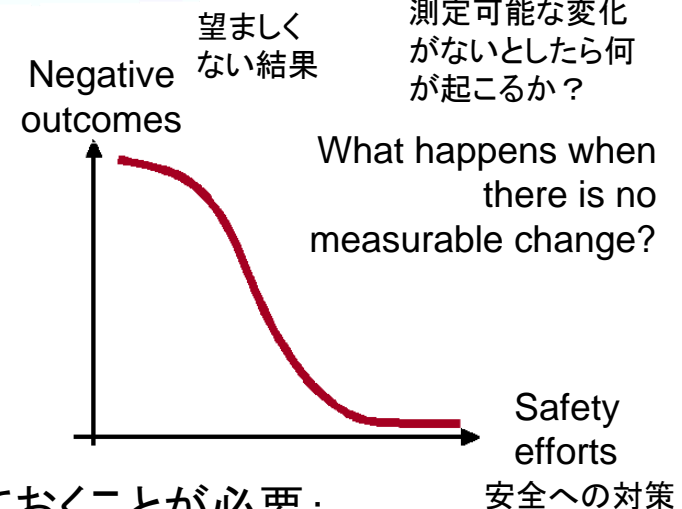
NATS 安全戦略計画 -2004

事故(そのリスク)の排除としての安全

安全水準はふつう、有害な結果が無いことを以て計測される。

有害な結果を無くする方法は三通り:

- ハザードの排除(設計)
- 発端事象の発生防止(抑止手段)
- 発生の影響を拡大させない(防護壁)



安全のためには、以下の二つの違いをはっきりさせておくことが必要:

システムが思った通りに機能して、期待どおりの結果を生み出すことを保証する“ノーマルオペレーション”

ノーマルオペレーションを停止させる、阻害する、または効果を失わせる“アブノーマルオペレーション”

安全マネジメントの目的は、停止や阻害を防止してノーマルオペレーションを継続させることである。安全対策はふつう、過去に起きたことを元に行っているものであり、後追い型、リアクティブである。

安全はプロセスをコントロールするようなもの



プロセス: 既知
目的: 明確に分かっている
管理・制御の対象: 十分理解されている(速度、進路)



プロセス: 既知
目的: 明確に分かっている
管理・制御の対象: 十分理解されている(速度、方位、高度)

安全を維持する



プロセス: 漠然と分かっているだけか、全く理解されてない。
目的: 事故を起こすな(リスクなし)と定められているだけ
管理・制御の対象: ほとんど理解されてない。管理／制御の効果も不明確

安全マネジメントは旅行と同じ

プロセス:

現在地はどこか？（現在のレベルは？）

いままで、どれだけうまく事が運んだか？

目的地（目的）:

次の目的地にいつまでに到着したいのか？／どこまで（目標）、いつまでに到達したいのか？

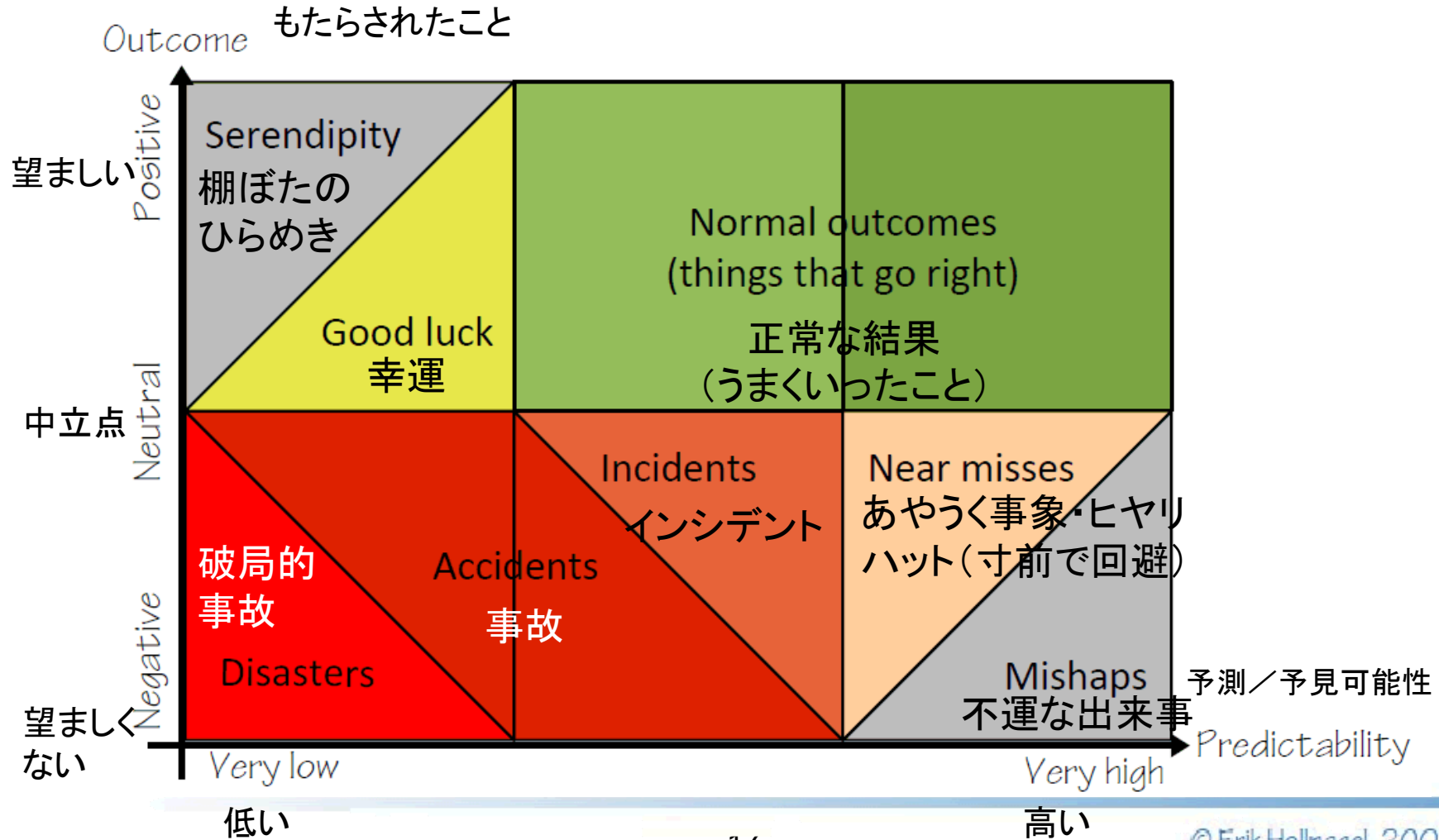
管理・制御:

そこにたどり着くには、どうすればよいか（効果的な手段は？）

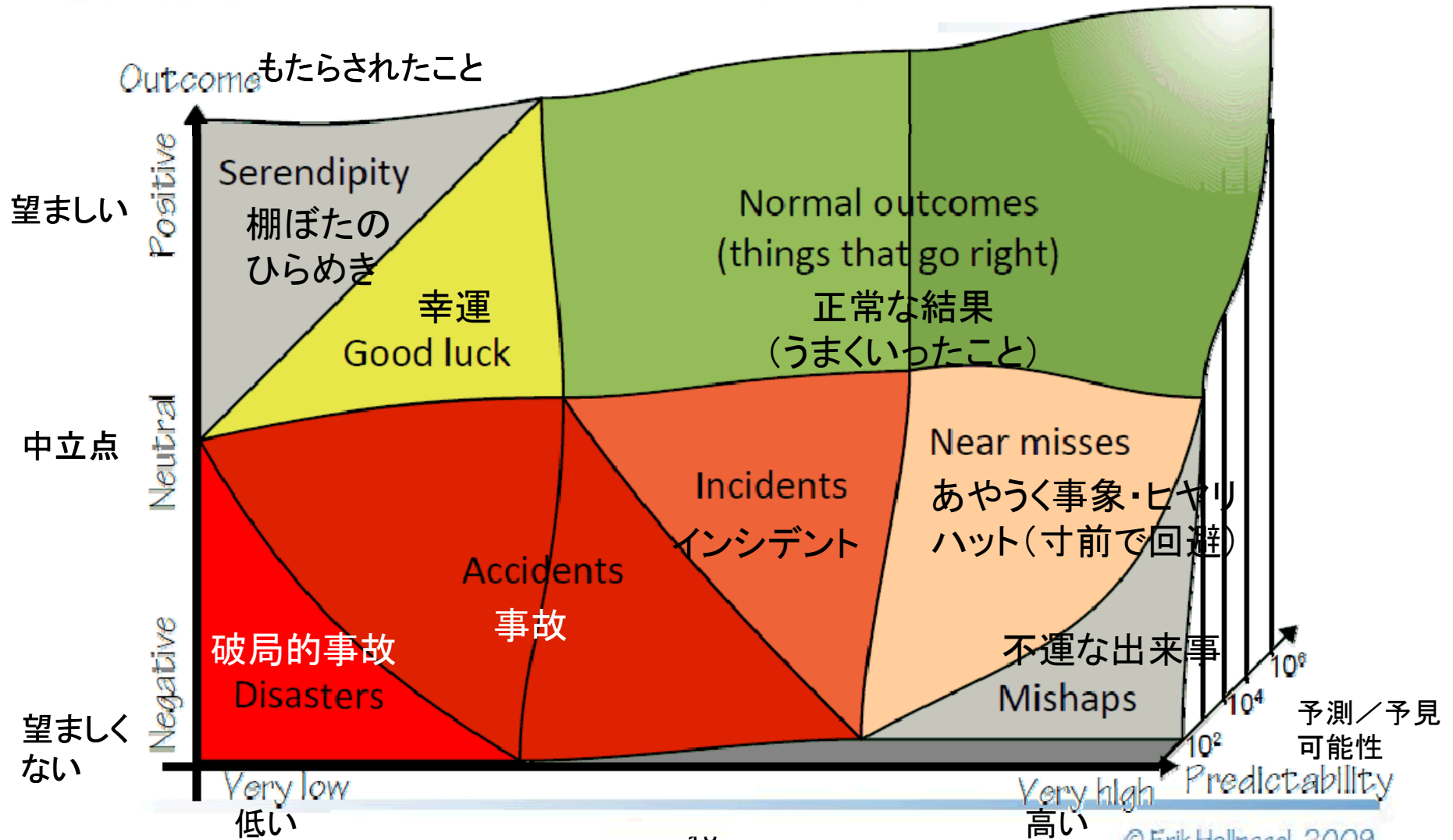
到着までの間に目を光らせておくべき事は何か？



事象発生の結果を分類すると

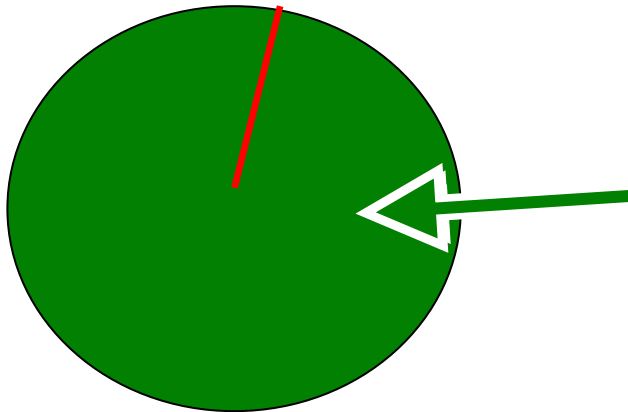


安全であることの頻度に着目



なぜ、うまく行かなかったことだけに注目するの？

10^{-4} := 事象10,000回
に1回の失敗



$1 - 10^{-4}$:= 事象10,000回
のうち9.999回は失敗なし

安全 = 有害な事象を減少させること

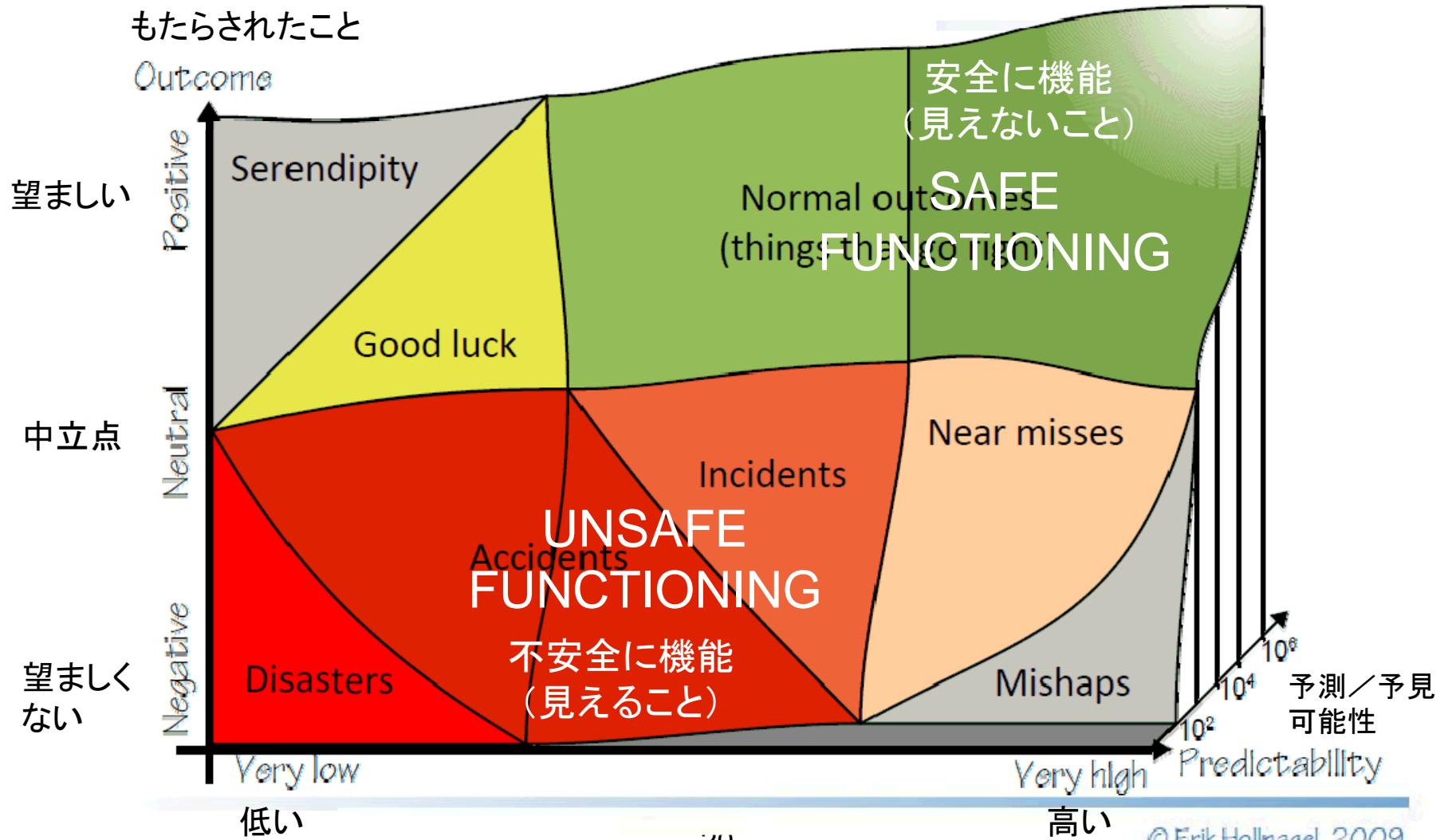
まずい結果(事故)になったことに注目
要因となった失敗と機能不良を探求
(複数)原因の除去と防護壁の改善を追求

安全と本業(コアビジネス)は資源を取り合う関係。
得られるデータのほんの一部を使ってしか、学習しない

安全 = 変動する条件下で成功する能力

うまく行っていることに注目
ノーマルパフォーマンスとして、なぜ成功するのかを理解する
その理解を、業務の改善と安全向上に生かす..
安全とコアビジネスは互いに支援しあう関係
得られるデータの殆どすべてを使って学習

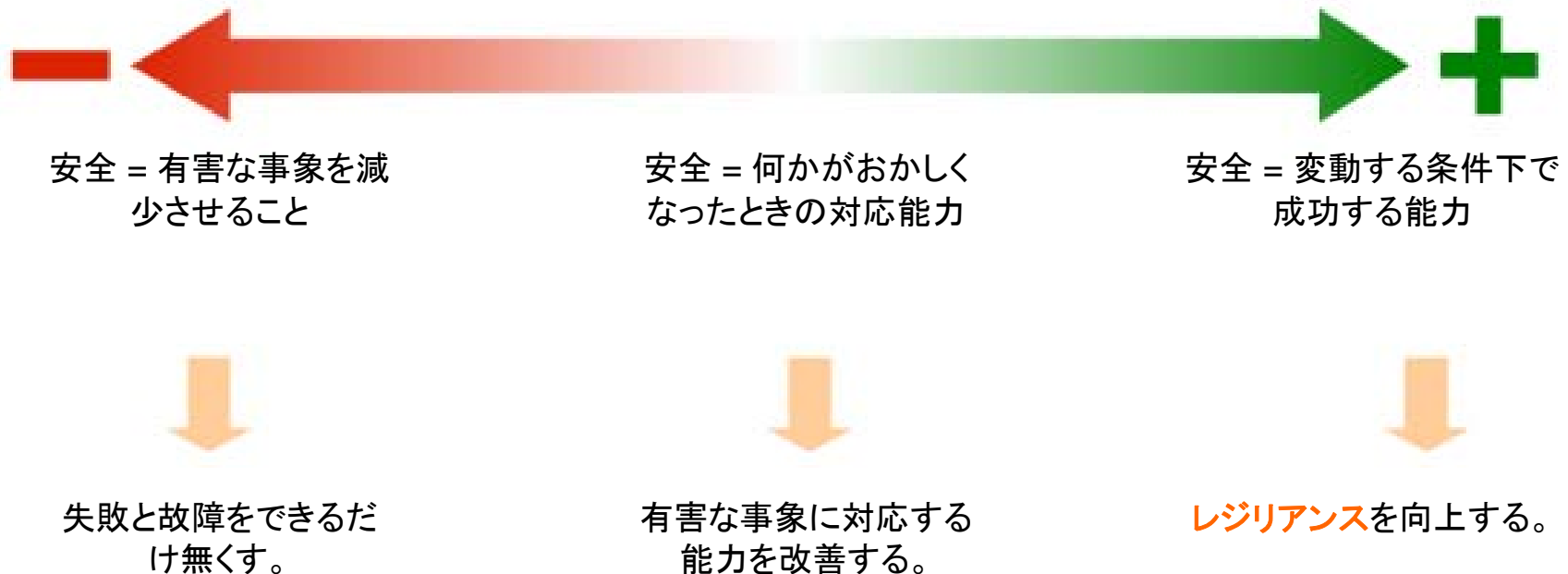
安全であること VS 不安全であること



マイナス面から、プラス面に視点を移す

失敗、故障により悪い結果が生じる

全ての結果(良い結果、悪い結果とも)は、複雑な業務の実施手順が細部まで決めきれなかったり、システムの作動状況や実務者のリソース変動が組み込まれていない(underspecified)ことから必然的に生じる(青字は原文にない補足説明)行動の自由度(performance variability)によるもの。



レジリアンス・エンジニアリングの前提

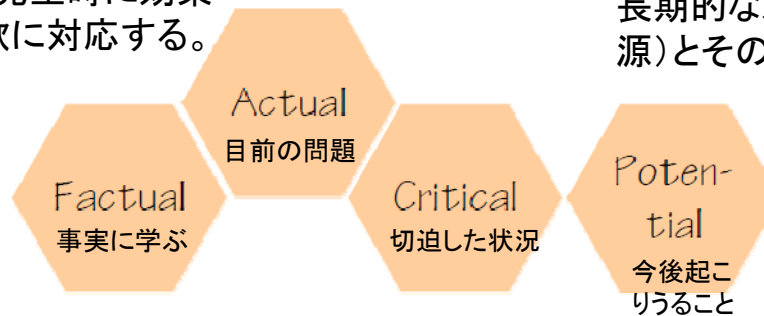
- 業務遂行の条件や環境には必ず不明確さ／決めきれないところが残る (underspecified). このため個人、組織ともに必ず、現況の要件とリソースに応じてそれぞれのパフォーマンスを適合させなければならない。リソースにも時間にも限りがあるため、パフォーマンスの適合は、どうしても、おおよそのところで行くこととなる。
- 事故の多くはシステムの構成要素(部品・要員・ソフトウェア)や通常システムの機能が破損・機能停止・誤作動・機能不良したことが原因と言えるが、それ以外の原因も多い。後者は判断／行動の自由度 (performance variability) が想定外の組み合わせとなってしまう結果と考えられる。
- 「こうすべきだった」という後知恵の批判、エラーを数え上げること、失敗確率の計算などに基づいて安全マネジメントを実行することはできない。安全マネジメントには事後対応だけでなく先取り型の対応が必要。
- 安全は組織にとって本業の業務プロセスと不可分であり、逆もまた真である。安全は生産の前提条件であり、生産は安全の前提条件でもある。安全は制約を設けることではなく、業務の改善を通じて実現されるもの。

レジリアント(柔軟で強靱な)組織

レジリアンスとは、システムが本来的に持っている能力であり、環境変化や外乱に応じてシステム機能を事前に、その最中に、または事後において調整する能力のこと。これにより、想定内また想定外の変動条件下で所要の業務を継続できる。
 レジリアンス・エンジニアリング / 先取り・事前対応型安全マネジメントを実行するには、当該組織の全階層が次のことを実行できなければならない：

通常の、また通常以外の
 状況変化発生時に効果
 的かつ柔軟に対応する。

長期的なスレット(潜在的危険発生
 源)とその生起機会を予測する



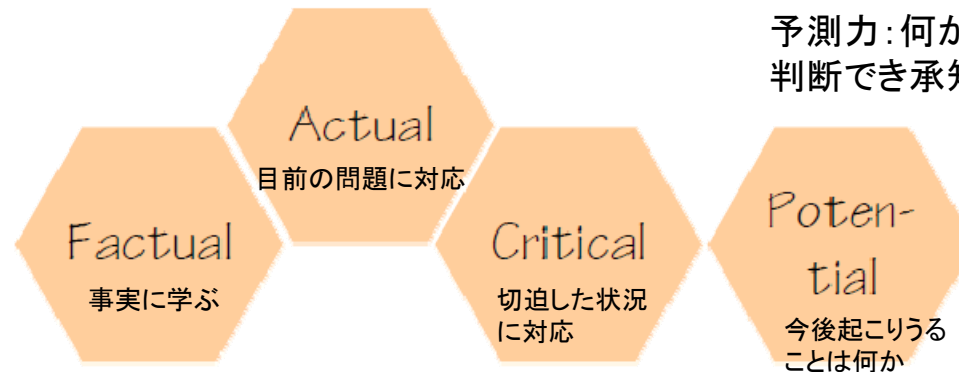
過去の事象から、何が
 起きて何が原因だった
 のかを、正しく学ぶ。

短期的な展開とスレット
 を監視する。リスクモデ
 ルを更新する。

レジリアンスをデザインする



即応力:何をすべき
か分かり、対応する
実行力がある



予測力:何が起こりそうか
判断でき承知する。



学習力:何が発生し
たか理解する。

監視力:何に眼
を光らせるべき
か分かる。



これらを組織の全階層で実行できる能力と信頼度を向上することにより、安全向上と管理能力の向上を同時に実現でき、予測・計画・生産の力量が強化できる。

効率性と完璧さのトレードオフ(ETTO)

完璧さ: 考えるための時間
状況を把握する
オプションを選択し、計画する

完璧さに徹すると、実行の時間
が不足する結果になること
がある。

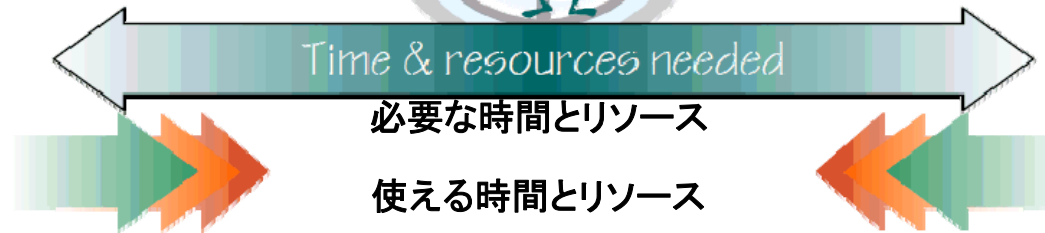
急を要する措置を見過ごす
新たに生じた事象に気づかない



効率性: 実行のための時間
計画を実行に移す
計画項目を実行する

効率性に徹すると、実行したいこと
のお膳立てが整ってなかったり
計画が不適切であったりする。

前提条件を見落とす
見たい結果だけしか見ない



よく見受けられる ETTO の経験則

認知面 (個人)

状況が不明確な中での
判断

本能的認知傾向
(Similarity Matching –
Frequency Gambling)

入力情報への対処方法

ワークロード過大、過小

認知のスタイル

確認バイアス(類似性、
経験頻度等による)



個人特性 (作業関連)

良いんじゃないの

大したことじゃない

たいてい大丈夫。チェック不要

何百回もこうやってきた

誰かがチェックするだろう

この方がずっと早い

いまやる時間(or リソース)が無い

やり方を忘れた

ここではいつもこうしている

Xらしい(だから X に違いない)

とにかくやりとげなくちゃ

期限に間に合わせなければ

X(資源)をあまり使っちゃいけない

集団として (組織)

最悪事態になったことし
か報告しない

冗長性/バックアップを
低下させる

「生産目標」を達成

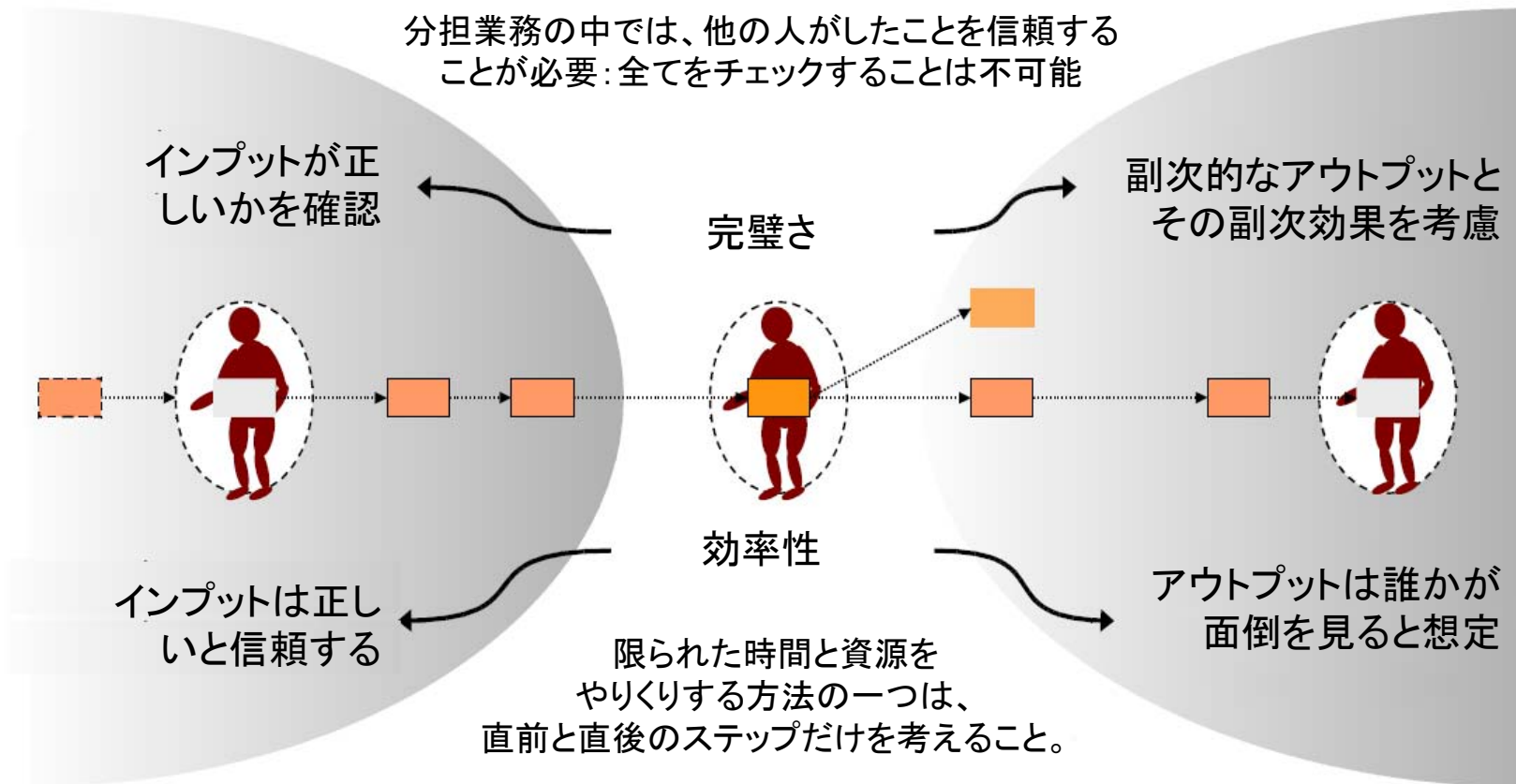
不要なコストの低減

板挟み

不都合な情報を無視

Similarity matching, Frequency gambling – 認知したものを記憶の中のパターンと
対比して解釈するやりかた。「似ているからきっとこれ」「よくあるあれか」といったこと。
いずれも James Reason “Human Error” 第4章参照。和訳版「ヒューマンエラー」(林
喜男監訳 海文堂)では「類似性による照合」、「頻度による賭」とされている。

効率性と完璧さのトレードオフ (ETTO)



ETTO 原理

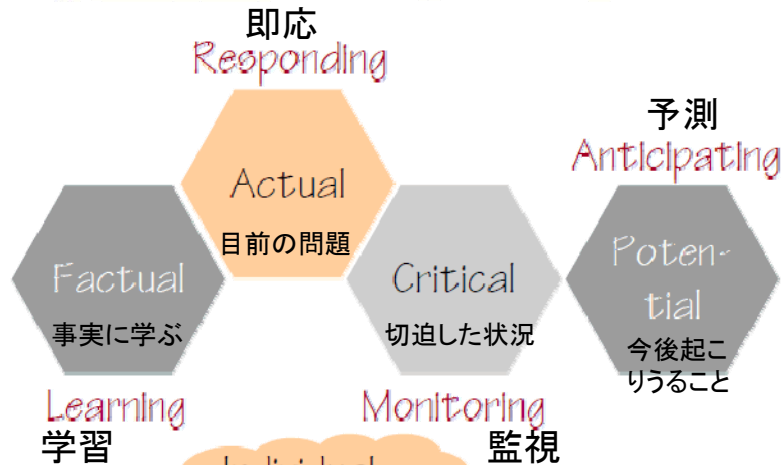
ETTO原理が語ること — 人々(と組織)が活動の一部として必ずと言えるほど、活動の準備に費やすリソース(時間と労力)および活動の実行に使うリソース(時間・労力・材料)のトレードオフを判断することが必要だという事実

もし生産量や出来高が主要な関心事なら、ETTOすることは完璧さより効率性に重きを置く。安全と品質が主な関心事なら、効率性より完璧さが上に来る。

ETTO原理から言えることとして、完璧さと効率性を同時に最大化することはできない。またどちらも最低限が存在しないと、どんな活動も成功は期待しがたい。



レジリアンスと個人がすること



個人のETTOルール ...



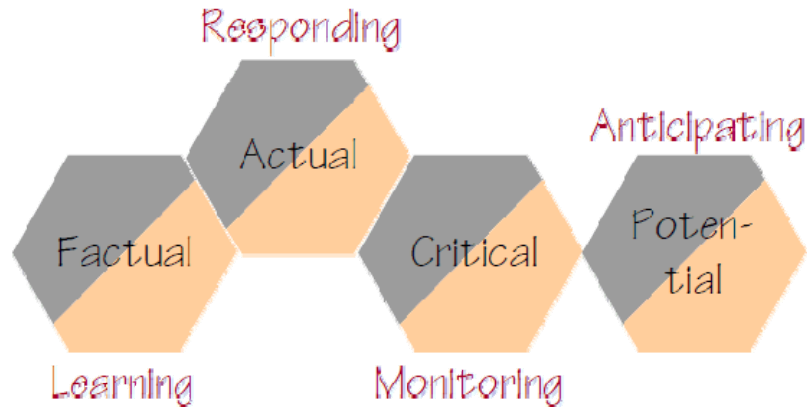
Individual ETTO rules

良いんじゃないの
大したことじゃない
たいてい大丈夫。いまチェックは不要
何百回もこうやってきた
誰かがチェックするだろう
誰かがもうチェックしてある

一人一人が4つの能力全てを均等にこなすことはできないので、ふつうは優先度を付けて対処する。
ETTOすることは、4つの能力への配分バランスに影響をあたえるだろう。

この方がずっと早い
いまやる時間(or リソース)が無い
やり方を忘れた
ここではいつもこうしている
Xらしい(だからXに違いない)
とにかくやりとげなくちゃ(期限までに仕上げる)
X(資源)をあまり使っちゃいけない

レジリアンスと組織がすること

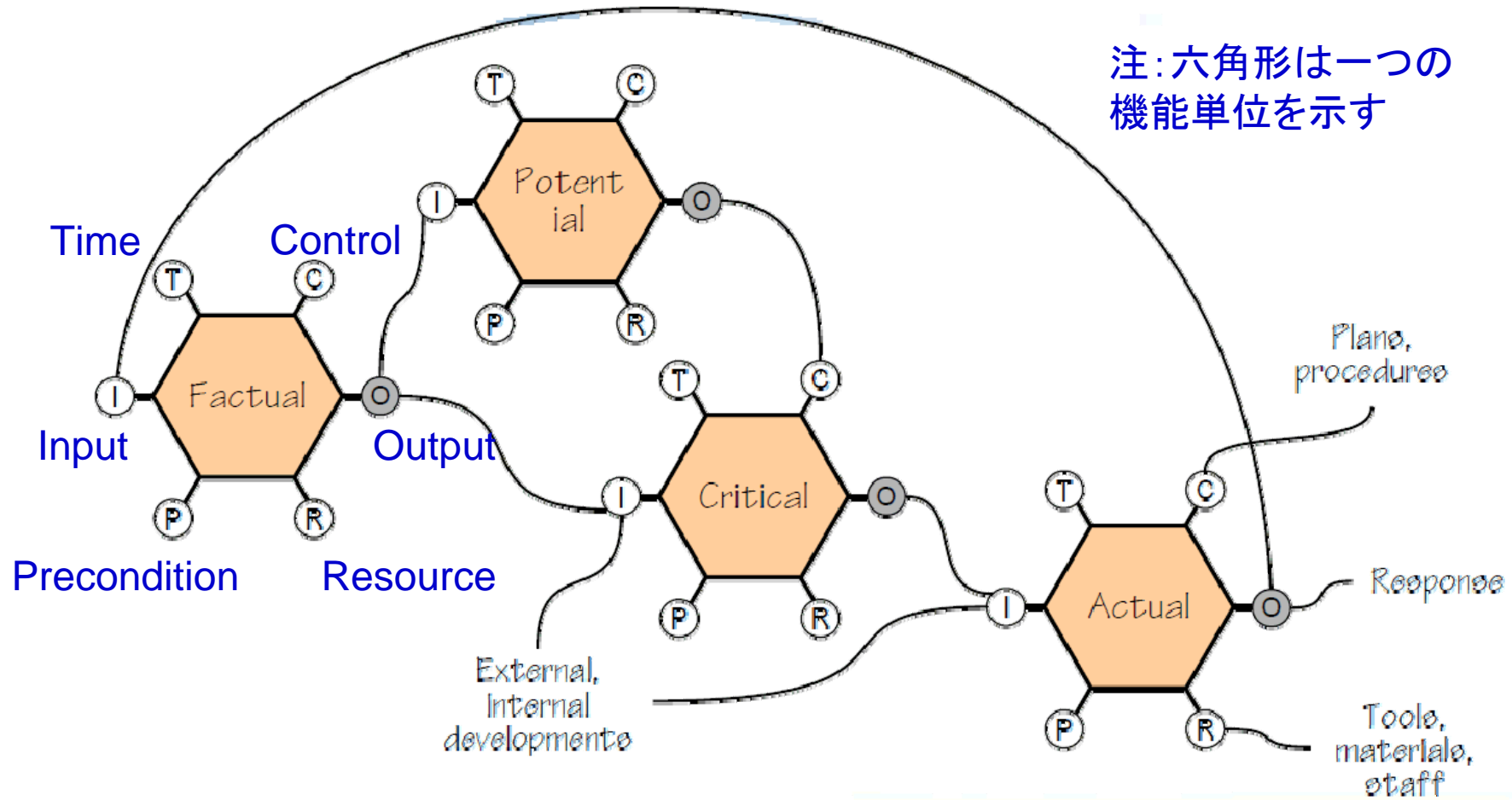


組織はその優先度に応じて4つの能力・機能全てに資源を投入できる。ETTOすることは、どの機能にどこまで取り組めるかの配分バランスに影響を与える。

組織又は集団の
ETTO ルール

冗長性／バックアップを低下させる
板挟み(やれ、と、やるな、の間で)
不都合な情報を無視
不要なコストと作業を減らす
「生産目標」を達成(「安全最優先」、しかし・・・)
ネガティブ報告(最悪自体になったことしか報告しない)

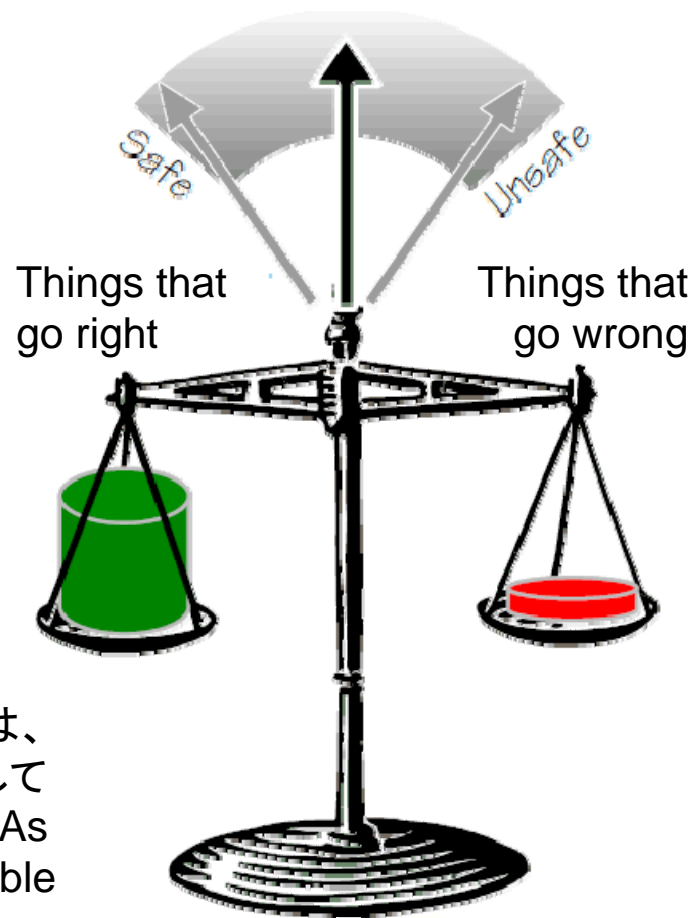
4つの能力の相互依存関係



注:六角形は一つの機能単位を示す

レジリアンスをマネージする

レジリアンス・マネジメント
の到達目標は、うまくいく件
数を増やすこと・・・

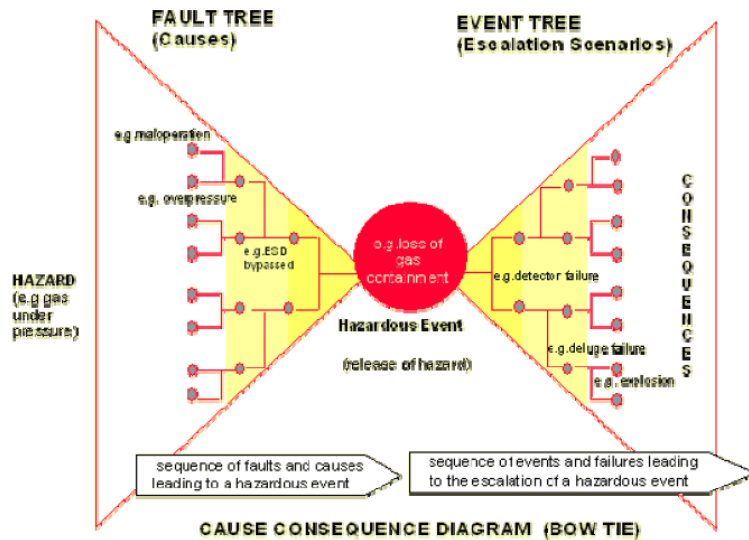


・・・まずい結果(事故など)の
数を減らすことよりも

レジリアンスエンジニアリングは、
失敗への着目ではなく全体として
のパフォーマンスに着目する。As
Low As Reasonably Practicable
/ALARP ではなく、As High As
Reasonably Practicable
/AHARP が目標になる。

既存のツールや技法の多くは
引き続き使えるが、新たな視点
の下で使うことになる

安全マネジメントへの二つの見方



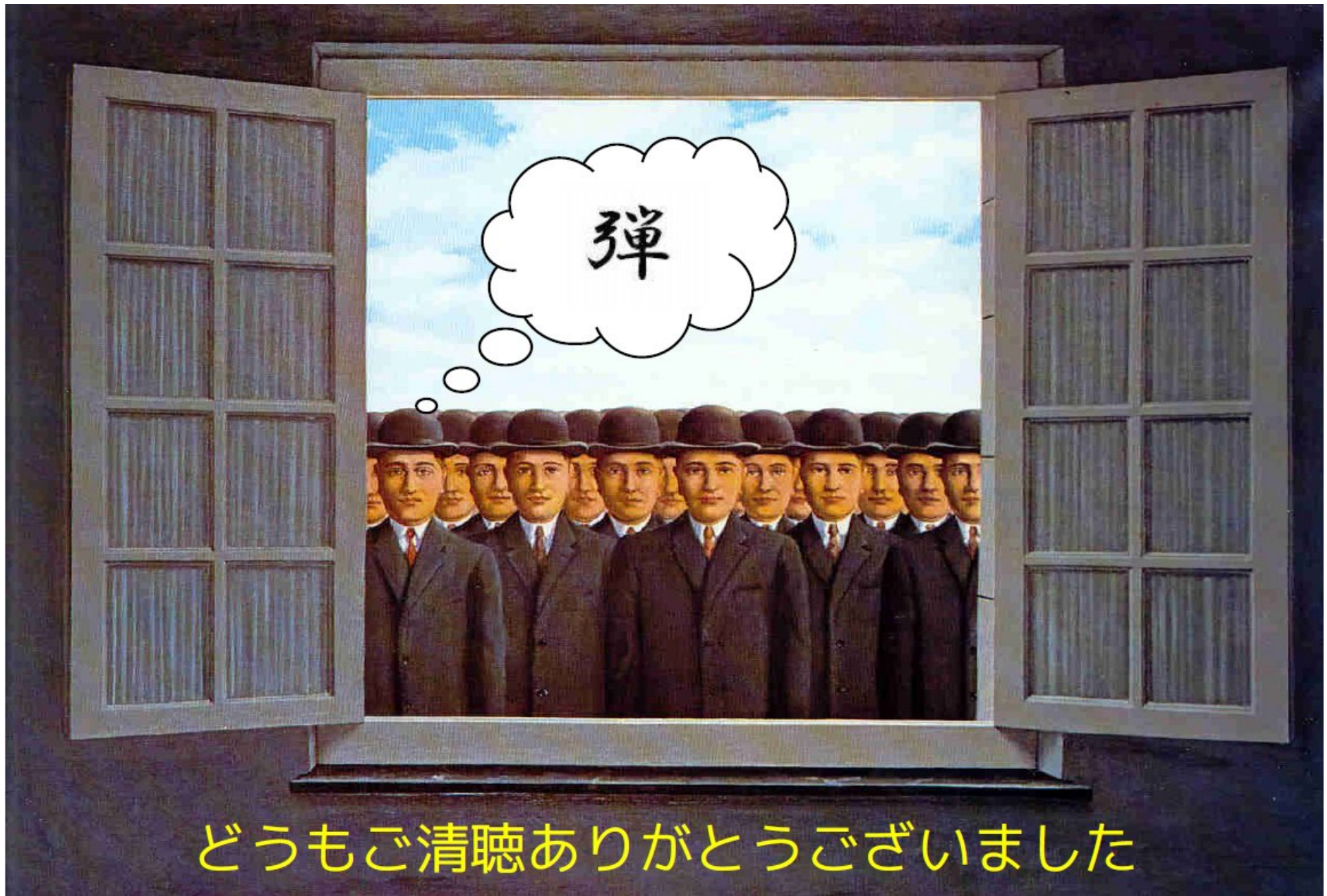
従来の安全マネジメントは、細かく辿っていく(構造化)モデルを使う。狙いは有害な事象を減らすこと。活動の焦点は、何かの再発を防止すること(弱点の是正、防止、防護)

注:この図は通称Bow-tie(蝶ネクタイ)モデル。左半分は故障の木解析FTA、右半分が発生事象モード解析ETAで構成される

レジリアンス・エンジニアリングは自明でない(機能中心の)モデルを使う。ねらいは、変動する条件下で成功する能力を改善すること。活動の中心は組織の即応力・監視力・予見力・学習力を増強すること。

宮本武蔵:目に見えぬ所をさとってしること(五輪書、地の巻)





どうもご清聴ありがとうございました