一般財団法人日本科学技術連盟
第36年度ソフトウェア品質管理研究会
成果発表会 2021年2月26日(金)

システム思考とレジリエンスエンジニアリングを用いた安全性分析の試行

第6分科会 研究コース6　セーフティ&セキュリティ

研 究 員:
吉田　篤(東芝)
藤原　真哉(NTTコミュニケーションズ)
里富　豊(リコーITソリューションズ)
鎌田　桂太郎(アイホン)
黒田　知佳(テックエンジンソリューションズ)
松崎　美保(TIS)
大森　裕介(エプソンアヴァシス)
西　啓行(富士通)

主　査 :金子　朋子(国立情報学研究所)
副 主 査:髙橋　雄志(日本AIシステムサービス)
アドバイザー:佐々木　良一(東京電機大学)

目次

- チームメンバ紹介
- 背景
- 課題／仮説
- 課題解決のアプローチ
- 提案内容
- 効果検証
- まとめと今後の展開

チームメンバ紹介

	名　前	所　属	部 署	開発対象	一言
CASTチーム	大森　裕介	エプソンアヴァシス	設計	SW全般	学んだ分析手法を身につけたい
	鎌田　桂太郎	アイホン	品質保証部	インターホン	色んな考えもあり、楽しかったです
	里富　豊	リコーITソリューションズ	IT検証部	SW全般	一度くらいリアルで会いたかった
	松崎　美保	TIS	品質部門	サービス、SW全般	リアルでお会いしたかったです
	吉田　篤	東芝	品質部門	SW全般	一年間楽しく活動できました
STPA／FRAMチーム	西　啓行	富士通	品質保証・セキュリティ・ビジネス開発	システム全般	いつか会えること楽しみにしております。
	黒田　知佳	テックエンジンソリューションズ	製造1部	客先維持業務支援	1年間ありがとうございました
	藤原　真哉	NTTコミュニケーションズ	企画部門	情報システム	メンバーに一度も会えない想定外の活動でしたが勉強になりました

技術習得を目的に集まったメンバ（８人）

背景

AI・IoTを始めとした技術の革新により，多様性があり複雑な構成を持つシステムが登場してきている．

我が国でも政府主体で自動走行ビジネス検討会を立上げ，自動走行の実現に向けた取組報告と方針が発表されている．

自動運転の例では，自動車に先駆けて航空宇宙分野や鉄道などで運用されているが，いくつもの事故事例が報告されている．

事故事例の多数は，想定外の事象によって発生

課題／仮説

想定外の事象によって引き起こされる「事故の未然防止対策」の検討不足が問題点と感じ，経時的な問題の抽出や要素間の関係性の図示，成功要因からの**安全性分析の拡充が課題**であると考えた．

刻一刻と変化する環境や技術への対応，複雑なシステム要素間の関係性の理解等が必要であり，失敗要因からの分析だけでは想定できる状況に限りがあると考え，**従来の分析（FTA，FMEA，なぜなぜ分析等）とは異なる新しいやり方を用いることで解決できると考えた．**

安全性分析への取組み（新しいやり方が必要）

課題解決のアプローチ

AIを含むシステムの安全性分析を行うことで，想定外を想定する分析方法への挑戦・検証　（本研究の実験では，事故報告書に記載されていない内容を想定外と位置付けている）

従来の分析（FTA，FMEA，なぜなぜ分析等）とは異なる特徴を持つ，以下の安全解析手法を用いて，多角的な分析を行うことで課題解決を進められると考えた。

- **システム理論を用いた分析：STAMP**（Systems Theoretic Accident Model and Processes）
- **レジリエンス分析：FRAM**（Functional Resonance Analysis Method）

①事後分析

事故理由及び事故発生を許した安全制御構造の弱点を，経時的な変遷を含めて明らかにすることを目的に**STAMP/CAST**（以降CASTと記す）を用いた。

②リスク分析

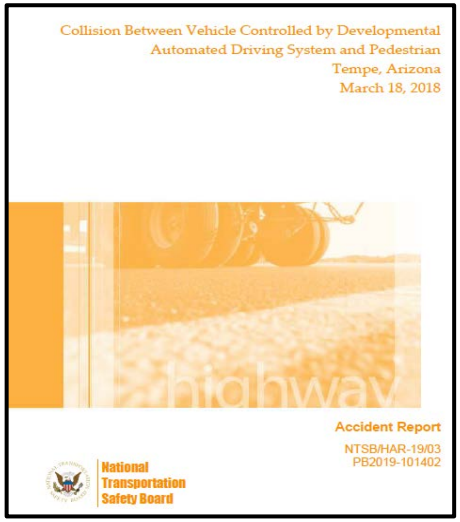
- 事故事例のシステム構成をもとに想定外のリスク抽出を目的に**STAMP/STPA**（以降STPAと記す）を用いた.
- 各機能がどのように影響しているかを分析し、システムの失敗要因を定義せず，成功要因に着目することで、総合的な安全性を導出することを目的に**FRAM**を用いた.

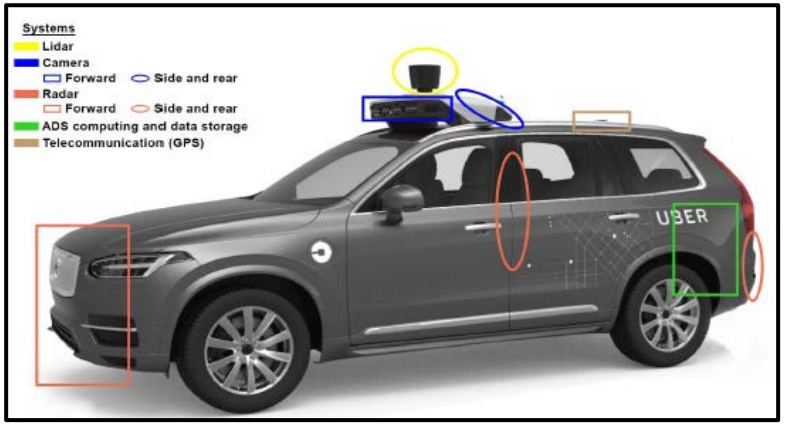
システム理論を用いた分析，レジリエンス分析の適用

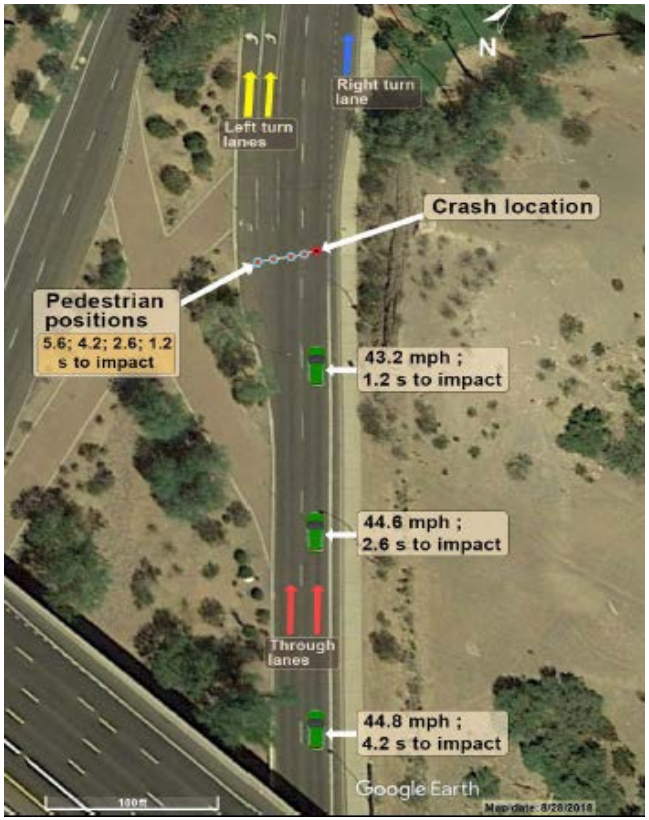
課題解決のアプローチ

＜具体的な事故事例＞

2018年3月にアリゾナ州で発生した**Uberの自動運転システム**の事故事例を用いた．**事故報告書に記載されている改善勧告と我々が導出した改善勧告内容との比較を行い有効性を確認する．**







事故報告書：Uber_Accident_report.pdf　／　参照動画：www.youtube.com/watch?v=SDZFkhd6OMs

提案内容（CAST分析から導出したこと）

＜CAST手法の概要・特徴＞

【CAST】(Causal Analysis based on System Theory)

・CASTはSTAMPに対し，事故全体の理解のためのフレームワークとプロセスを提供する.

・CASTを用いることで，**人を含むシステム構成の関係性や，システムが置かれた状況(コンテキスト)を考慮した事故分析ができる**と期待されている.

【STAMP/S&S】(System Theoretic Architecture Model and Process S&S)

・従来のSTAMPを拡張した考えを提供する.

・S&Sは，Safety ，Securityの他，**Society，Stakeholder，Service，System，Softwareの5階層のアーキテクチャ**と，Specification，Standard，Scenarioの略称を指す.

・従来のSTAMP事例ではシステムレベルが中心であり，自然や社会環境,ソフトウェア等の特徴にあわせた詳細な相互分析までは触れられていない.

上記の特徴から本手法が，事故分析に適用できると考え，Societyから Softwareに至るまでの階層において**「法制度」，「AIシステムを含む複雑な構成要素」の関係を考慮した分析**が可能になると考えた.

新規性の試みとしてCASTとSTAMP/S&Sを組合わせて分析

提案内容（CAST分析から導出したこと）

＜CASTを用いた分析結果＞

CAST分析で導出された改善勧告のうち，想定外のものがないかを確認したところ、**想定外の改善勧告が18件導出できた.**

例）

①事故報告書については「人がルールを守る」，「人が自発的行動を起こす」前提の対策となっているため，事故の抑制かゼロにするのか目的・目標の明確化が必要

②安全性およびリスクに対する評価・冗長性に対してより積極的な対応が必要

③自動運転（レベル5等）レベルに応じた免許制度（ドライバー，搭乗者の役割・責任等）や道路環境の実現等の運用面や法整備への対応が必要

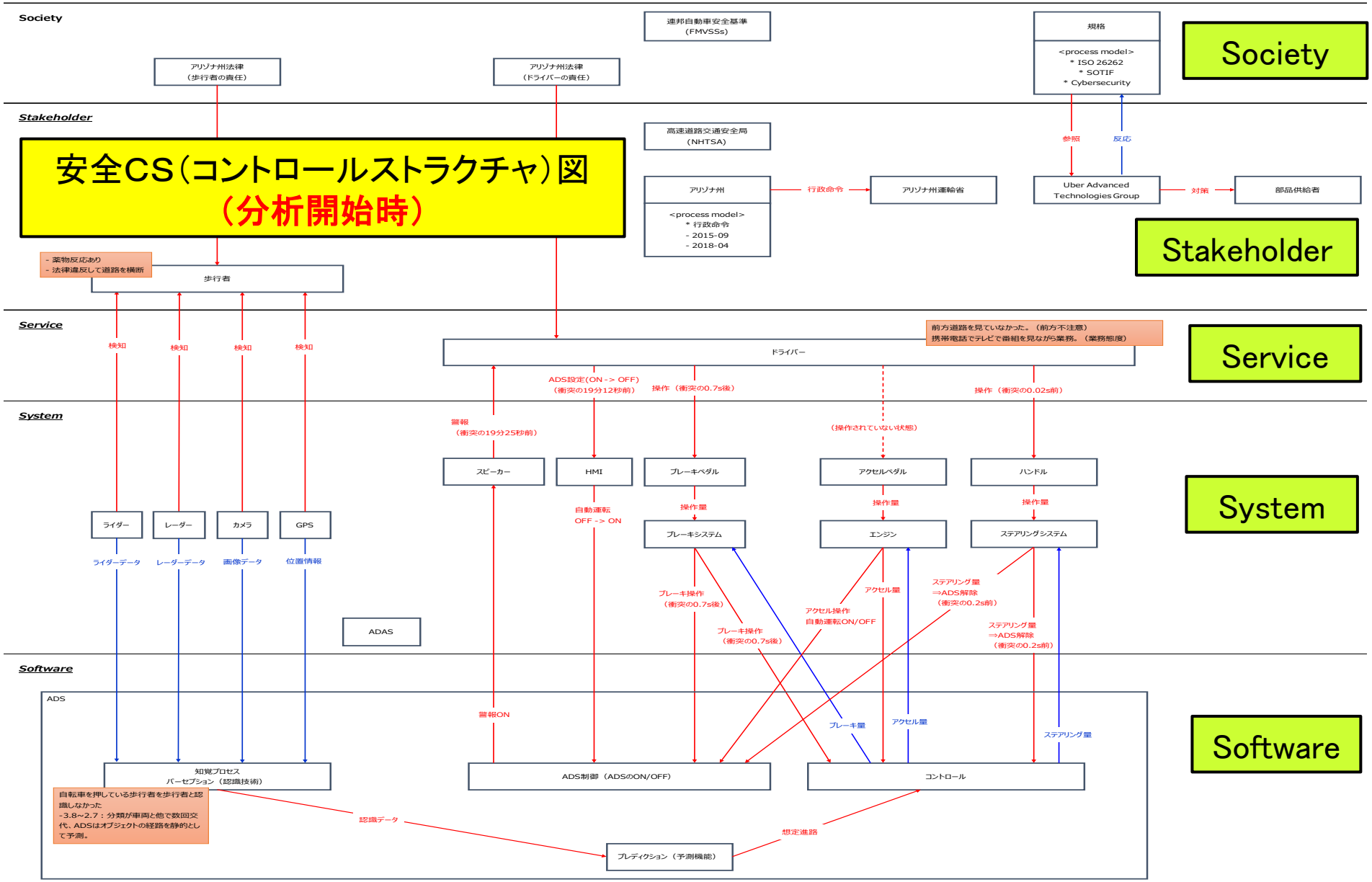
以上のことから，**CASTへの5階層モデルの適用及びAIシステムを含めた分析は，想定外を想定することができたと結論付けた.**

こんな工夫をしたよ！

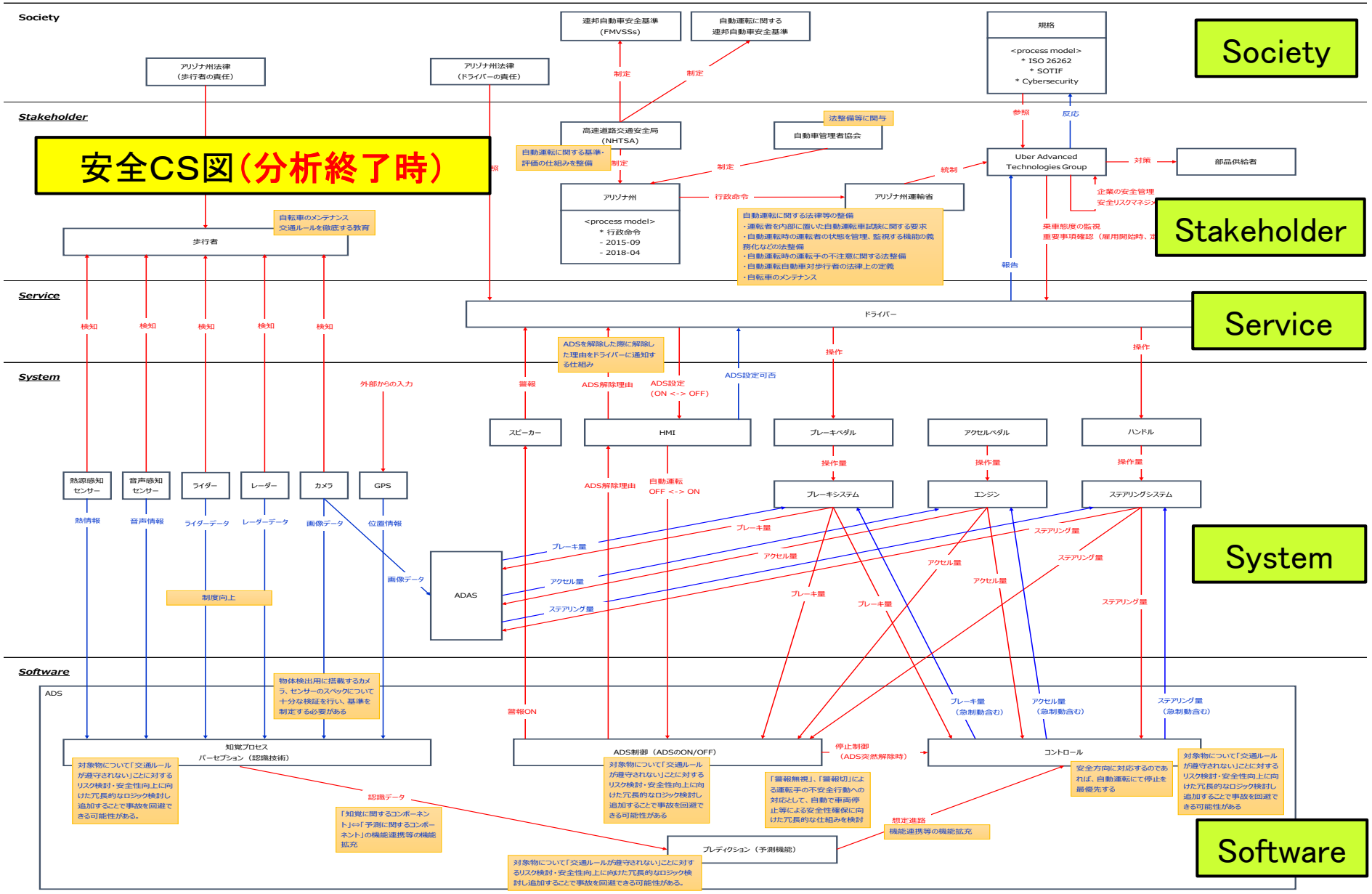
システム理論に基づく事故分析手法として過去事例にない「新規性のある試み」として STAMP/S&Sにおける5階層モデルのアーキテクチャを組込みこんだ。

CAST＆5階層モデルでシステム全体を広く俯瞰的に捉えられた

提案内容（CAST分析から導出したこと）



提案内容（CAST分析から導出したこと）



提案内容（STPA分析から導出したこと）

SQiP Software Quality Profession

＜概要・特徴＞

【STPA】（STAMP based Process Analysis）

STPA は STAMP アクシデントモデルを前提として，システムのハザード要因を分析する新しい安全解析手法である.

＜想定＞

STPA の手法により早すぎる遅すぎるというチェック観点からの経時的なハザード要因洗い出したり，また登場人物とハザードを照らし合わせ分析に不足がないかを繰り返し確認したりすることによって「想定外」を改善勧告することが出来るのではないかと考えた.

＜分析結果＞

①改善勧告を新規機能（聴覚、嗅覚、体感）に基づき導出することができた.

②「ディープラーニング，ネットワーク，サイバーセキュリティ，交通ルール，インフラ整備」等が抽出され改善勧告を洗い出した.

こんな工夫をしたよ！

ツールを使用し、登場人物とハザードを照らし合わせ分析に不足がないかを繰り返し確認

こんなことが注意点だよ！

ツールを使用したが、今回6人日程度の工数が掛かっている

STPAではガイドワードのサポートにより経時的な問題を捉えた

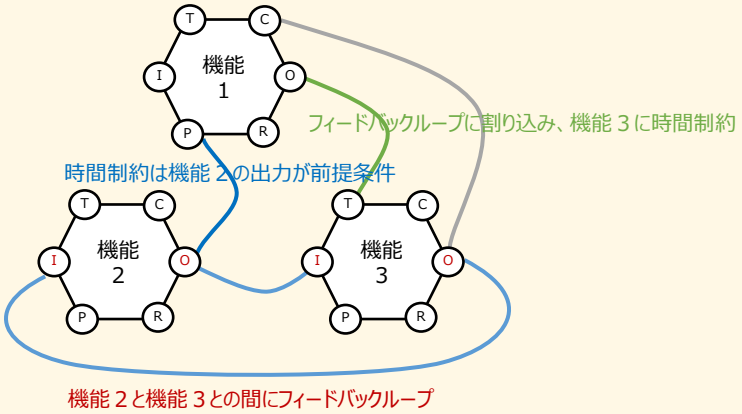
提案内容（FRAM分析から導出したこと）

＜FRAM手法の概要・特徴＞

◆FRAMとは、レジリエンス・エンジニアリングにおける分析手法であり、動的システムにおけるリスクの特定に用いられる。

◆機能と機能がどのように影響し、依存し、強め/弱めあっているか（機能共鳴）を分析
・個別のコンポーネントやデータではなく、**総合的な視点でネットワークトポロジーに着目する**
・システムの失敗要因を定義せず，**成功要因に着目する**

◆モデル図は機能を六角形で示し、各頂点を入出力として曲線で依存関係を表現する



I	Input	機能の開始トリガーとなる入力
P	Precondition	機能の開始の前提条件となる入力
R	Resource	機能に実施に必要な資源となる入力
T	Time	機能の実施の制約となる時間情報
C	Control	機能の実施方法を変える制御入力
O	Output	機能の出力

人間が運転するモデルから自動運転のモデルを創出することで、**自動運転システムの想定外のリスク分析に適用できる**と考えた。

人間の運転機能を自動運転に置き換えることでリスク要因を抽出

提案内容（FRAM分析から導出したこと）

＜FRAMを用いた分析結果＞
人間が運転する機能をFRAMによりモデル化し、人間の機能を自動運転に置き換えることで、事故報告書では想定外のリスク要因の観点が示された。

◆自動車の運転において「危険を予知」した際、安全面に配慮した「パッシング」、「クラクション」などを利用した外部環境とのコミュニケーションを取ることで、交通全体としての安全性が確保できる。（成功要因）
◆自動運転において、外部環境とのコミュニケーション機能が欠如している場合には、外部環境との**コミュニケーション断絶により、安全性が確保できない**可能性がある。（リスク要因）

以上のことから，**FRAM分析により，想定外を想定することができたと結論付けた．**

こんな工夫をしたよ！

・人間が運転する機能の分析過程では、目・耳・手・足といった、人体構造を分解して検討することで、発想が広がった。
・モデル作成時の抽象化の粒度がポイント。はじめは機能を詳細に分割し、徐々に入出力の共通機能を統合/入出力の少ない機能を省略して、抽象度を上げた。

FRAMでは成功要因に基づく新たな着眼点を得た

効果検証（考察）

＜CAST分析＞
5階層モデルを組み合わせることで，分析の軸や多数のヒントを得ることができ，より具体的な欠陥の導出，経時的な変化に対する欠陥が導出ができた．

＜STPA分析＞
ガイドワードが経時的な内容を示しているため，想定範囲が広がり，コンポーネント間の関係性を考慮することでハザード抜けが発生しにくく，ピンポイントで欠陥の導出ができた．

＜FRAM分析＞
成功要因を事例に反映する事で，新たな気付きが得る事ができ，レジリエンスエンジニアリングの有効性を確認した．

＜3つの分析の統合的な考察＞
・STPAとCASTのハザードを共通化することで連動した分析が可能では？
・システム思考とレジリエンスエンジニアリングの統合的な活用の可能性？
（FRAMの機能はアクションであり，STAMPの安全CS図におけるCAに相当すると考えることで連動できると考えた．）

各分析で効果と有効性を確認．特徴に応じた使い分けが必要

効果検証

今後の課題

(1)CASTを使う際のポイントは，損失に至った不適切な制御をいかに多く抽出できるかである．
（多くの利害関係者，事実情報，本来備わっているべきと考えられるコントロールアクション等）

(2)本実験では，自動運転レベル5を踏まえて検討できているかの視点では十分とは言えず，今後の課題となる．

(3)セキュリティ観点での分析が十分にできていない．
物理の世界とソフトの世界が融合されたシステムでは，セキュリティの検討が必要．

(4)システム思考とレジリエンスエンジニアリングの統合的な活用を行うための具体的な方法論の検討と構築が課題．

システム思考とレジリエンスエンジニアリングは新しい分野であり開拓の余地あり

まとめと今後の展開

実際の事故事例に対してCAST，STPA，FRAMを用いた分析を行い，事故報告書の改善勧告にない新たな弱点の抽出ができた.

経時的な問題の抽出や要素間の関係性の図示，成功要因からの安全性分析技術が有効であることを示した.

課題への取り組みと共に，研究を発展させていきたい

仲間
募集中

システム思考とレジリエンスエンジニアリングは有効（一緒に取組みませんか？）

おわり

ご清聴
ありがとうございました。

金子主査、髙橋副主査、佐々木アドバイザー
ご指導ご鞭撻ありがとうございました！
今後ともよろしくお願いします.

STAMP/CAST

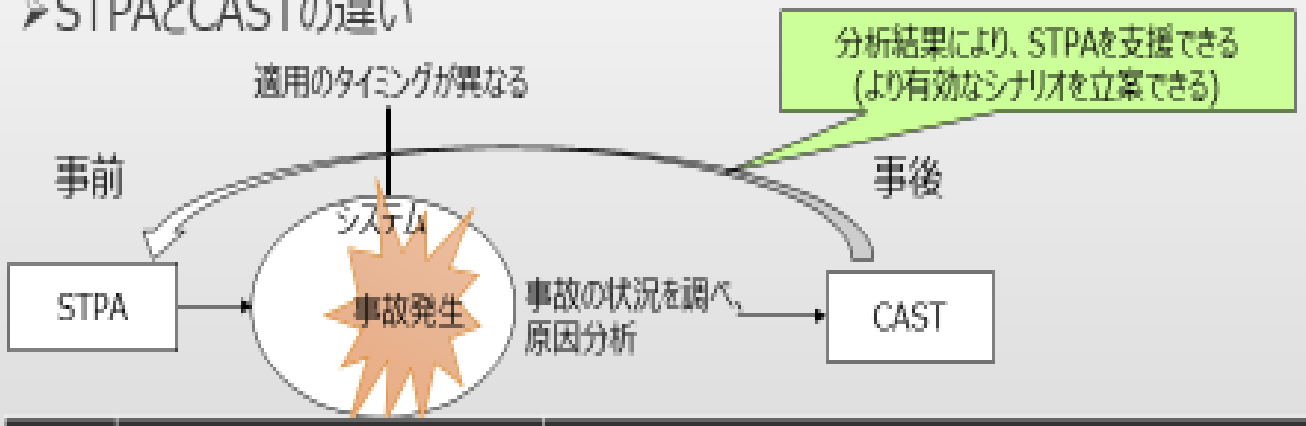
APPENDIX-A1

STAMP/CAST（Causal Analysis using System Theo

- 目的
  相互作用によって発生したハザードを分析する為（事後）

- 特徴
  さらなる損失を防ぐ為に排除または管理する必要があるもっともらしいシナリオ（弱点）を識別できる
  - 発生した特定のシナリオのみを識別できる
  - 安全制御構造の破綻にフォーカスし、先入観や偏見による影響や偏りを小さくする（後知恵の偏り防止）

- STPAとCASTの違い

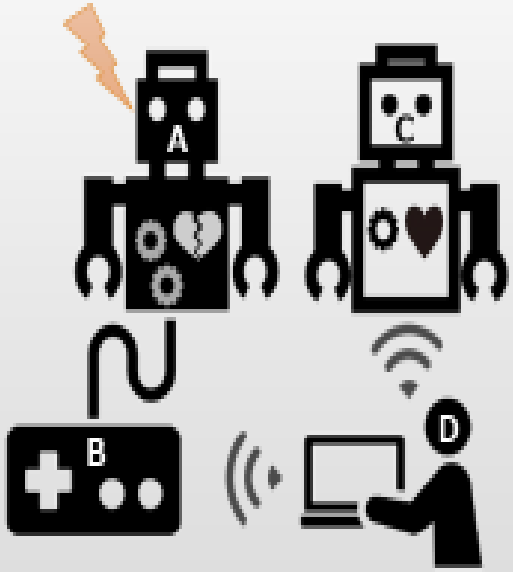


手法	作成するシナリオ	期待効果
STPA	潜在的なシナリオ	設計が作成される前に使用できる為、 セーフティ&セキュリティに関する開発コスト低減が可能
CAST	発生した特定のシナリオ	更なる損失を防ぐ為に、排除、管理する必要があるプロセスを特定することで、 STPAプロセスを支援可能。

STAMP/CAST分析手順

1. 不具合、事故情報の内容把握
   ① 損失に関与したシステムと分析対象の範囲を定義
   ② 識別したハザードからハザードを防止するために必要なシステムレベルの安全制約を特定
   ③ 損失につながるイベントチェーンを究明

STAMP/STPAと同じ



アクシデント	ハザード	安全制約
システムAの機器１の異常に対して、システムA内で対処できず、物理的に離れた組織Dで対処せざるを得ない事象が発生	システムA内の機器異常にシステムA自ら対処できない	システムA内の機器異常にシステムAが自動で対処すること

損失に近接する発生イベント (What?：何が起きたのか)	イベントが発生した理由の回答を求める質問を作成 (Why？：原因究明の為明らかにしたいこと)
機器3が異常を検知しなかった	何故、異常を検知できなかったか？
	何故、応答が一定期間内場合を設計しなかったのか？
	何故、異常を正常とみなしたのか？
	・・・

STAMP/CAST分析手順

2. 対象のシステム分析

① 重要なイベント(障害および安全でない相互作用)とこれらのイベントから生じる質問を特定して、物理的な設計の欠陥と状況要因を説明する

実際に損失があったコンポーネント単位で、以下の観点から分析

この事故の防止のためのすべての物理的な安全要件と制約を識別

物理的な装置のあらゆる故障もしくは不適切な制御を識別

物理的な故障もしくは不適切な制御を説明するコンテキスト要因を識別

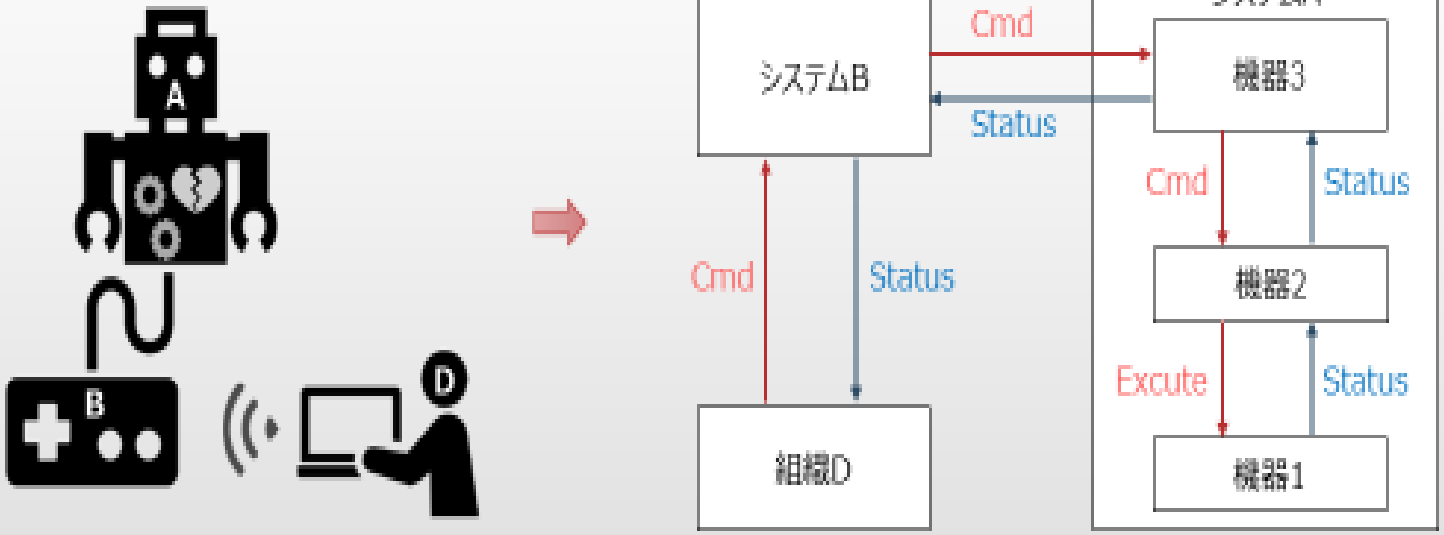
損失に関連するコンポーネント	安全上の責務	非安全なコントロールアクション	プロセス/メンタルモデルの欠陥	意思決定された状況・背景
機器3	機器2のステータスを監視し、異常が返ってきたら機器2に切替コマンドを発行する	異常が返ってきたのに、機器2に切替コマンドを発行しなかった	機器3の切替コマンド発行が無効になっていることを検知できない	数日前に、メンテナンス対応のため切替コマンド発行を無効にする設定にした後、そのままになっていた

STAMP/CAST分析手順

3. 安全コントロールストラクチャの作成

STAMP/STPAと同じ

① システムの構成要素間の構造と相互作用を表すために、既存の安全制御構造をモデル化する



STAMP/CAST分析手順

4. 論理モデルの分析

① 安全コントロールストラクチャで損失があったコンポーネントとその周辺のコンポーネントを抽象的事象と捉え、なぜ不適切な制御に寄与したかを解明

以下の観点から分析

- 抽象化レベルの制御に対する、安全制約の責務を識別
- 非安全な決定と制御アクションを識別
- 非安全な決定と制御アクションを説明するプロセスモデルの欠点を識別
- その時点でなぜその振る舞いが適切に思えたか説明するコンテキスト要因を識別

損失に関連するコンポーネント	安全上の責務	非安全なコントロールアクション	プロセス/メンタルモデルの欠陥	意思決定された状況・背景
機器3'	対象機器の状態を監視し、返ってくるステータスに応じてコマンドを発行する	ステータスに応じたコマンドを発行しない	コマンド発行を制御するための設定値が、通常運用時と異なっていることを検知しない	機器設定値の確認は変更者の責務とし別途運用ルールを定めていたため、システム的に検知する手段を備えていなかった

STAMP/CAST分析手順

5. 制御構造の欠陥特定

① 損失の原因となったシステミック要因を調査することで制御構造全体の欠陥を特定する。
システム全体を俯瞰し、手順2から4の結果から個々のコンポーネントが個々の安全責任を果たせなかった理由、コンポーネントの動作が一緒になってシステムの安全制約を満たせなかった理由を抽出

↓ 抽出後、システミック要因（経時的な変化とダイナミクス）に分類

- 情報交換と相互連携
- 安全な情報システム
- 安全なマネジメントシステムの設計
- 安全な文化

② 経時変化により劣化し事故に至る要因となった制御構造全体の欠陥を特定する。
手順2から4で抽出した欠陥から、システミック要因に当てはまる欠陥があるか確認する 。

情報交換と相互連携	安全な情報システム	安全なマネジメントシステムの設計	安全な文化	経時的な変化とダイナミクス
機器の設定を通常運用から変える際の運用ルールが周知できていなかった	設定値変更時の作業記録及び通常運用時の設定値の正当性を照合する機能がなかった	機器設定を変えた後に元に戻すことの確認をとるプロセスがなかった	メンテナンス作業が運用に与える影響を精査せずに作業する風土があった	当初は厳格なルールで運用していたが、作業効率の低下を招くため、現場作業者の判断で逸脱する状況になっていた

STAMP/CAST分析手順

6. 改善勧告（案）の作成

① 将来同様の損失を防ぐために、統制構造の変更に関する推奨事項を作成。
機器やオペレータ、さらに組織といった要素から成るコントロールストラクチャを、
どう変えると欠陥を防止できるか提言する。

欠陥	改善勧告（案）
自身の状態が異常であることを検知しない	通常運用とかけ離れた機器状態が続く場合はアラートを出す仕組みを入れる
機器の設定を通常運用から変える際の運用ルールが周知できていなかった	メンテナンス等で機器設定を変える際の作業/運用ルールを運用チームで教育する
機器設定変更の作業記録を残すデータベースがなかった	機器設定変更の作業記録データベースを用意し、運用チームで共有する
…	…

STAMP/STPA

APPENDIX-A2

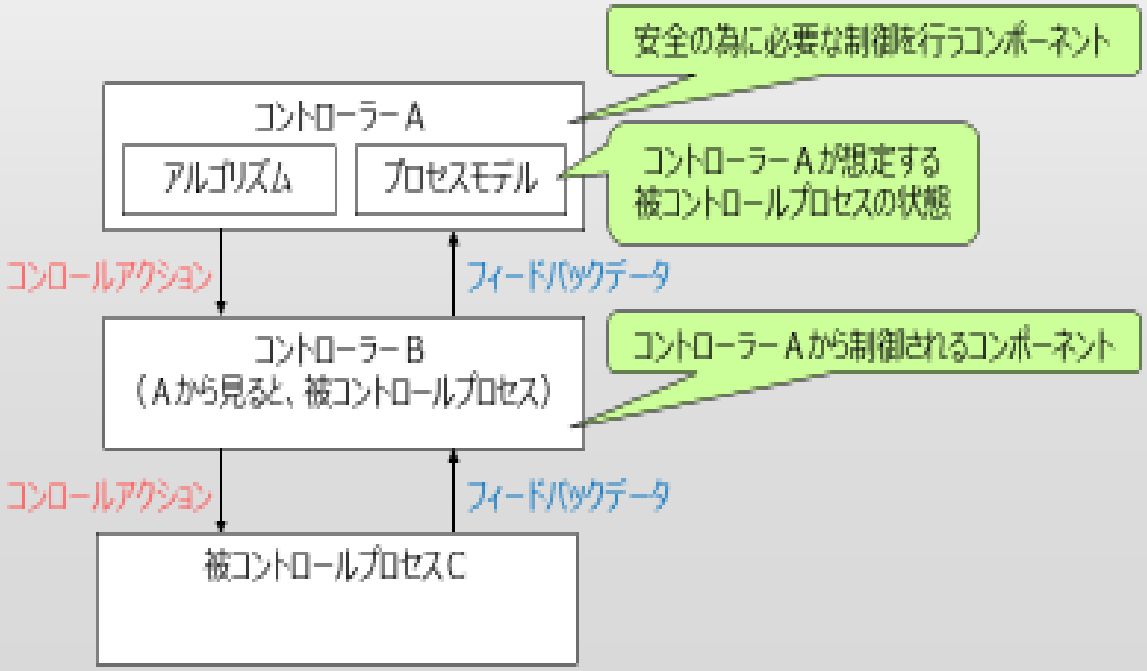
STAMP/STPA（Systems-Theoretic Accident Model and Process

Software Quality Profession

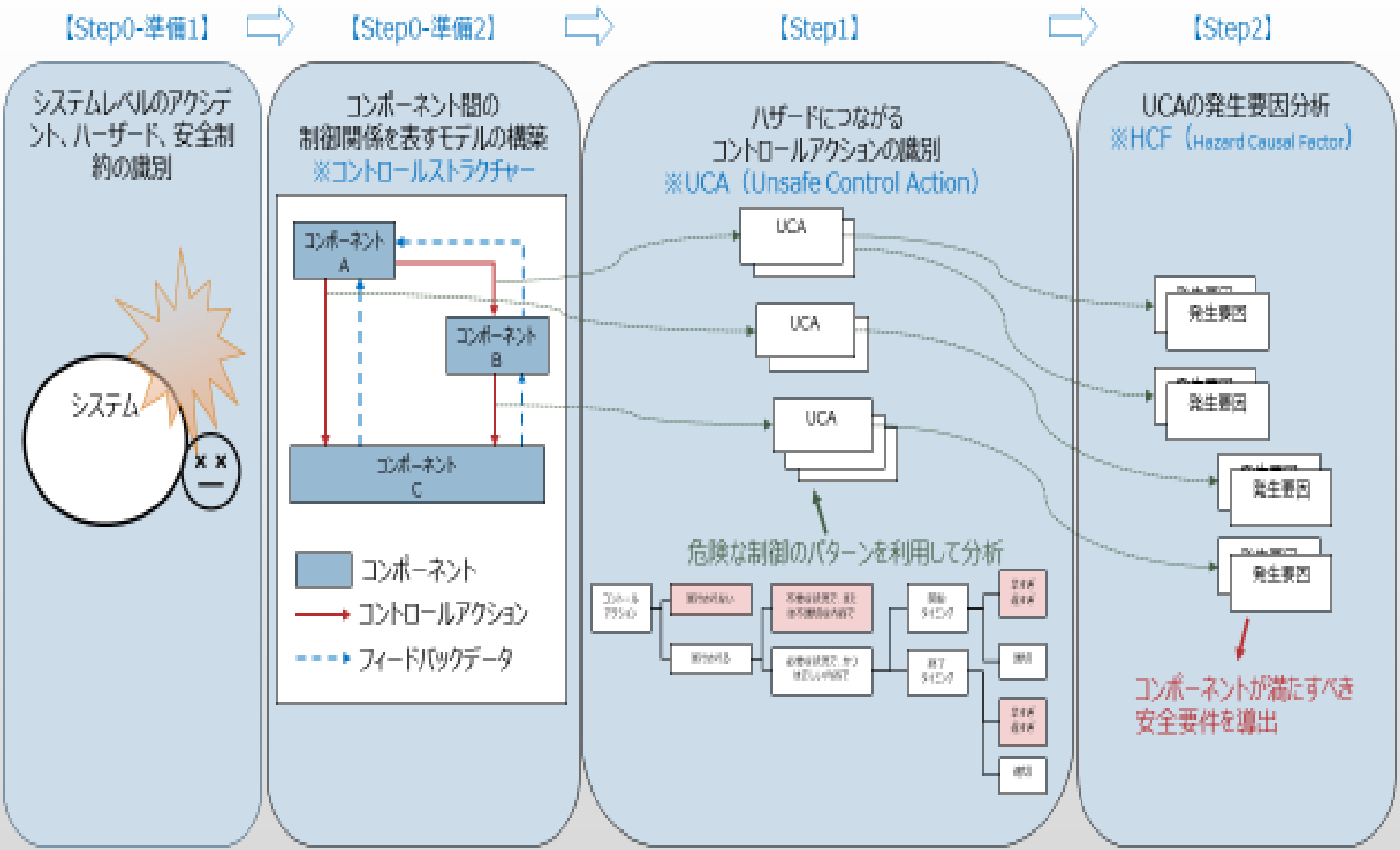
- 目的
  相互作用によって発生するハザードのリスクを分析する為（事前）

- 特徴
  システムを安全に維持するための相互作用に着目して網羅的に確認することで想定外を削減
  - コンポーネント間のインターラクション異常に着目する
  - システムの大まかな構成要素が決まる概念設計の段階から適用できる

- モデル図（コントロールストラクチャー図）



STAMP/STPA分析手順



詳細は、「はじめてのSTAMP/STPA」を参照。https://www.ipa.go.jp/files/000055009.pdf

FRAM

APPENDIX-B

FRAM

目的

システムの成功要因と、そこから導かれるリスク要因を発見する為

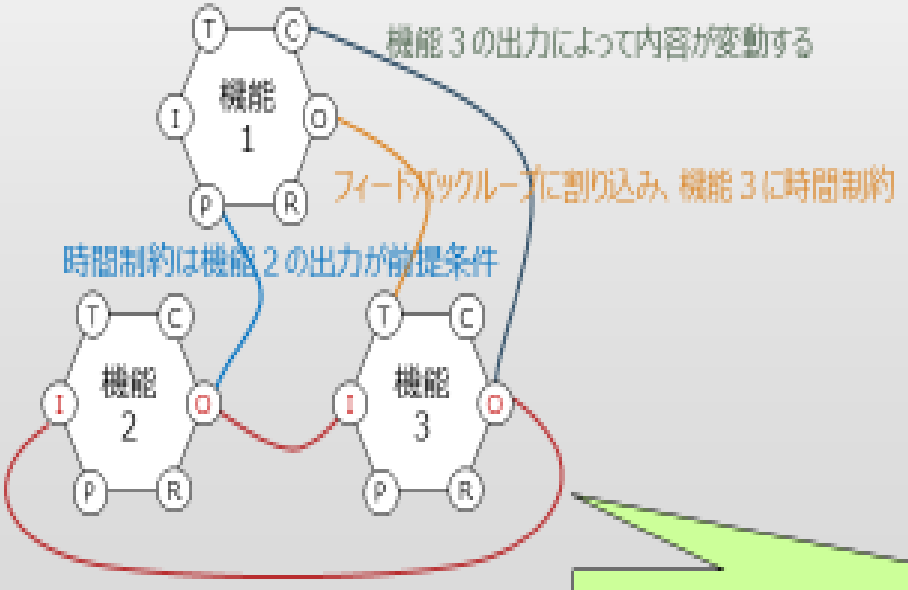
特徴

機能と機能がどのように影響しあい、依存しあい、強めあい、弱めあっているのか（機能共鳴）を分析

- 個別のコンポーネントやデータではなく、統合的な視点でネットワークトポロジーに着目する
- システムの失敗要因を定義せず、成功要因に着目する

事故は故障やミスから起こらないというのが最近のトレンド

モデル図



I	Input	機能の開始トリガーとなる入力
P	Precondition	機能の開始の前提条件となる入力
R	Resource	機能に実施に必要な資源となる入力
T	Time	機能の実施の制約となる時間情報
C	Control	機能の実施方法を変える制御入力
O	Output	機能の出力

機能１，２，３でダイナミックな共鳴関係が築かれている
不意なタイミングで機能３が処理時間超過となるリスクがあることを読み取れる

FRAMの分析手順

1. モデリング手順

① 質問による機能の把握

機能の６要素を網羅的に分析する。
この網羅性によって、機能間の相互作用の見落としがないことが保証される。

その機能の目的は何か？
機能はどのような処理を行っているか？
機能にはどのような入出力が存在するか？

機能概要が把握できたら、詳細を把握する

I	その機能の開始トリガー（入力）は何か？
	条件が変わった場合、どのように適応するか？
	正常でない条件にどう反応するか？
R	リソースは安定的に供給されるか？不安定要因は？
	外部環境はどのくらい安定？不安定要因は？
	正常でない条件はたびたび発生？
P	「当然」と思われている前提条件はあるか？
T	時間制約によるプレッシャーはどこにかかるか？
	特別なスキル，特別な高機能，特別な高信頼性を必要とする個所は？
C	最適な実行方法というものが存在しているか？

FRAMの分析手順

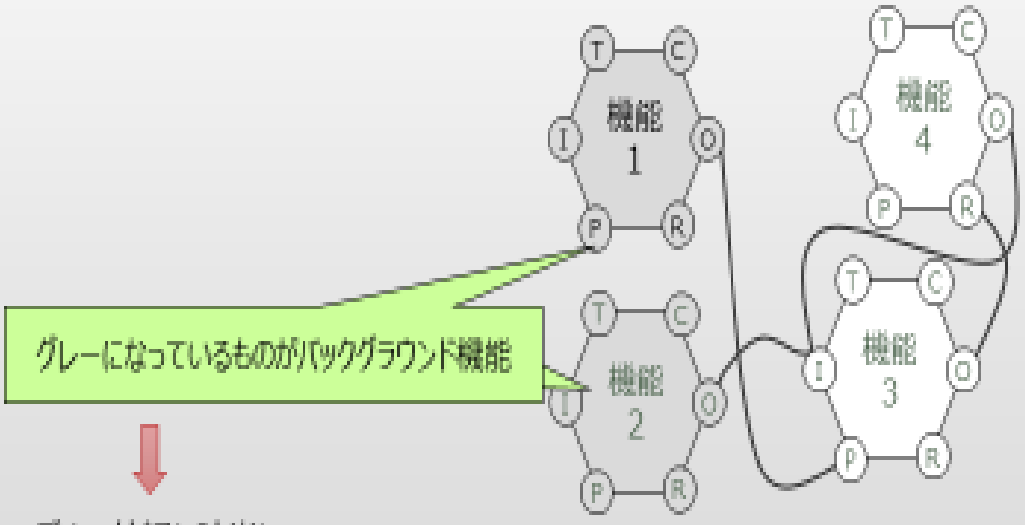
② 各機能の定義

各要素の名前（やりとりされる情報・データ・もの・締め切り時間）

相手の機能の名前

③ モデルの可視化

FRAM Visualizerで行う。(http://functionalresonance.com/FMV/index.html)



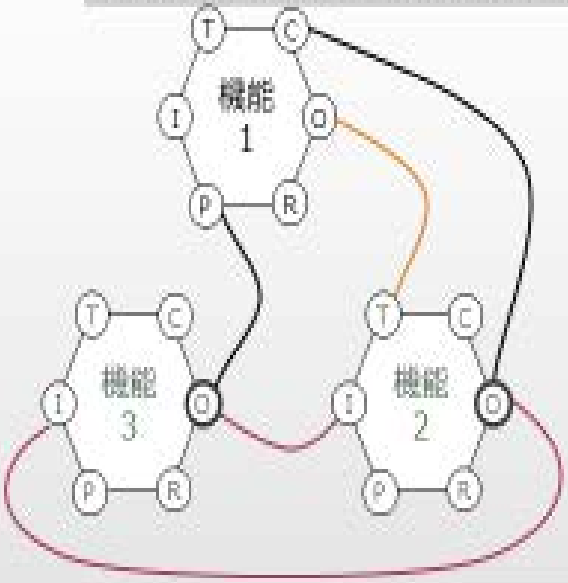
モデルの外縁に該当し、
注目する機能からバックグラウンド機能までがFRAM分析の対象となる

FRAMの分析手順

④ 可視化したモデルを使った分析

このシステム（モデル化した範囲全体）の成功要因は何か？

成功要因を識別し、それを育てると共に、成功要因の実現を阻むリスクを抽出する為、必ず先に成功要因を分析すること



機能2や機能３からの放射線状の出力

機能3と機能2の間のループ構造

機能1と機能2の間のループ構造

機能3から機能2・機能1を経由して機能3に帰る大ループ構造

機能3と機能2は通常はシーケンシャルに処理を行っており、
機能1からの時間制約が発生しても、機能3、2の処理順序逆転することがない。
（必ず順番が守られる）
これが成功要因の1つ。

このシステムのリスク要因は何か？

機能2は時間制約あり。制約を満たせない場合、ストップする

機能2の停止により、機能3は開始トリガーを失う

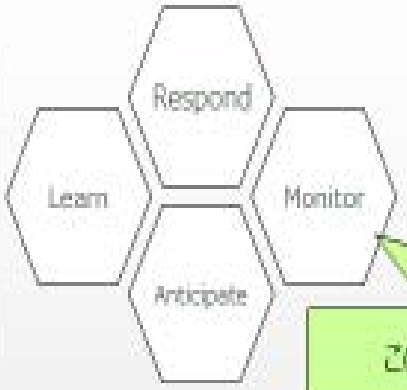
機能3がタイムアウトを検知して再実行するとしたら、その時の機能2はどのような状態か？機能2が停止している状況で動作できるのか？

成功要因の分析からリスク要因の分析につなげることが重要

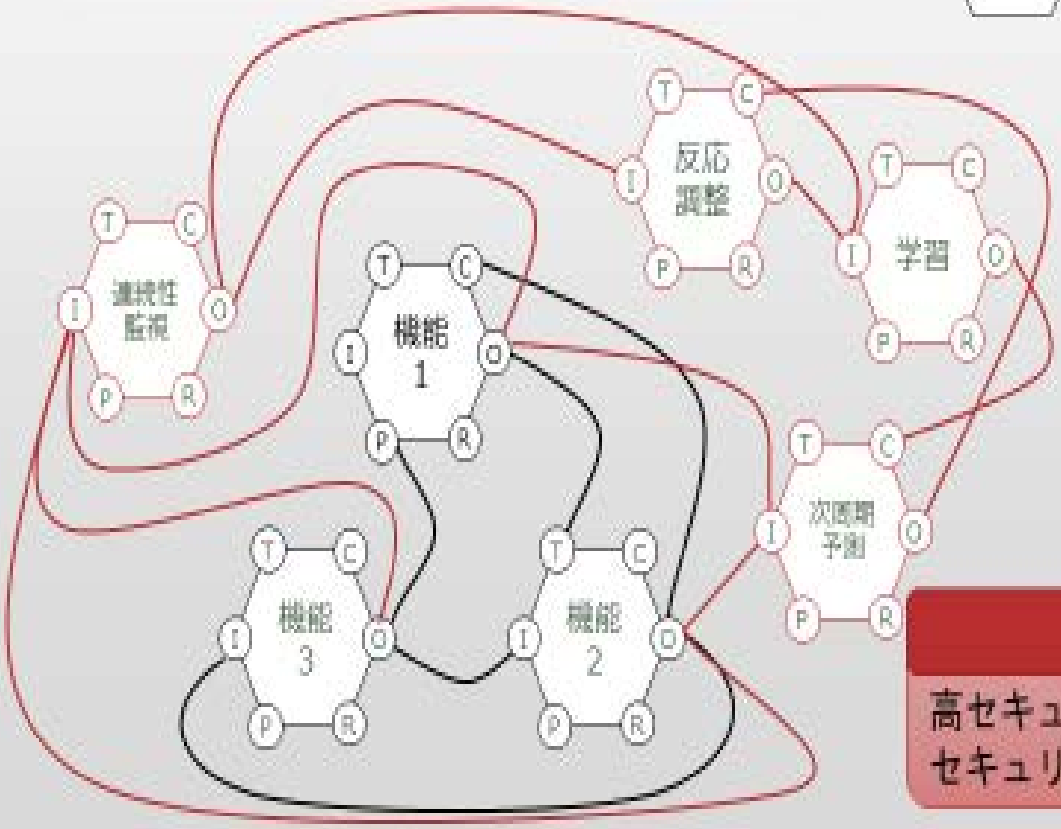
FRAMの分析手順

2. レジリエンス機能の追加

Monitor	危険な予兆を察知する能力
Respond	予兆に素早く反応できる能力
Learn	過去の成功・失敗から学ぶ能力
Anticipate	将来のリスクを予測する能力



この4機能により、乗っ取りに対してきわめて強靭になる



レジリエント・セキュリティの実現

高セキュリティ＝高パフォーマンス
セキュリティとパフォーマンスのトレードオフからの脱却