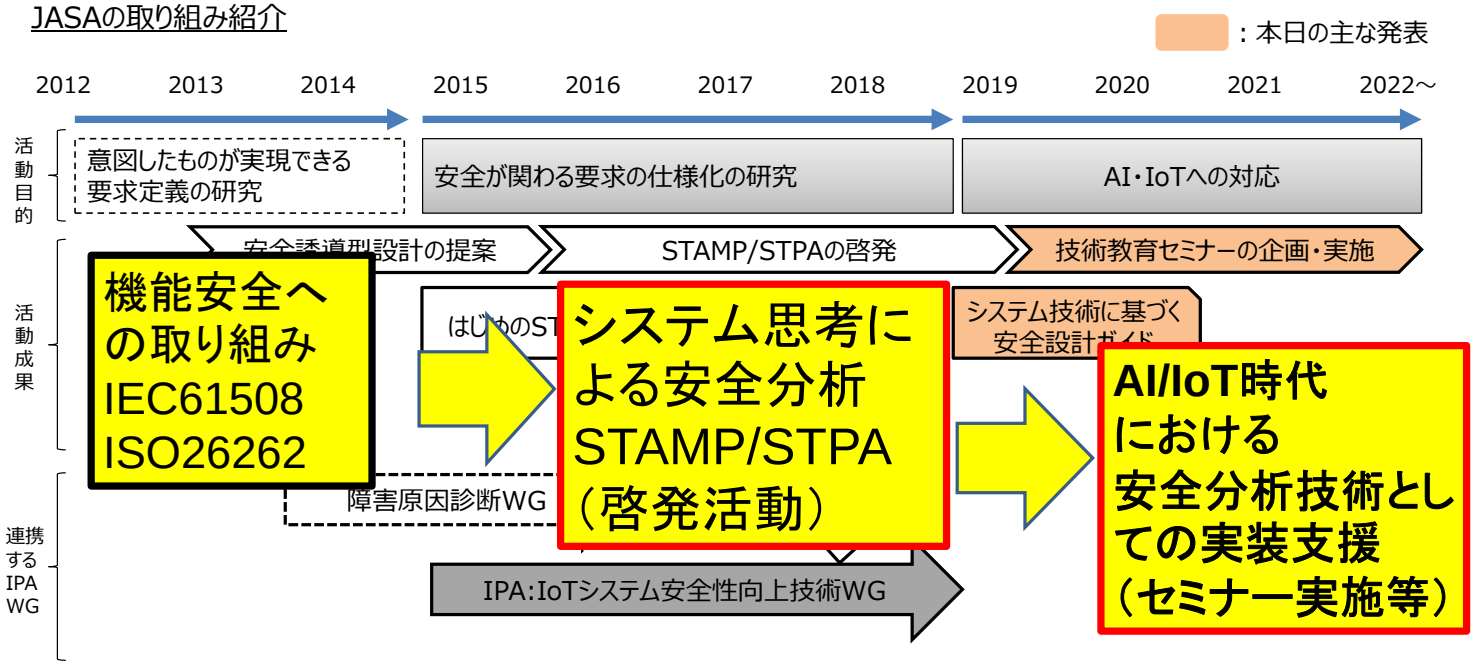
複雑システムの安全分析／STAMP
～システミック思考にもとづく安全分析のパラダイムシフト～

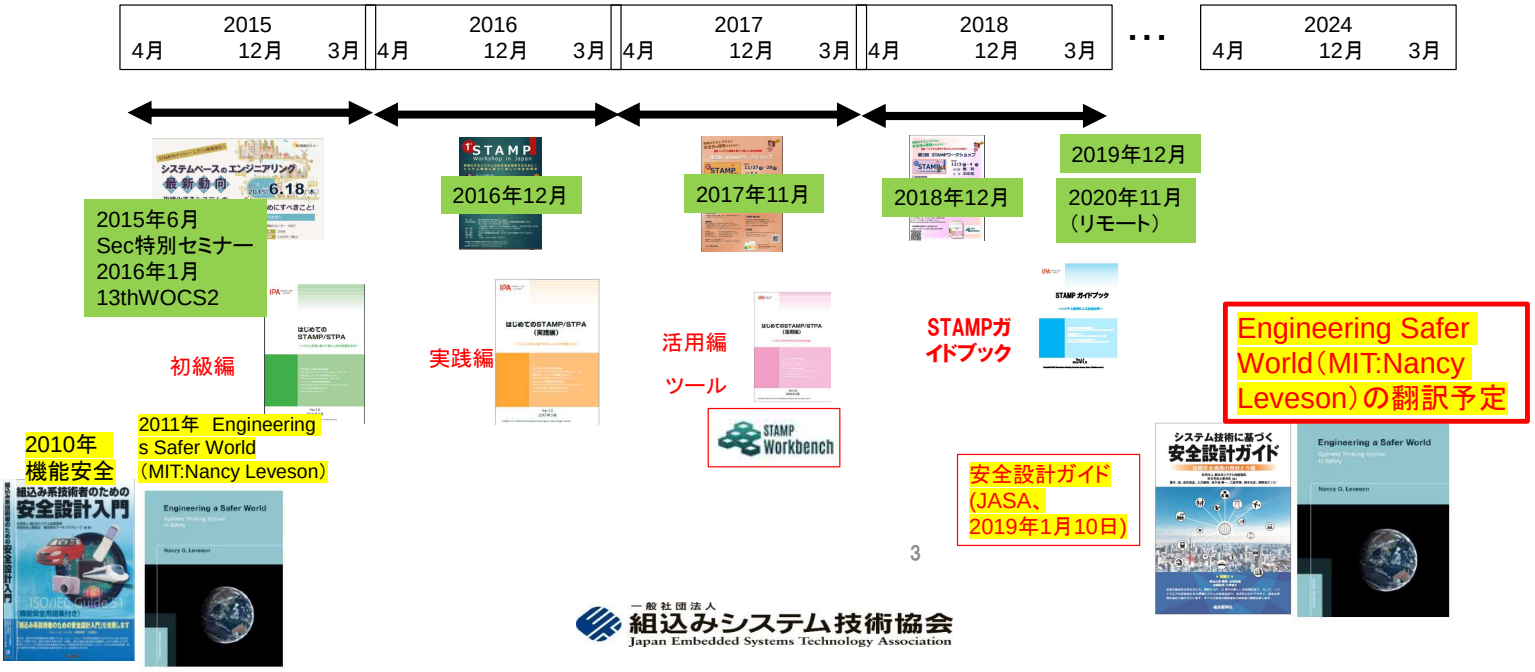
2023年11月
JASA・安全性向上委員会
兼本　茂（会津大学　名誉教授）

JASA　安全性向上委員会の取り組み

JASAの取り組み紹介



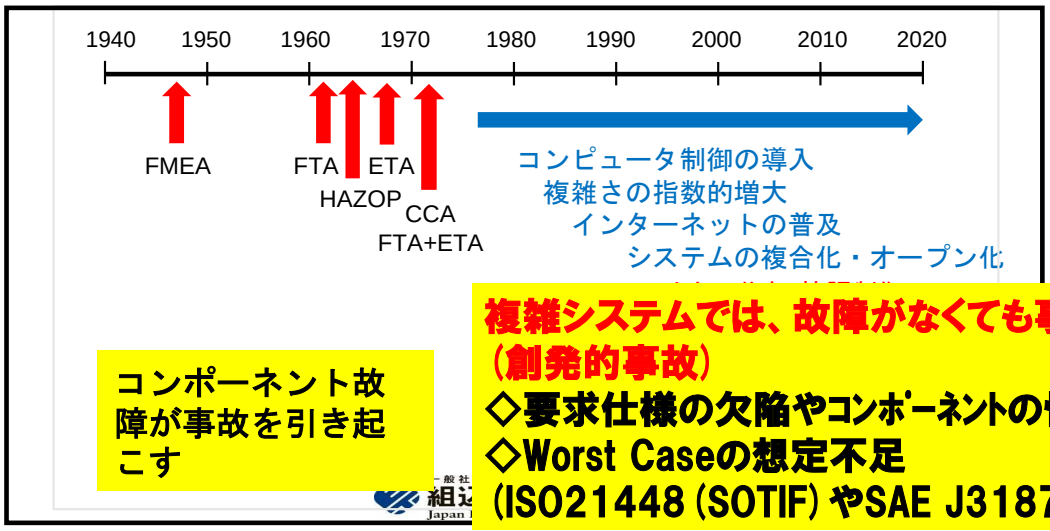
IPA・JASAでの活動（安全性向上委員会・IoTシステム安全性向上技術WG）



IoT時代の環境変化と新しい安全解析法　STAMP

Sec-Seminar(2015.6.18) Lecture by Nancy Leveson

現状の安全分析ツールは、40-65年も昔に開発されたものであり、現代の新しい技術の入った複雑な工学システムの安全分析には限界がある　→　*パラダイムシフトとしてのSTAMPの登場*



コンポーネント故障が事故を引き起こす

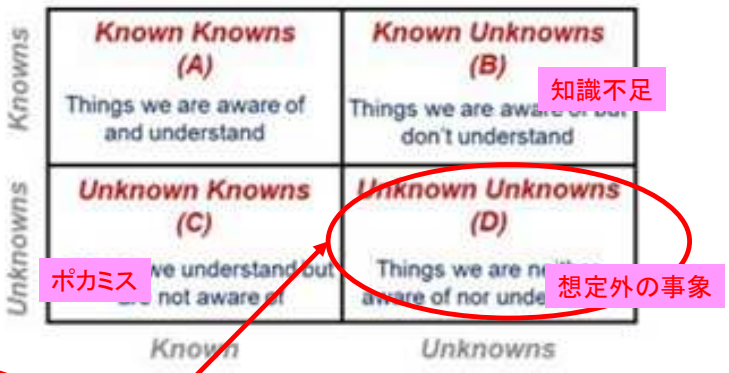
複雑システムでは、故障がなくても事故は起こる（創発的事故）
◇要求仕様の欠陥やコンポーネントの性能限界
◇Worst Caseの想定不足
（ISO21448（SOTIF）やSAE J3187）

背景(参考)

■ 複雑システムの事故は創発的(想定外)である。

ISO21448(SOTIF)
Safety Of The Intended Functionality

SAE J3187



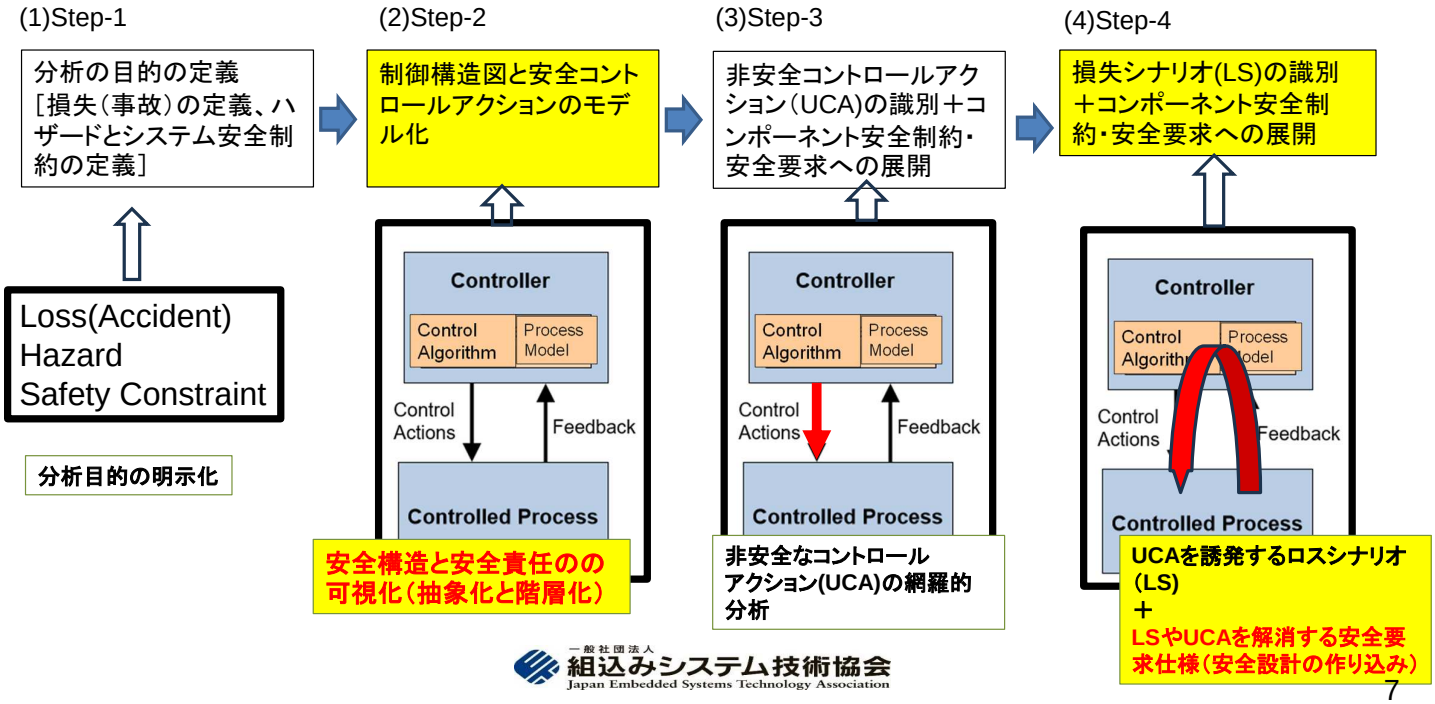
これらを少なくするにはSTAMP/STPAが有効

背景と目的

■ 還元論(Reductionism)
- FTA、FMEA、HAZOPなどの信頼性工学に基づく安全分析
- 設計が決まった後の安全分析法

■ 全体論(Holism)・創発論(Emergence)
- システム全体を包括的に捉えたシステミックな安全分析法(複雑システムの安全は創発的である) STAMP/STPA
- 概念設計段階での安全の作り込み(安全要求仕様の導出)
  - 抽象化と階層化により安全構造を可視化した安全制御構造図により安全分析を行う(多様なステークホルダーによる安全構造レビュー)
  - 階層的安全責任と安全制御指示(コントロールアクション)の明示化
  - 安全論証としてのエビデンス化

STAMP/STPAの手順（何が一番重要か？）



見逃しがちな二つの論点

- 可視化（Step-2）
  - 安全制御構造図は、多様なステークホルダーにとって理解できるものでないといけない－＞抽象化と（安全責任の）階層化
- ハザード誘発要因（Hazard Causal Factor、HCF）－＞損失シナリオ（Loss Scenario、LS）（Step-4）
  - HCF（STAMP執筆時点、2011年） → LS（STPA Handbook、2018年）
  - ロスシナリオでは、ハザード誘発（トリガー）要因から損失（事故）までのシナリオが記述される。シナリオのどこかの段階で安全措置（安全要求仕様）をとれば、その損失が防げる。即ち、設計段階で安全を作り込め、個別の要因への対応をしなくて済み、安全コスト低減に役立つ。

安全責任の階層化（N.Leveson,"Engineering a Safer World"）

4.2節　階層的安全制御構造(The hierarchical Safety Control Structure **P.80)**

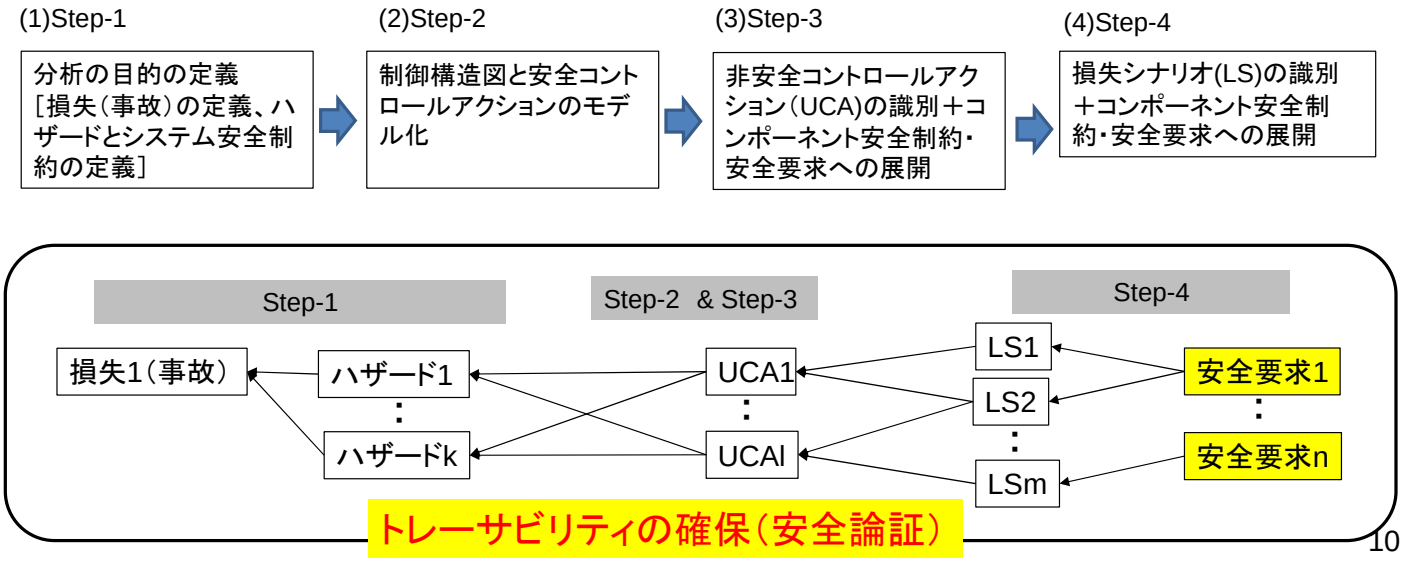
In systems theory, systems are viewed as hierarchical structures, where each level imposes constraints on the activity of the level beneath it—that is, constraints or lack of constraints at a higher level allow or control lower-level behavior.

ー＞システム理論（3章）では、システムは階層的構造を持つとみなされる。つまり、それぞれのレベルの意思は、それより下のレベルの活動に制約を課している。

Between the hierarchical levels of each safety control structure, effective communication channels are needed, both a downward reference channel providing the information necessary to impose safety constraints on the level below and an upward measuring channel to provide feedback about how effectively the constraints are being satisfied。

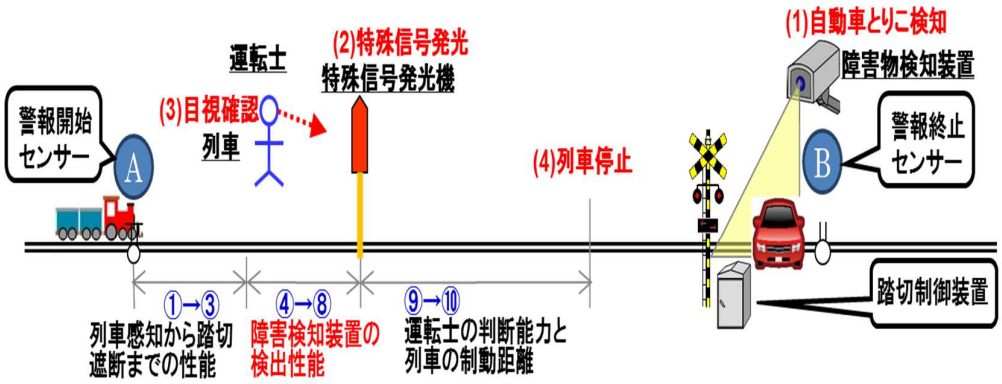
ー＞階層的レベルの間では、上から下へは、下に課した安全制約の実施に必要な情報を提供しなければならないし、下から上へは、与えられた安全制約を効率的に満たしているというフィードバック情報を提供しないといけない。

STAMP/STPAの手順（安全論証と安全設計の作り込み）



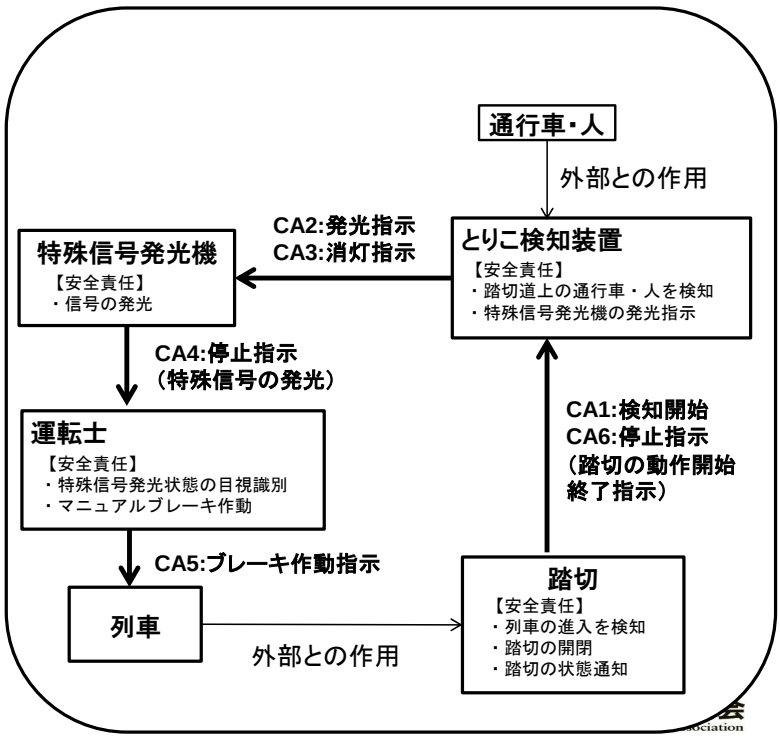
安全制御構造図の事例（踏切のとりこ検知装置）

踏切が閉まった時、踏切内に閉じ込められた人や車を検知し、
特殊信号発光機で列車運転士に知らせるシステム



今回の分析範囲は④から⑨

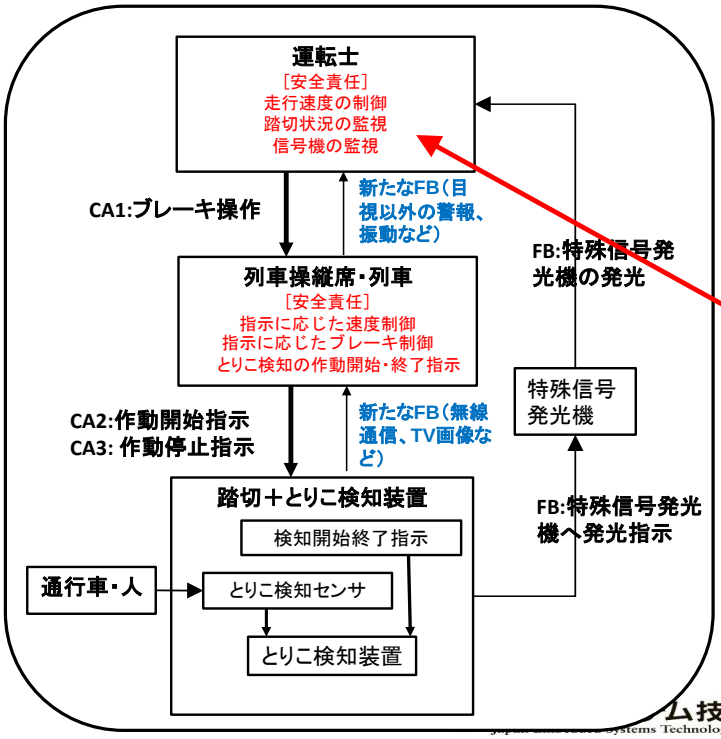
とりこ検知システムの安全制御構造図（階層化なし、2017年前半）



京急事故より前の2017年に分析を実施。すべてのコミュニケーションをコントロールアクション（CA)ととらえていて階層性がない。

運転士のヒューマンエラーは分析をしていたが、緊急時の運転手順書などの組織要因までは踏み込んでいなかった。

とりこ検知システムの安全制御構造図（階層化あり、2017年後半）



京急事故より前の2017年に分析を実施。
　制御構造図作成までで、UCA、損失シナリオまでは分析していない。また、**運転士の安全責任に乗客の転倒防止などの配慮が入っていない。**
　さらに、運転士の上位階層である運転管理部門などの組織までは考えていない。

とりこ検知装置はあったが・・京浜急行踏切事故（2019年9月5日11時40分）

神奈川新町～仲木戸間の踏切で大型トラックと衝突

踏切に設置した障害物（とりこ）検知装置で停止信号を点灯
・カーブがあるが、570m手前で確認可能
・時速120kmで走行時の制動距離は517.5m、空走距離は53m（120km/Hrで1.6秒の余裕しかない）
・社内規定では、信号機点滅を確認した場合、「速やかに停止」としていたが、今後、「直ちに非常ブレーキ」に変更するとのこと
・運転士は、「速やかに停止」の場合、常用ブレーキか非常ブレーキ併用かの判断が必要

京浜急行杉田駅近くの踏切　2023年3月25日（土）

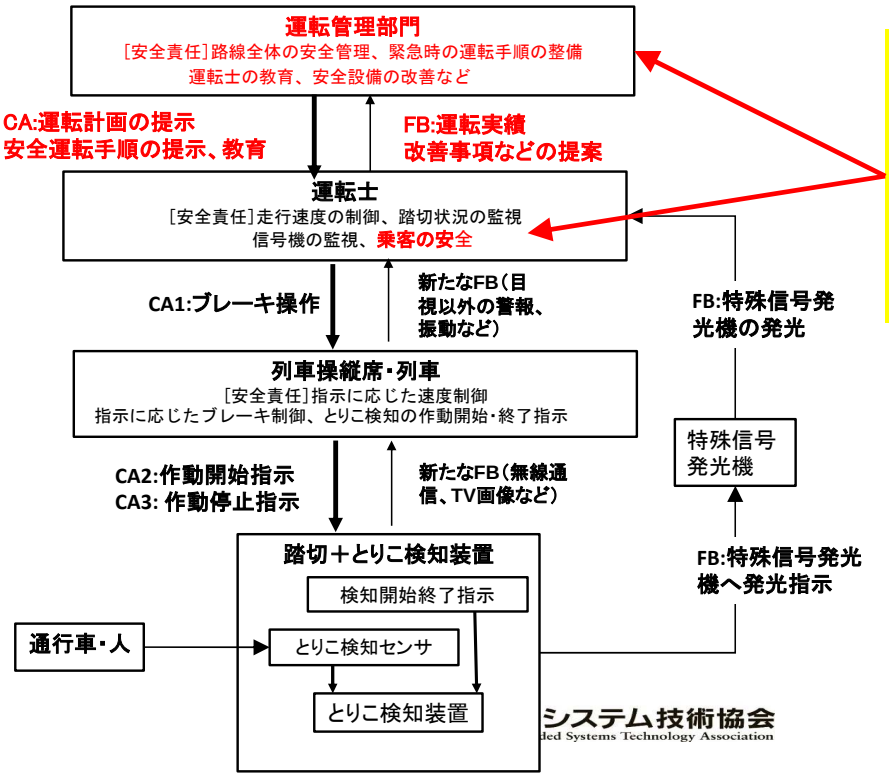
ポスター掲示

踏切遮断後の侵入防止のための監視員

踏切内のとりこだけでなく、列車の乗客の安全にも配慮が必要）！

約50件／日（京急線）！

とりこ検知システムの安全制御構造図（階層化あり、2023年）



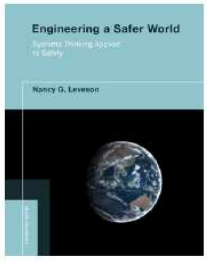
組織要因も安全制御の大事なコンポーネントであるべき。
また、踏切の安全だけでなく、乗客の安全を考える責任も運転士にはある。

システム技術協会
ed Systems Technology Association

STAMP14章　SUBSAFE(1963年発行）の事例

- 米国原子力潜水艦の安全プログラムなのに・・・
  - 原子炉の安全については、何も述べていない
  - STAMPの教えを体現している成功例なのに、制御構造図も非安全コントロールアクション（UCA)もほとんど記載がない（むしろ、STAMPがこちらから学んだといえる）
  - しかし、驚くほどの成功を収めている
- 安全プロクラムSUBSAFEの成功要因は何か？
  - 安全管理を、機械の故障だけに留めず、組織の在り方まで立ち入って見直したこと。（1963年という時期にここまで考えた！）
  - 組織と権力の独立性と協調性を明確に定義。組織の階層[illegible]への要求を義務付けた。
  - 安全目標を明確に設定した。事故の防止ではなく、緊急時にも確実に浮上[illegible]と目標（レジリエンスという考え方）

2011年発行　Engineering a Safer World（MIT:Nancy Leveson）翻訳中



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

米国の潜水艦の戦闘外の事故の歴史とSUBSAFE発足（1963年）

原子力潜水艦スレッシャー号の事故：1963年4月10日、深海潜水テスト中に、112人の要員と17名の民間人を乗せたまま沈没し、全員が亡くなった。

SUBSAFEプログラム（1963年6月3日に創設され、同年12月20日に発布）開始後、事故は一度も起こっていない。（たった半年で開発・発布）

SUBSAFEプログラム開始後の唯一の事故（1968年スコーピオン号）は、冷戦のプレッシャーで監査対象外であった。

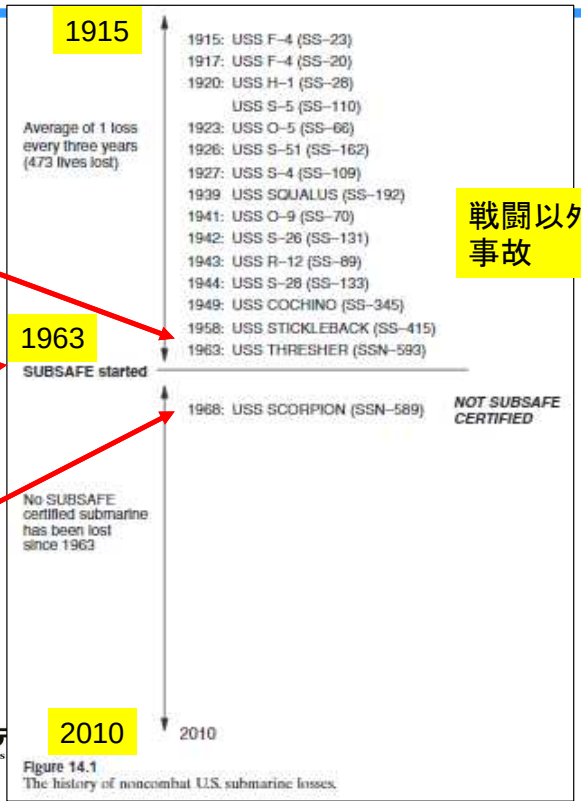


Figure 14.1
The history of noncombat U.S. submarine losses.

戦闘以外での事故

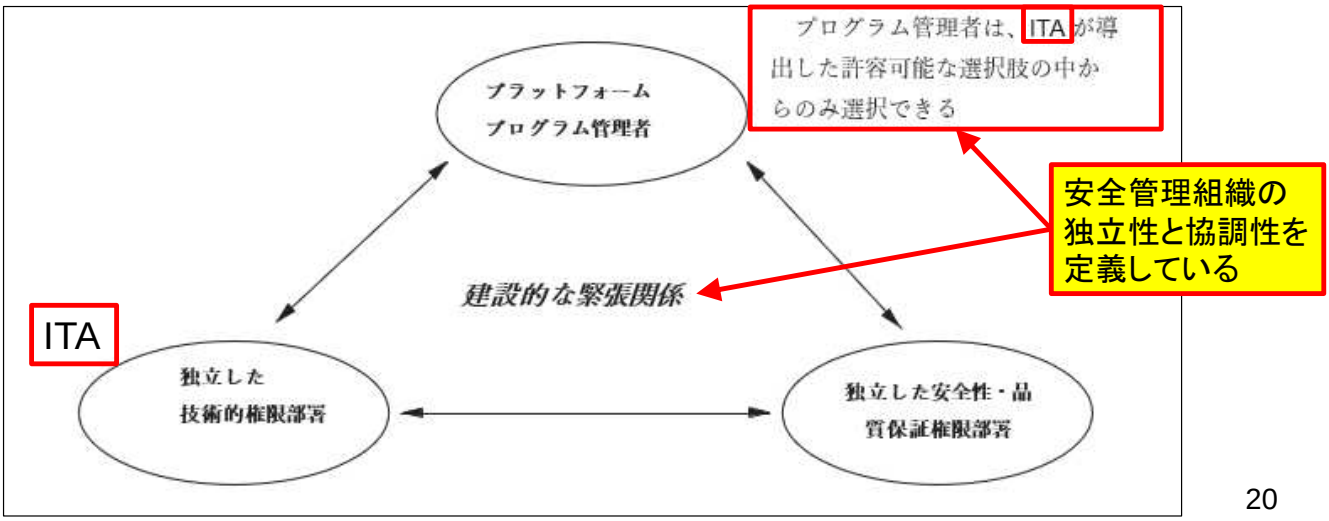
一般社団法人 組込みシステム Japan Embedded Systems

スレッシャー号の事故詳細

- The accident was thoroughly investigated including, to the Navy's credit, the systemic factors as well as the technical failures and deficiencies.
  - この事故は、海軍の威信をかけて 、技術的な失敗や欠陥だけでなく、システミックな要因 も含めて徹底的に調査された
- 事故の直接要因と組織要因
  - （直接要因）溶接の代わりに銀ろう付けに頼っていた塩水配管システムの接合部の欠陥が、エンジンルームの浸水を引き起こしたが、乗組員は浸水を止めるために重要な設備にアクセスすることができず、浮上もできなかった。対策として、隔離バルブを中央操作パネルから遠隔で閉じることができる浸水制御レバーを設置するよう提言した。
  - （組織要因）調査結果からは、仕様・建造体制・保守実施体制の不備、不適切な建造・保守活動の文書化、さらには、運用手順の不備が見つかった。その一例として、スレッシャー号では3000箇所の銀ろう付け配管の継ぎ手があり、最後の造船所での保守の際、これらの継手のうち145個が超音波テストで点検され、その14%が規格をはずれた接合状態であることが分かった。この結果から船全体では400以上の継ぎ手が規格外であった可能性がある。この状態で、船は出航することが許された。

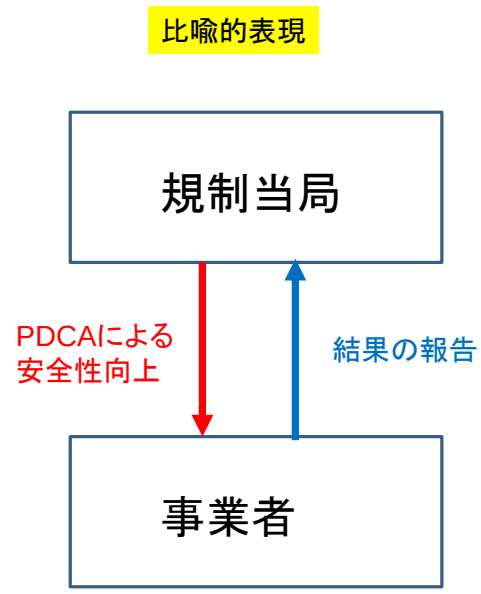
SUBSAFE 権力の分離（「3本脚の腰掛」）

SUBSAFE has created a unique management structure they call *separation of powers* or, less formally, the *three-legged stool.*
→SUBSAFE は、「権力の分離」と呼ぶ独自の管理体制を構築した。わかり易く言い換えると、3本脚の腰掛のように、独立した脚（権力）で安全を支える仕組みである。
This management structure only works because of support from top management
→この管理体制は、経営上層部からの支援があって初めて機能する。



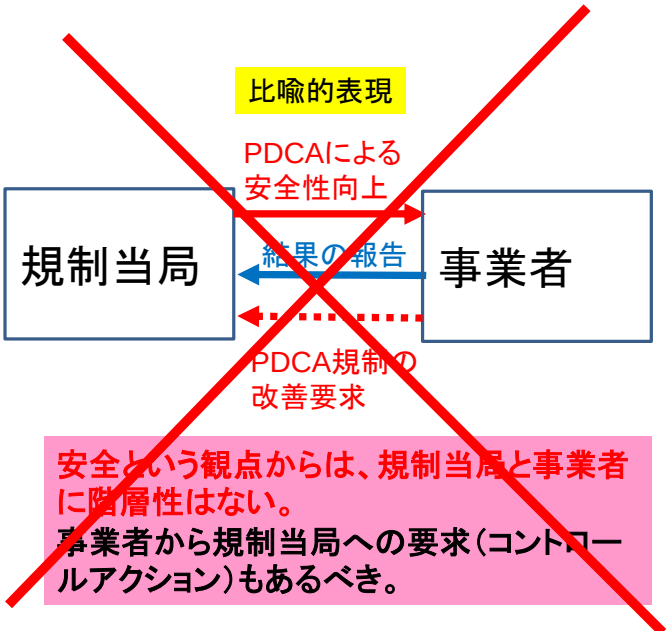
監査手順とアプローチ（下位から上位へのCA）

A biennial NAVSEA internal audit gives the field activities　a chance to evaluate operations at headquarters. Headquarters personnel must be willing to accept and resolve audit findings just like any other member of the nuclear submarine community.
→隔年で行われるNAVSEAの内部監査の中で、**現場活動の一つとして、本部の指揮・運用を評価**する機会が生まれた。 本部要員は、他の原子力潜水艦共同体のメンバーと同じように、監査結果を受け入れ、解決する姿勢が必要になった。



監査手順とアプローチ（下位から上位へのCA）

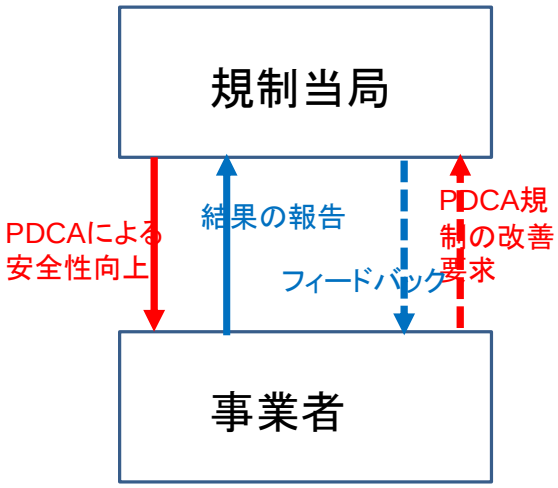
A biennial NAVSEA internal audit gives the field activities　a chance to evaluate operations at headquarters. Headquarters personnel must be willing to accept and resolve audit findings just like any other member of the nuclear submarine community.
→隔年で行われるNAVSEAの内部監査の中で、現場活動の一つとして、本部の指揮・運用を評価する機会が生まれた。 本部要員は、他の原子力潜水艦共同体のメンバーと同じように、監査結果を受け入れ、解決する姿勢が必要になった。



監査手順とアプローチ（下位から上位へのCA）

A biennial NAVSEA internal audit gives the field activities a chance to evaluate operations at headquarters. Headquarters personnel must be willing to accept and resolve audit findings just like any other member of the nuclear submarine community.
→隔年で行われるNAVSEAの内部監査の中で、現場活動の一つとして、本部の指揮・運用を評価する機会が生まれた。 本部要員は、他の原子力潜水艦共同体のメンバーと同じように、監査結果を受け入れ、解決する姿勢が必要になった。

比喩的表現



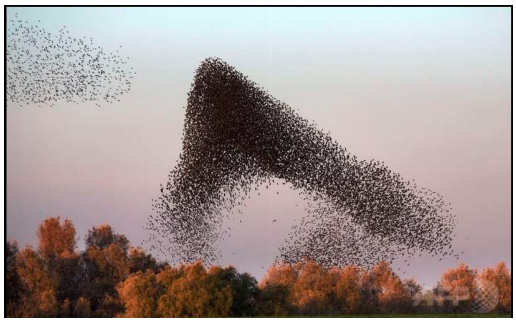
安全責任の階層性は変わらない。しかし、安全という観点からは、下位から上位への要求（コントロールアクション）もある。その場合、その要求にどう答えたかのフィードバックも必要（義務）になる。
安全責任の階層性から下位から上位への要求はやりにくいが、それへのフィードバックはさらに難しくなる。

何故、14章　SUBSAFEの事例か？

- 米国原子力潜水艦の安全プログラムなのに・・・
  - 原子炉の安全については、何も述べていない
  - STAMPの教えを体現している成功例なのに、制御構造図も非安全コントロールアクション（UCA）もほとんど記載がない
  - しかし、驚くほどの成功を収めている
- 安全プログラムSUBSAFEの成功要因は・・・
  - 安全管理を、機械の故障だけに留めず、組織の在り方まで立ち入って見直したこと。（1963年という時期にここまで考えた！）
  - 組織と権力の独立性と協調性を明確に定義。組織の階層性についても、下位から上位へ要求する機会を設けた。
  - 安全目標を明確に設定した。事故の防止ではなく、緊急時にも確実に浮上して帰港することを目標（レジリエンスという考え方）

創発事象の事例：鳥の編隊飛行

～先頭に追随する鳥は飛行の省エネを目指している。ミクロシミュレーションで説明可能 ～



ムクドリの群れ

ガンの編隊飛行

盗難防止用ロックシステムのついたレンタカーのトラブル例（ワシントン州でのカーフェリー内）

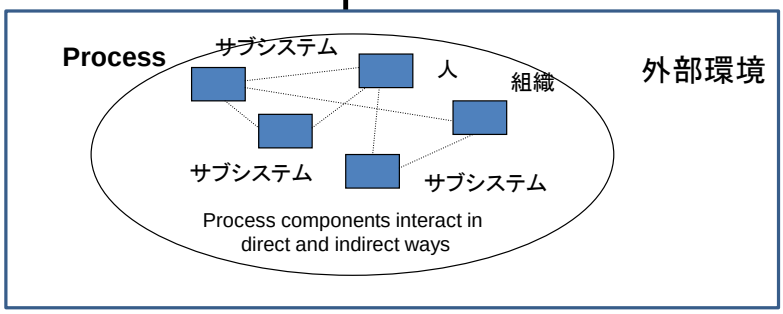
レンタカー盗難防止のため、エンジン停止時に車が移動すると、車を運転できないようにロックする機能が、レンタカー管理会社により設置されていた。
カーフェリーで移動した際、このロック機能で運転不能になった。レッカー車で車を移動するまで、フェリーが運航中止を余儀なくされた。
→設計段階での要求仕様の欠陥で、システムコンポーネントの故障ではない。
→管理会社にとっては便利な機能だが、レンタカー利用者やフェリー運航者といった関係者（ステークホルダー）にとっては問題のある機能である。
→コンセプト設計段階で、ステークホルダーが誰か、それぞれの損失が何か、を分析していれば、防げたトラブルである。（設計欠陥ともいえる）
→N.Levesonは、この事例も創発事故の一例として上げている。（コンセプト段階での検討の未熟さが余計な損失を生む）

複雑システムの安全とセキュリティ：創発特性
～複雑システムの事故は、創発的（想定外）に起こる～

Emergent properties（創発特性）
(arise from complex interactions)

Emergent Property:
“The whole is greater than the sum of the parts”

複雑な相互作用に
起因する創発的特性



Safety and security are emergent properties

Sec-Seminar(2015.6.18) Lecture by Nancy Leveson

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

“The whole is greater than the sum of the parts”
をどう解釈するか？

物理の理論では、個の集合で全体が成り立つ。しかし、個の集合で説明できない事象が多く発見され、それを「創発」と名付けた。

しかし、ミクロの計算科学の進歩で説明できる事象も多くなった。工学的には、多くの場合、個の相互作用を解明し、全体の創発事象を説明・制御し、問題解決をしている。（後知恵で解決）

個の相互作用や複雑性に対する知識不足は、事故後の後知恵で考えると、設計欠陥とみなされることもある。

ではどうするか？

Emergent Property:
“The whole is greater than the sum of the parts”

個の相互作用や複雑性に対する知識不足は、事故後の後知恵で考えると、設計欠陥とみなされることもある。

意図した機能の性能限界、合理的に予見可能なミスユースなどを丁寧に考えて設計する
（ISO21448/SOTIF）

できるだけWorst Caseで考え、最悪の事故を避けるように設計する（レジリエンス工学）

想定外を想定して設計する（STAMP/STPA）
◆UCAを利用して漏れのない設計をする
◆システム全体を俯瞰的にとらえて、最悪の事態を防ぐ安全制御メカニズムを実装する
◆安全制御構造図で安全を可視化してステークホルダー間で相互レビューする
◆抽象化と階層化を利用して対象システムをステークホルダー全員が理解できるように表現して、安全であることを相互レビューする

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

まとめ

- 還元論（Reductionism）
  - FTA、FMEA、HAZOPなどの信頼性工学に基づく安全分析
  - 設計が決まった後の安全分析法
- 全体論（Holism）・創発論（Emergence）
  - システム全体を包括的に捉えたシステミックな安全分析法（複雑システムの安全は創発的である）ー＞***STPA***
    - ー 抽象化と階層化により安全構造を可視化した安全制御構造図により安全分析を行う（多様なステークホルダーによる安全構造レビュー）
    - ー 階層的安全責任の明示化、安全制御指示の明示化
    - ー 概念設計段階での安全の作り込み（安全要求仕様）
    - ー 安全論証としてのエビデンス化
  - 創発的事故も後知恵で分析すれば還元論で説明できる（創発的事故を想定外として追及をあきらめてはいけない）ー＞***CAST***

ご静聴ありがとうございました。

ご質問等、興味があれば、JASA安全性向上委員会（https://www.jasa.or.jp/tech/safety/）へアクセスください。
安全設計ガイド、STAMP等に関するリモートセミナー、個別のオンサイトセミナーなどを実施しております。

JASA事務局
TEL: **03-6372-0211**　　Email: jasainfo@jasa.or.jp