

シンビオ講演会 (2021.5.18)

プラント分野への
レジリエンス・エンジニアリングの応用のための
今後の研究課題

岡山大学 大学院ヘルスシステム統合科学研究科
五福 明夫

Erik Hollnagel先生 2013講演スライド
より

RESILIENCE ENGINEERING:
FROM SAFETY-I TO SAFETY-II

回復力

ERIK HOLLNAGEL, PROFESSOR, PH.D.
WWW.ERIKHOLLNAGEL.COM

© Erik Hollnagel, 2013

Resilience and safety management



A system is resilient if it can adjust its functioning prior to, during, or following changes and disturbances, and thereby sustain required operations under both expected and unexpected conditions.

This requires that all levels of the organisation are able to:

Respond to regular and irregular conditions in an effective, flexible manner,

Anticipate long-term threats and opportunities



Learn from past events, understand correctly what happened and why

Monitor short-term developments and threats; revise risk models

背景：福島第一事故の教訓と新規制規準

□ 福島第一事故の教訓

■ “想定外事象”への備えの困難さ

- 想定を超える津波高さ
- 「冷やす」 ↔ 「閉じ込める」

■ 超人的で献身的な所員の活動が被害を軽減

- 本質を踏まえた対応
- 機転によるアイデア

□ 原子力プラントの新規制基準

■ シビアアクシデント対策やテロ対策の6項目の基本方針

- 『ハード（設備）とソフト（現場作業）が一体として機能を発揮することが重要であり、手順書の整備や人員の確保、訓練の実施等も要求』

□ 原子力白書（令和元年度版）

- 更なる安全性向上における人材の重要性が意識された編集
-

脅威とレジリエントなシステム

□ 基本的視点

- 脅威の予測可能性
- 脅威がシステム混乱に導くポテンシャル（可能性）
- 脅威の起源（内部または外部）

□ 擾乱要素

- 自然要素，社会要素，技術要素，人的要素

□ 対応のアプローチ

- **ロバストネス**：強固な備えにより安定を維持し続ける
- **レジリエンス**

- 『1つのレジリエントなシステムは，1つの混乱や1つの大きな災難の後の連続的なストレスの存在の下で，それが要求されたように振る舞い続けられるように，それが持っている機能を変化や外乱の前，最中，後に効果的に適応できる』 [Hollnagel2013]
-

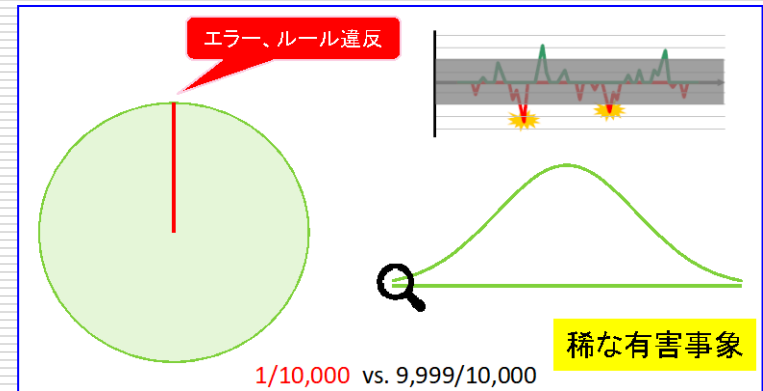
不測の事態への2通りの対応方針

- 不測の事態自体を減らす（想定事象を増やす）
 - 想定事象：本発表では、「起こり得ると想定される事象」
 - 困難さ
 - 全ては想定できない
 - 全ての想定事象に対策は施せない
人工物にはEngineering Judgementにより対策をしない
想定事象がある
例：隕石の落下
- 致命傷とならないように柔軟に対応する
 - 代替案の発想と実施
 - 例：原子炉を「冷やす」ための海水注入
自動車用バッテリーを直列接続して計装用電源に
消防車を直列につないで必要な水頭圧を得る
 - 許容できる被害で止める
 - 例：格納容器ベントによる減圧

Resilience Engineeringが与える新しい視点

□ 日常の良好行動に着目 (Safety-II) : 正常状態を増やす

- これまでは異常事象 (事故事例) のみ着目: Safety-I
 - 異常事象は稀
 - 大成功と同じ構図
 - システムが正常に動作するための現場の働きかけ (良好行動) が常にある



□ 現状を深く理解 (WAD)

- これまでのプラント業界 (特に原子力業界) は, 理想的状态 (WAI) を追求
- 規則に厳密に従うことを強要
- 現場の状況は時事刻々と変化
 - 同じ状況は無い
 - 現場要員は柔軟に対応

Work-as-imagined (formal work) is what designers, managers, regulators, and authorities assume happens or should happen.

Work-as-done (actual work) is what people have to do to get the job done. It is what happens in everyday practice.

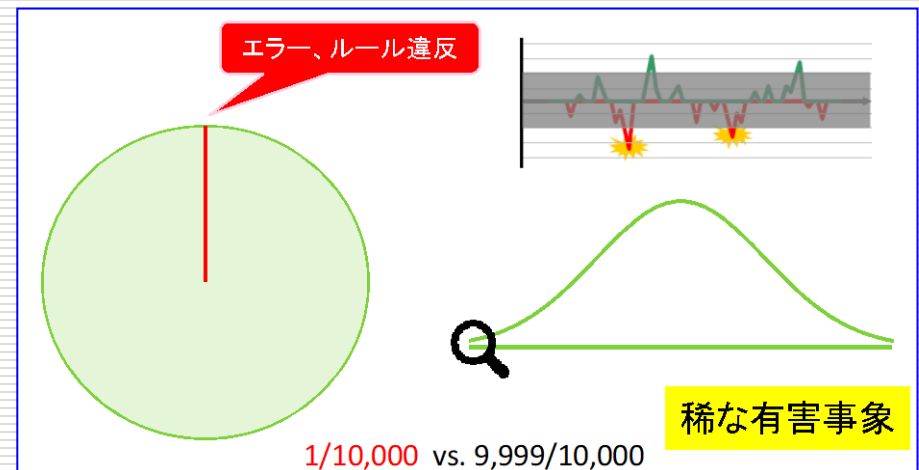
The Most Advanced Hospital Manual of Clinical Nursing Procedures
Edited by Linda Dougherty and Siera Lister

Work-As-Imagined will always be different from Work-As-Done. It is important for Resilient Health Care to accept and understand this difference.

© Erik Hollnagel, 2014

Safety IIによる安全対策

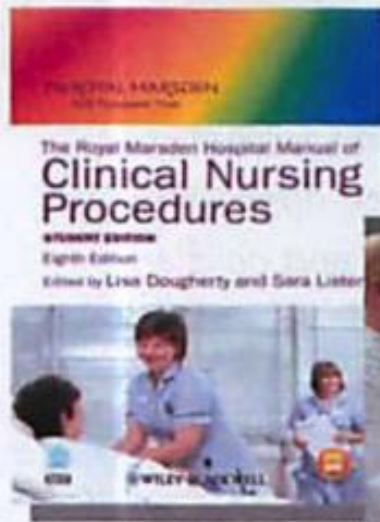
- Safety I : 異常状態（事故）を減らす
 - 従来の方考え方
 - 異常原因を追求しその発生を防止する手段を講じる
- Safety II : 正常状態（良好事例）を増やす
 - 日常がうまくいっている要因を追求して異常時に柔軟に対応する能力を身につける（方策を見つける）
- レジリエンス・エンジニアリングでは, Safety Iに加えて Safety IIの重要性を強調



Work As ImaginedとWork As Done

- 想定されている行動 (WAI) と実際の行動 (WAD) は異なっている

Work-as-imagined (formal work) is what designers, managers, regulators, and authorities assume happens or should happen.



Work-as-done (actual work) is what people have to do to get the job done. It is what happens in everyday practice.



Work-As-Imagined will always be different from Work-As-Done.
It is important for Resilient Health Care to accept and understand this difference.

レジリエントのための4能力と補完的要件

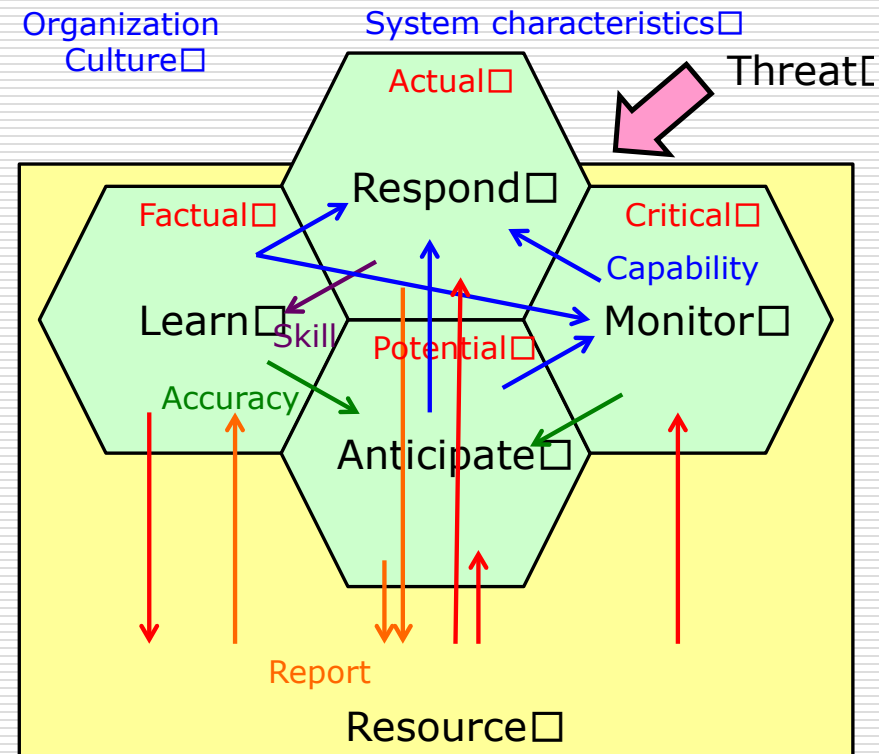
□ Resilience Engineering : 安全を脅かす事態が事故やインシデントに結びつかないように「しなやかに」対応する方法論

□ 4能力

- Respond : 何をすべきか
- Monitor : 何を探索すべきか
- Learn : 何が起こったか
- Anticipate : 何を予見すべきか

□ 補完的要件[北村2012]

- リソースを管理する
 - 機器や装置, 資材, 予算, 人員など
 - 対処のために事前に用意
 - 状況に応じて適切に配備
- プロアクティブ (Proactive) な行為選択ができる



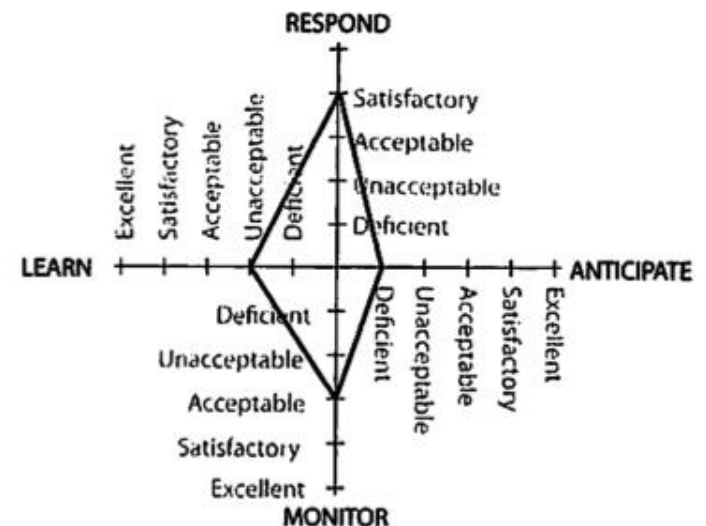
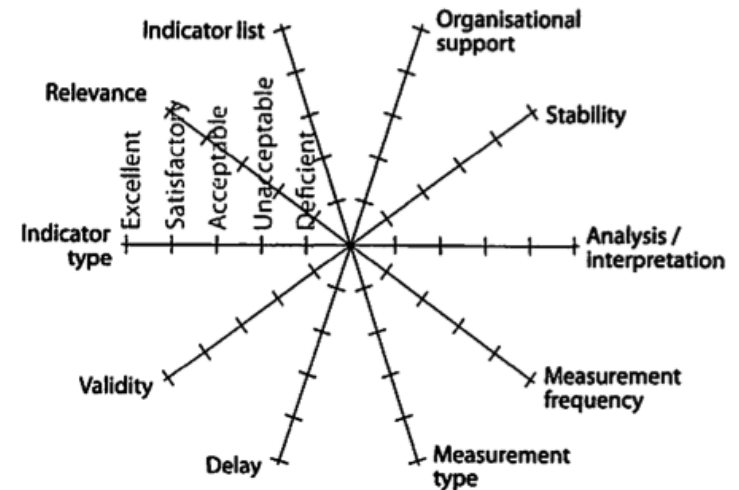
RAG : レジリエンスを評価 [Hollnagel2011]

□ Resilience Analysis Grid

- Resilience Engineeringが求める能力のレベルを測定する質問群

□ 定性的評価

- 優秀な (Excellent)
- 満足する (Satisfactory)
- 受容できる (Acceptable)
- 受容できない (Unacceptable)
- 弱い (Deficient)
- 欠如 (Missing)



Respond能力測定の質問項目1 [Hollnagel2011]

	分析項目（反応する能力）
イベントリスト	そのシステムが反応を準備されたイベントの リストがあるか？ リスト上のイベントは 意味があるものか？ また、リストは 完全か？
背景	イベントを選択する明確な 基盤があるか？ そのリストは伝統，規制要求，設計基盤，経験，専門的意見，リスクアセスメント，工業基準などに 基づいているか？
適切性	そのリストは最新のものに 更新され続けているか？ いつそれが 改訂されるかの規則／ガイドライン はあるか？（例：規則的か必要に応じてか？） それは どんな基盤に基づいて改訂されるか？ （例：事象の統計か事故発生か？）
閾値	反応を起こすための明確な 判断基準があるか？ その判断基準は閾値や変化率を参照しているか？ その判断基準は絶対的であるか，あるいは，内部／外部要因に依存しているか？ 安全と生産性の間のトレードオフがあるか？

Respond能力測定の問題項目2 [Hollnagel2011]

	分析項目（反応する能力）
反応リスト	<p>反応が参照される状況に対して、それらが適切であるかをどのようにして決定するか？（経験的にか、解析あるいはモデルに基づいてか？）</p> <p>どのようにして反応が選択されたかが明確か？</p>
早さ	<p>どれだけ早く効果的な反応を開始できるか？</p> <p>どれだけ早く100%の反応能力が確立できるか？</p>
期間	<p>どれだけ長く効果的な反応が維持できるか？</p> <p>どれだけ早くリソースが補充できるか？</p> <p>「手に負えない」期間は何か？</p>
リソース	<p>反応に使い得る適切なリソースがあるか？（人員、材料、能力、熟練度、時間、など）</p> <p>準備された反応に対してどれだけのものを排他的な状態で保持されるか？</p>
終了規則	<p>「正常な」状態に戻るための明確な判断基準があるか？</p>
検証	<p>反応することの準備が維持されているか？</p> <p>反応することの準備を、どのように、また、いつ検証するか？</p>

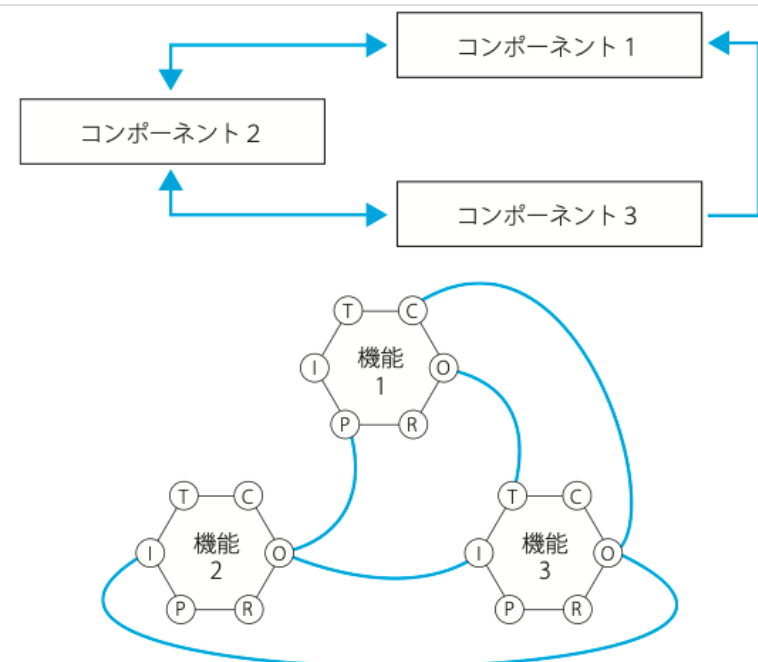
Resilience Engineeringの適用の困難さ

- Resilience Engineering
 - 適用の想定状況
 - 常に変動する現場状況
 - 現場要員の適応的な行動（WAD）により業務があたかもWAI通りに行われている
 - 概念が抽象的
- 工業プラントの運転の状況
 - 出来るだけ変動要因を少なくするように設計，建設，運転
 - 事故の発生が限りなくゼロが求められる
- 工業プラント業界での意見
 - 適用が困難
 - 適用性に懐疑的

Resilience Engineeringの今後の研究課題 1

- 1 : プラントの異常時対応における運転員等のWADとWAIを表現する枠組みの検討
 - REではWADの表現にFRAMがよく用いられる
 - FRAM : 機能共鳴の事象の可能性とその排除のための分析の切り口を提供
 - 工業プラント運転では要員の役割と活動が規定
 - 別の表現方法の開発が必要

I: 入力	機能の動作トリガー
P: 前提	機能が動作開始するための事前条件
C: 制御	機能の挙動方法を操作する事後条件
R: 資源	機能の動作に必要な資源 (事後条件)
T: 時間	機能実行可能時間 (事後条件)
O: 出力	機能の出力



Resilience Engineeringの今後の研究課題 2

- 2 : 失敗からの学びと成功からの学びの内容の相違の検討
 - 人間は成功を冷徹に分析できるか？
 - 成功からの学びの範囲には限界がある
 - 失敗しないようにする範囲を広げることができるが、失敗した場合の対応は学ぶことはできない
 - 例：転けないように体のバランスを取る技を磨く
→ 転けた時の衝撃を防ぐ転け方を学ぶことは困難
 - 学びの様相や性質の相違を明確にして、学習で使い分ける必要
 - サブテーマ
 - 2a：成功からの学びで失敗を回避できる範囲は？
 - 2b：失敗からの学びが安全性向上においてカバーする範囲は？
 - 2c：どのような研究でそれぞれの範囲を明らかにできる？
 - 効果：失敗しないことで気づかないことに気づく
 - 失敗の条件の厳密な考察
 - 失敗した場合のリスク想定のための分析力や想像力の向上

Resilience Engineeringの今後の研究課題 3

- 3 : 失敗を回避するために成功から学ぶための、日頃からの心がけや考え方の検討とその教育・訓練への展開
 - 成功から学ぶ観点, 考え方や方法を具体化して教育や訓練に取り入れることが重要
 - 例:パイロットの話
「正常に離陸している時に, もしある異常が発生した場合にどのように対処するかを想像しながら離陸操作をする」
 - 効果
 - 異常事象の発生時に迅速で適切な対応ができるようになる
 - 整備されている手順の根拠への知識を深めたり, 不備な点に気づくことができる

Resilience Engineeringの今後の研究課題 4

□ 4 : リスクアセスメントへのREの応用性の検討

■ RAGが参考になる

□ RAGの質問には、**現状の前提条件や根拠を問うもの**が多く含まれている

■ 効果：システム（ハードウェアやソフトウェア）の設計段階での安全性確保の検討の質が向上

	分析項目(反応する能力)
イベントリスト	そのシステムが反応を準備されたイベントの リストがあるか？ リスト上のイベントは 意味があるものか？ また、リストは 完全か？
背景	イベントを選択する明確な 基盤があるか？ そのリストは伝統、規制要求、設計基盤、経験、専門的意見、リスクアセスメント、工業基準などに基づいているか？
適切性	そのリストは最新のものに 更新され続けているか？ いつそれが 改訂されるかの規則／ガイドライン はあるか？（例：規則的か必要に応じてか？） それは どんな基盤に基づいて改訂されるか？ （例：事象の統計か事故発生か？）
閾値	反応を起こすための明確な 判断基準があるか？ その判断基準は閾値や変化率を参照しているか？ その判断基準は絶対的であるか、あるいは、内部／外部要因に依存しているか？ 安全と生産性の間のトレードオフがあるか？

Resilience Engineeringの今後の研究課題 5

- 5 : 安全確保のためのレジリエンスでの柔軟に変更する項目決定方法の検討
 - レジリエントな対応が許容されたり, レジリエントな対応に移行したりするための基準が明確になっていることが必要
 - 現状のRE研究の主要テーマ: 変動がある環境でより良いレジリエント性の発揮
 - 基準設定に必要な情報
 - 選択肢
 - 選択肢を選んだ場合の効果や影響の予測
 - 精度良い予測が困難
 - コンピュータシミュレーション技術の一層の向上が必要
 - 広範囲な環境への影響が発生することから多様な価値観に基づく合意形成が困難

Resilience Engineeringの今後の研究課題 6

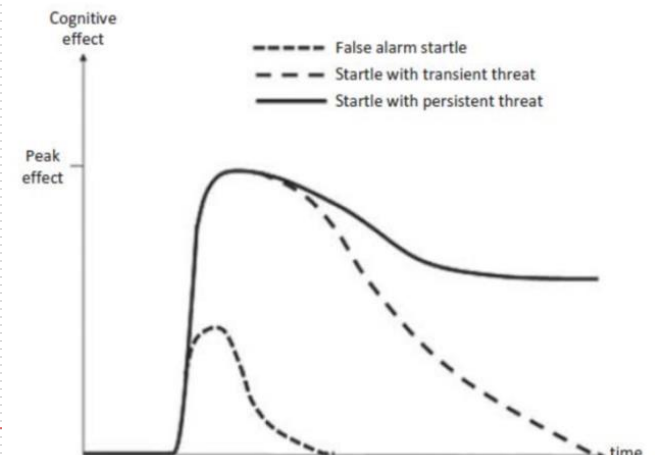
- 6 : 手順書等で行動が規定されている場合に, それとは異なる行動をレジリエントに採ることが許容される条件の検討
 - 現場要員は手順書に従った行動が求められる
 - ヒューマン・エラー防止のため異常対応手順が細かく規定
 - 手順とは異なる行動 : 失敗確率はある程度ある
 - 手順通りに行動しても失敗する確率はある
 - レジリエントな行動が成功した例
 - 東日本大震災時に, 列車の停車位置を乗客の意見に基づいて変更したことで大津波から免れる
 - 規則と指示に従った行動が批判された例
 - 沿線火災時に, 電車の屋根に飛び火したことにより, 停車位置が不適切と批判



<https://www.buzzfeed.com/jp/kotahatachi/odakyu2>

Resilience Engineeringの今後の研究課題 7

- 7 : レジリエントな行動が採れる能力が身につく訓練の検討
 - シリアスゲーム（ゲーム感覚の訓練法） [Lammers, 2019]
 - Compliance vs Resilienceの枠組み（2種類の参加者）
 - Compliance（規制，規則や手順書重視）の立場
 - Resilience（柔軟な発想重視）の立場
 - 事象シナリオ想定：進展によりレジリエンスに対処せざるを得ない外乱や阻害要因が導入
 - それぞれの立場に立った対応策を提案
 - 航空パイロットの驚き（Startle）対応能力向上訓練
 - 驚愕事象への対応の経験で，適切な対応能力が改善される
 - 困難ではあるがマネジメント可能な事象として評価
 - 驚愕レベルは低下して対応力向上の可能性が高い



おわりに

- Resilience Engineering (RE) の考え方を整理
 - Safety-IとSafety-II
 - WAIとWAD
 - 4つの能力
- プラント（特に運転）の更なる安全性向上のために適用するための課題を考察
 - 1. 運転員等のWADとWAIを表現する枠組み
 - 2. 失敗からの学びと成功からの学びの内容の相違
 - 3. 成功から学ぶための、日頃からの心がけや考え方
 - 4. リスクアセスメントへのREの応用性
 - 5. 柔軟に変更する項目決定方法
 - 6. レジリエントな行動を採ることが許容される条件
 - 7. レジリエントな行動が採れる能力が身につく訓練
- 課題に対する研究が進展し、REがプラント分野へ浸透して、
不測の事態への対応能力が格段に向上することを期待