Nancy G. Leveson

Engineering a Safer World

～System Thinking Applied to Safety～

邦訳　「システム理論による安全工学」
～想定外に気づくための思考法STAMP～

STPAやCASTといった方法論を使うだけでなく、STAMPのもとになっている
思想を理解することで、より効果的な利用が可能になる。

2024年11月22日

会津大学　名誉教授　兼本茂

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

「Engineering a Safer World」の翻訳（共立出版）

10年前の本の翻訳が役に立つか？
内容は超うスマート社会を先取りしている。
STPAやCASTといった方法論を使うだけでなく、STAMPのもとになっている思想を理解することで、より効果的な利用が可能になる。

2011年原著

2024年10月11日翻訳本販売

一般社団法人 組込みシステム Japan Embedded Systems Technology Association

本書の目的と想定読者

- 本書は、新しい事故因果関係モデルとシステム安全手法について述べたものであり、現代のシステム思考とシステム理論に基づいた安全へのアプローチに基づいて構築されている
  - 事故を減らし、システムや高度な製品をより安全にするために、エンジニアや安全性に関心のある人々が使える**ツールを提供**する
  - 医療や金融も含め、**あらゆる複雑な社会技術システムに適用**できる
- 想定読者層
  - システム安全に興味を持つ、企業の経営者／管理者／担当者／開発者、大学教員／学生
  - 安全エンジニアを含む（全ての）エンジニアの方々
  - エンジニアではない方々

日本語版刊行へのナンシー・G・レブソン教授のメッセージ（2024年）

今、我々の使っている事故防止のためのエンジニアリング・ツールの多くは、すべて60年以上も前の、より単純でアナログな世界において開発されたものです。当時は、今とはまったく違う種類の技術が使われており、ソフトウェアを含むシステムや、今日のような複雑なシステムはほとんどありませんでした。

これらの古いツールを使って、今日の非常に複雑なソフトウェア集約型システムの事故を防ごうとしても、その有効性はだんだんと小さくなってゆくでしょう。そのようなシステムの事故の原因は、過去に起きていた事故とは異なります。社会技術的でソフトウェア集約的なこの複雑な世界と、私たちの周りで繰り広げられている技術革命の中では、より適した「何か新しいもの」が必要とされています。

本書は、システム理論とより包括的で最新の事故原因モデルに基づいた、安全工学への新しいアプローチについて述べています。この新しいアプローチは有効なのでしょうか？このアプローチは航空や防衛を中心としたほとんどの産業で損失を防ぐために使われており、世界中に広がりつつあります。そして、科学的、経験的に比較することによって、従来の安全工学的アプローチよりも優れていることが示されています。この新しいアプローチは、過去のシステムではなく、今日運用されているシステムに合わせて設計されているため、従来の手法に比べて、より効果的で、コストがかからず、使いやすい手法です。

本書では、安全工学における「何か新しいもの」の必要性を説明した上で、コンポーネントの単純な故障を超えた因果関係の拡張モデルと、新しい事故・ハザード分析手法を提案します。また、今日の重要なシステムの運用と管理に必要とされているのは何かということを、具体例を交えて概説します。本書で提示したツールは、従来のエンジニアリングの枠を超えて、安全性向上とリスク管理のために、今日のあらゆる種類の大規模な社会技術システムに適用され、活用されています。

このたび本書が日本語で読めるようになり、世界をより安全に暮らせる場所にするためのこの画期的なアプローチが、より多くの方々に触れてもらえることをとてもうれしく思います。

日本語版刊行へのナンシー・G・レブソン教授のメッセージ（2024年）

今、我々の使っている事故防止のためのエンジニアリング・ツールの多くは、すべて60年以上も前の、より単純でアナログな世界において開発されたものです。当時は、今とはまったく違う種類の技術が使われており、ソフトウェアを含むシステムや、今日のような複雑なシステムはほとんどありませんでした。

これらの古いツールを使って、今日の非常に複雑なソフトウェア集約型システムの事故を防ごうとしても、その有効性はだんだんと小さくなってゆくでしょう。そのようなシステムの事故の原因は、過去に起きていた事故とは異なります。社会技術的でソフトウェア集約的なこの複雑な世界と、私たちの周りで繰り広げられている技術革命の中では、より適した「何か新しいもの」が必要とされています。

本書は、システム理論とより包括的で最新の事故原因モデルに基づいた、安全工学への新しいアプローチについて述べています。この新しいアプローチは有効なのでしょうか？このアプローチは航空や防衛を中心としたほとんどの産業で損失を防ぐために使われており、世界中に広がりつつあります。そして、科学的、経験的に比較することによって、従来の安全工学的アプローチよりも優れていることが示されています。この新しいアプ[illegible]従来の[illegible]を超[illegible]ム[illegible]ル[illegible]模[illegible]プローチが、より多くの方々に触れてもらえることをとてもうれしく思います。

このたび本書が日本語で読めるようになり、世界をより安全に暮らせる場所にするためのこの画期的なアプローチが、より多くの方々に触れてもらえることをとてもうれしく思います。

目次

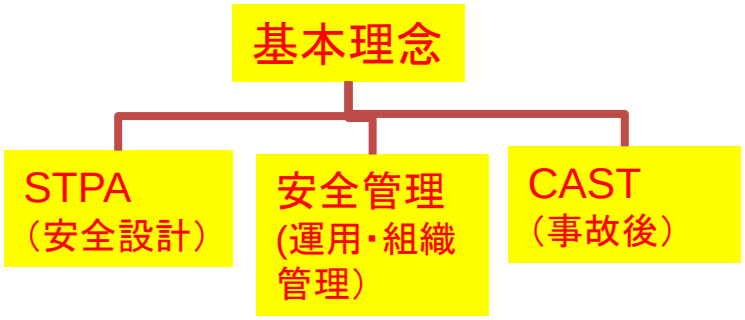
第1部　基礎
　第1章　なぜ今までと違うものが必要なのか？
　第2章　伝統的な安全工学の基礎を疑う
　第3章　システム理論と安全性の関係
第2部　STAMP：システム理論に基づく事故モデル
　第4章　因果関係に対するシステム理論的な見方
　第5章　味方への誤射による事故
第3部　STAMPの活用
　第6章　STAMPを用いたより安全なシステムのエンジニアリングと運用
　第7章　基本的な活動
　第8章　STPA：新しいハザード分析手法
　第9章　安全主導設計
　第10章　システム工学への安全の統合
　第11章　CAST：事故とインシデントの分析
　第12章　運用時の安全コントロール
　第13章　安全のための経営と安全文化
　第14章　SUBSAFE：米国海軍の潜水艦安全プログラムの成功事例
付録
　付録A　定義
　付録B　人工衛星の損失
　付録C　公共水道の細菌汚染
　付録D　システムダイナミクス・モデリングの概要

目次

新しい安全工学の必要性
システム理論とは？
STAMPの基本理念

STPA（新しいハザード分析法）
安全主導設計

運用と組織の安全文化
事故時の分析と対策



第1部　基礎
第1章　なぜ今までと違うものが必要なのか？
第2章　伝統的な安全工学の基礎を疑う
第3章　システム理論と安全性の関係
第2部　STAMP：システム理論に基づく事故モデル
第4章　因果関係に対するシステム理論的な見方
第5章　味方への誤射による事故
第3部　STAMPの活用
第6章　STAMPを用いたより安全なシステムのエンジニアリングと運用
第7章　基本的な活動
第8章　STPA：新しいハザード分析手法
第9章　安全主導設計
第10章　システム工学への安全の統合
第11章　CAST：事故とインシデントの分析
第12章　運用時の安全コントロール
第13章　安全のための経営と安全文化
第14章　SUBSAFE：米国海軍の潜水艦安全プログラムの成功事例
付録
付録A　定義
付録B　人工衛星の損失
付録C　公共水道の細菌汚染
付録D　システムダイナミクス・モデリングの概要

Keywords

STAMP:　Systems-Theoretic Accident Model and Processes
STPA:　Systems-Theoretic Process Analysis
CAST:　Causal Analysis based on STAMP

Systems-Theoretic（システム理論）とは何か？

第1章　なぜ今までと違うものが必要なのか？

1. **技術の変化の速さ**
   - 新しい技術は、システムに未知のものを持ち込み、損失への新たな経路を作り出す
2. **経験からの学習能力の低下**
3. **変化する事故の本質**
   - デジタルシステムやソフトウェアの使用によって発生する事故をコントロールするのには、既存の手法はもはや 有効ではない
4. **新しいタイプの危険（hazards）**
5. **複雑性の増加と結合の増加**
   - インタラクティブな複雑性、動的な複雑性、分解的な複雑性（構造分解と機能分解の不一致）、非線形な複雑性（原因と結果の複雑な関係）など。
6. **1つの事故に対する耐性の低下**
   - 事故から学ぶというやり方より、最初の事故を起こさないようにすることに注力すべき
7. **優先度の選択とトレードオフの難しさ**
8. **人間と自動化とのより複雑な関係**
   - 自動化モードの混乱や、作為と不作為のエラー増加といった新しいヒューマンエラーの増大
9. **安全に対する規制や人々の見解の変化**
   - 今日の複雑に絡み合う社会構造において、安全に対する責任は個人から政府（社会）へと移行

第3章　システム理論とは（Systems-Theoreticの意味）

～創発と階層、コミュニケーションとコントロール～

システムの階層化と創発

自然界の進化

環境に隠れて生き残る

環境に隠れやすい縞模様（創発特性）

コミュニケーションとコントロール

シマウマの生存戦略

プロセスモデル
細胞色素の拡散と反応による縞模様の発生
（チューリング・パターン）

$$\frac{\partial u}{\partial t} = f(u,v) + D_u \nabla^2 u,$$

$$\frac{\partial v}{\partial t} = g(u,v) + D_v \nabla^2 v$$

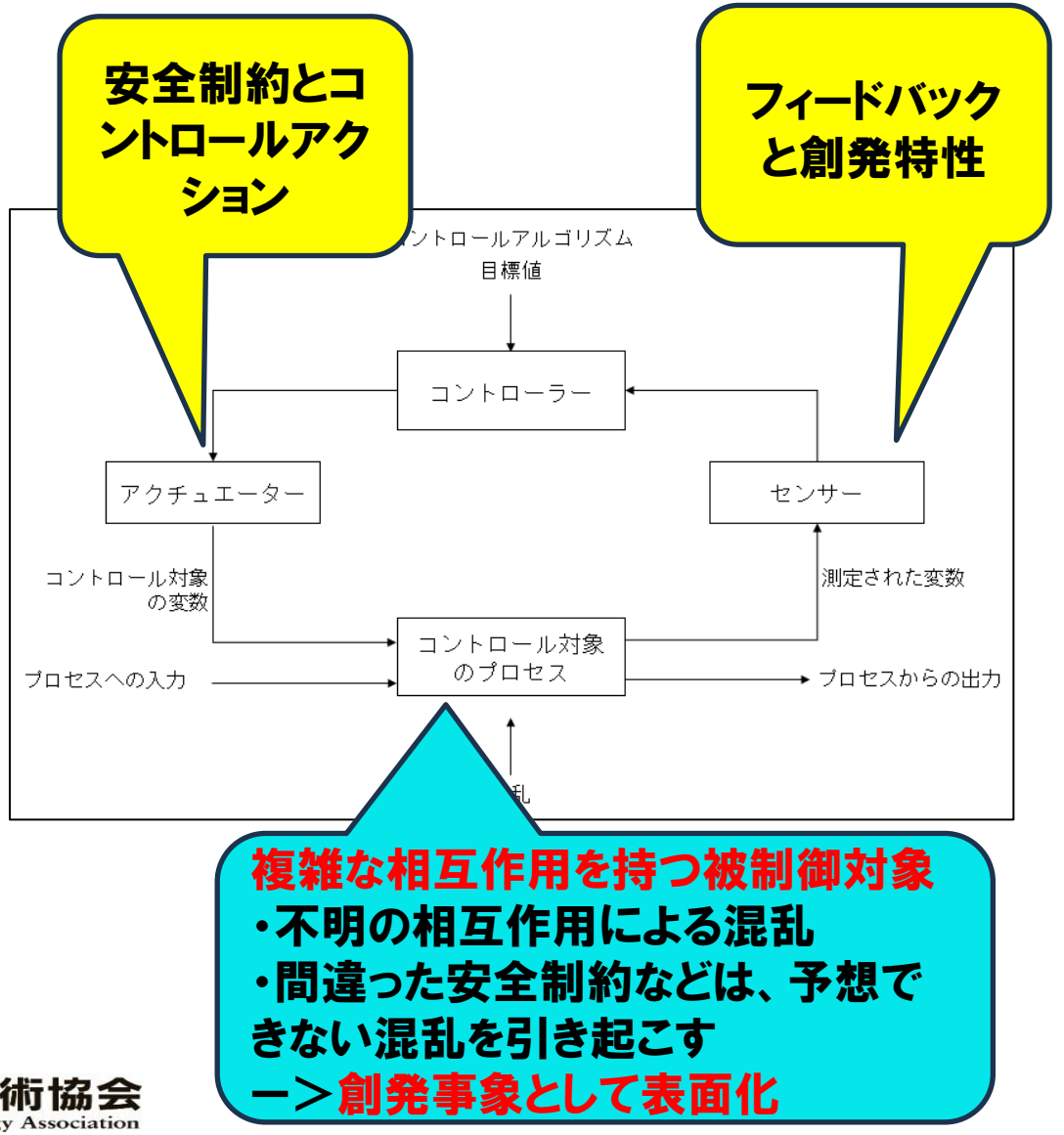
システム理論の二つの対をなす概念

■ 創発と階層

- 創発特性とは、1つ下の階層には存在しない、つまり、下位階層を記述するのに適した言語では意味をなさないような性質
- リンゴの形について、最終的に「リンゴの細胞」の観点で説明することができたとしても、下位階層の記述においては「リンゴの形」は意味を持たない。下位階層における細胞間の相互作用は、上位階層におけるリンゴ全体の複雑性（創発特性）をもたらす。

■ コミュニケーションとコントロール

- 規制やコントロールアクションは、下位の階層レベルの動作に**制約**を与え、そこでの「振る舞いの法則」（創発特性）が定められる。
- 階層システムを維持するためには、規制やコントロールのための情報伝達が行われるようなプロセスが必要である。コントロール対象のプロセスの状態を測定するフィードバック情報のら取得も含む。



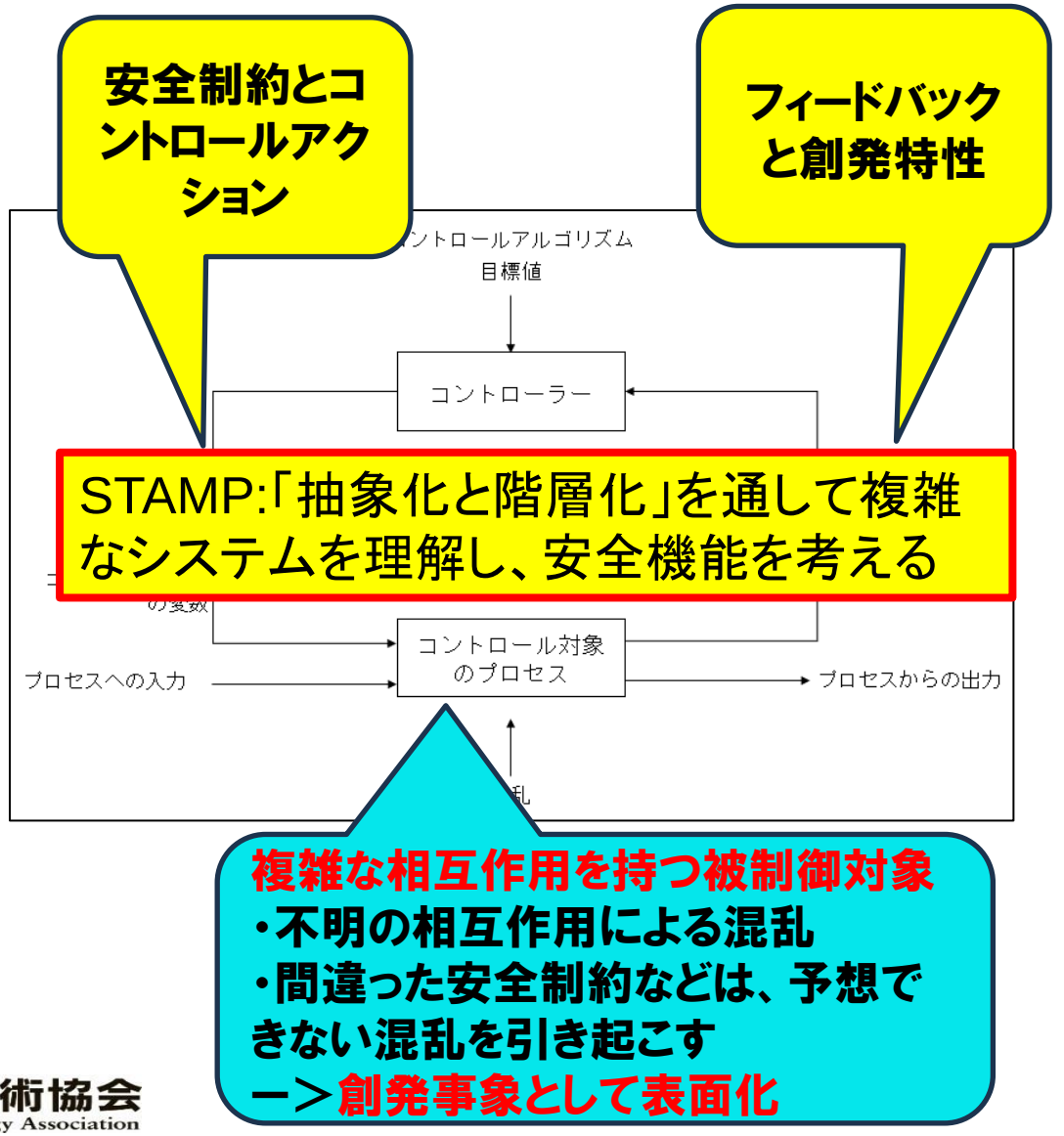
システム理論の二つの対をなす概念

■ 創発と階層

- 創発特性とは、1つ下の階層には存在しない、つまり、下位階層を記述するのに適した言語では意味をなさないような性質
- リンゴの形について、最終的に「リンゴの細胞」の観点で説明することができたとしても、下位階層の記述においては「リンゴの形」は意味を持たない。下位階層における細胞間の相互作用は、上位階層におけるリンゴ全体の複雑性（創発特性）をもたらす。

■ コミュニケーションとコントロール

- 規制やコントロールアクションは、下位の階層レベルの動作に**制約**を与え、そこでの「振る舞いの法則」（創発特性）が定められる。
- 階層システムを維持するためには、規制やコントロールのための情報伝達が行われるようなプロセスが必要である。コントロール対象のプロセスの状態を測定するフィードバック情報のら取得も含む。



第8章　STPA：新しいハザード分析手法

(1)Step-1

分析の目的の定義
[損失（アクシデント）の定義、ハザードとシステム安全制約の定義]

(2)Step-2

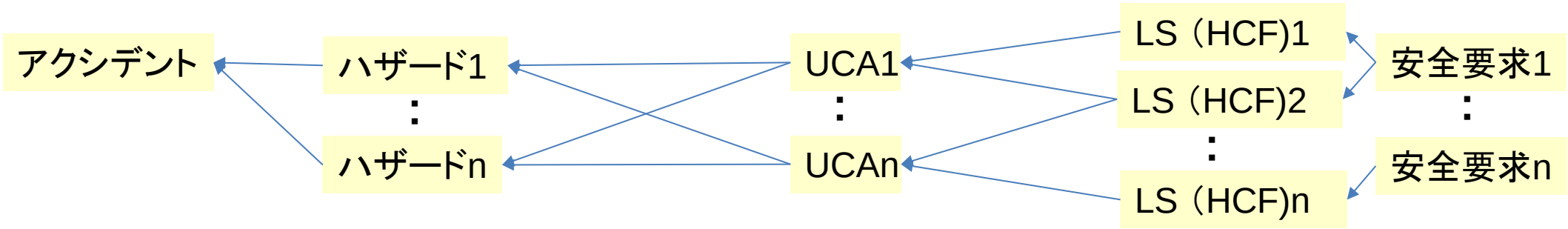
制御構造図と安全責任、ならびに、安全コントロールアクションをモデル化

(3)Step-3

非安全コントロールアクション（UCA)の同定＋（コンポーネント安全制約への展開）

(4)Step-4

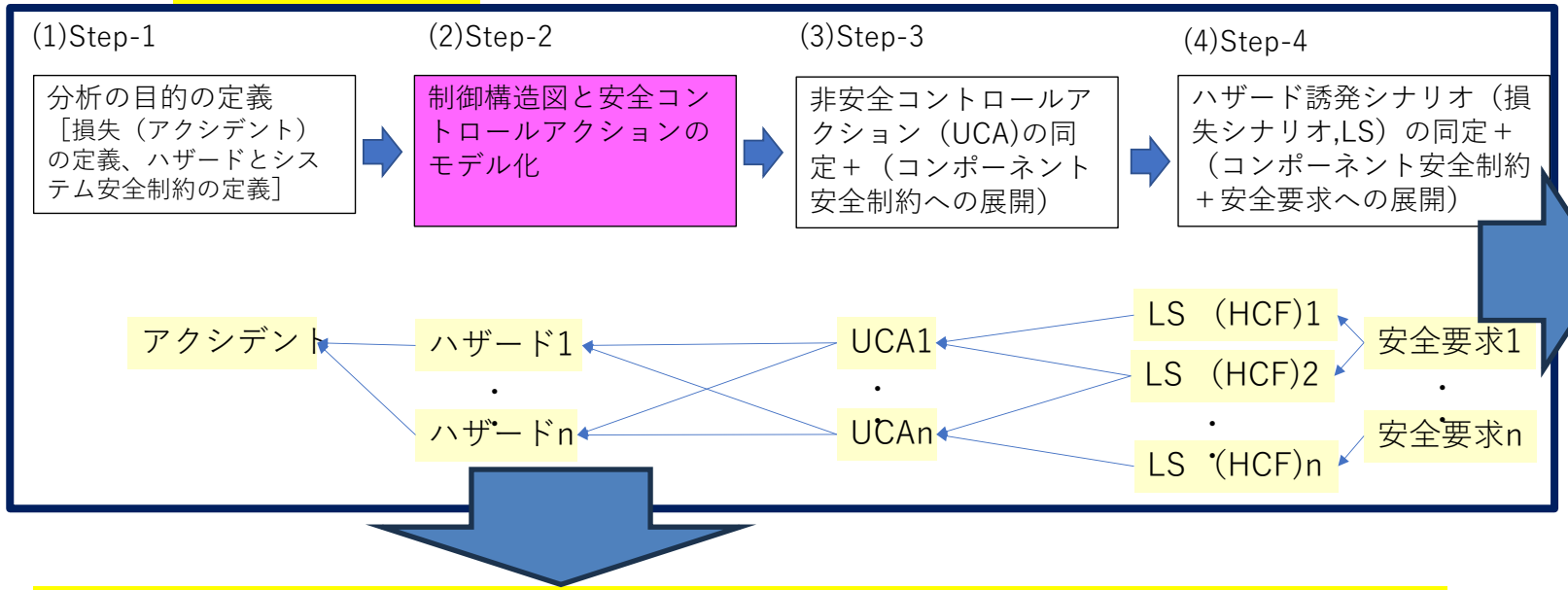
ハザード誘発シナリオ（損失シナリオ,LS）の同定＋（コンポーネント安全制約＋安全要求への展開）



アクシデント・ハザード・UCA・LS・安全要求は、追跡可能な論理構造になっており、網羅的なハザード分析法になっているだけでなく、安全論証としてのエビデンスにもなる（透明性の確保）

第9-14章　STPAから安全主導設計と運用管理へ

STPAの手順



<u>システム全体の安全要求の体系化とシステム設計への統合</u>

・個別の安全要求をまとめなおす（体系化）
・システム全体の安全設計思想としてまとめる（安全哲学）
・システム設計への統合

第9-10章　STPAから安全主導設計へ

<u>安全コントロールストラクチャーの可視化</u>

・目的（どんな事故を防ぐか）の明示化
・各要素の安全責任と権限を定義し可視化する
・安全責任を達成するためのCAと、CAを作るためのFBを明示化
・最悪の外部環境状態の明示化
・第三者の評価が可能な抽象化と階層化モデル
・運用管理体制への接続

第11-14章　運用後の組織管理への展開

STAMPの考え方を体現するGood Example！

～遠隔クレーン制御システムの事例：STPAから安全主導設計と運用管理へ～

◆STAMP による安全設計コンサルタント

移動式クレーンの遠隔操作システム「CRANET」の開発と安全設計

現場の画像

オペレータ操作装置

インターネット回線

現場のクレーン

損失（事故）の定義

↓

コントロールストラクチャー（安全制御構造）と安全責任の可視化

↓

ハザード分析（非安全制御構造の特定と損失シナリオの推定

↓

システムとコンポーネントの安全目標の導出とシステム設計への組み込み

↓

組織運用手順・安全管理手順の整備

STPA

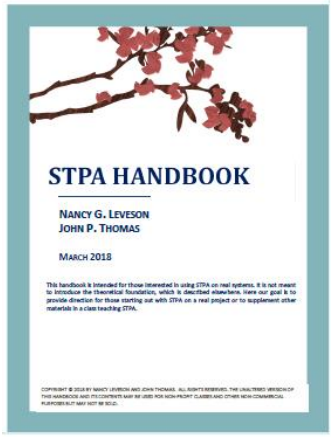
第9-10章　STPAから安全主導設計へ

第11-14章　運用後の組織管理への展開

原著と関連文書との関係

（STPAとCASTは詳細手順書があるが、その背景や安全設計全体の考え方は原著のみ）

Engineering a Safer World 2011

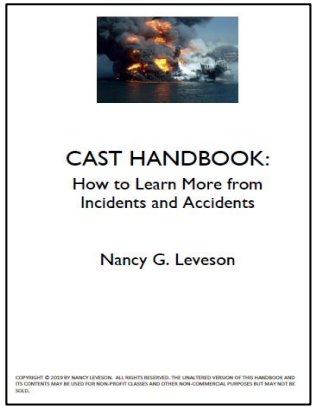


STPA HANDBOOK 2018

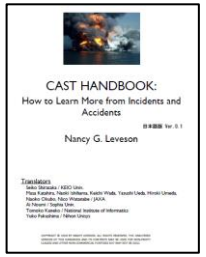
STPA HANDBOOK日本語版 2018

JASA 安全設計ガイド8章 2019年

IPA STAMP/STPAのガイドブック 2015～2018



CAST HANDBOOK 2019



CAST HANDBOOK 日本語版 2021

あとがき

- システム理論は、複雑性に対処する人間の限界を超えるために必要なツールを構築するための基礎を提供している
  - 「故障の防止」から「振る舞いに関する安全制約の強化」へ　→「信頼性の確保」から「安全のコントロール」へと焦点を変えた、安全工学の新しいアプローチ
- 事故防止に成功している産業（米国の原子力潜水艦安全プログラムなど）
  - 開発と運用の両面において、安全に対するシステムズアプローチをとっている。
  - 事故から効果的に学ぶ学習文化を確立している。
  - 安全を優先事項として設定し、長期的な成功が安全にかかっていることを理解している。
- あまり成功していない産業
  - 事故は進歩や利益の代償であると信じている
- システム安全（MIL-STD-882）は「組織化された常識」である　（1968年、Mueller）ー＞本書の趣旨

ご静聴ありがとうございました。質問などがあれば、
JASAの安全性向上委員会に問い合わせください。

（JASA技術本部事務局：JASAINFO@JASA.OR.JP）