原子力安全セミナー

宇宙分野における安全評価手法（STPA、FRAM）の紹介

2025年10月

有人宇宙システム株式会社
安全ソリューション・審査ユニット

アジェンダ

Japan Manned Space Systems Corporation
JAMSS
ひとと宇宙を結ぶインテグレータ

1. 安全解析技術の動向

2. 安全解析手法(STPA : System-Theoretic Process Analysis)
   2.1 STPA概要
   2.2 STPA適用事例

3. レジリエンス解析手法(FRAM: Functional Resonance Analysis Method)
   3.1 FRAM概要
   3.2 FRAM適用事例

1. 安全解析技術の動向

安全性解析技法のパラダイムシフト

Japan Manned Space Systems Corporation
JAMSS
ひとと宇宙を結ぶインテグレータ

パラダイムシフト

トラディショナルな技法
FMEA、FTA、HAZOPなど

アクシデントは構成機器の故障や
オペレーションミスに限定して発生

1940 1950 1960 1970

FMEA
FTA
HAZOP
ETA
CCA

旧来は
ハードウェア主体

新たな技法
STPA、FRAM

アクシデントは、一つの構成要素に
限定できる要因だけではなく、
構成要素間の相互作用から発生

1980 1990 2000 2010 2020

STPA
FRAM

大規模・複雑化が進むDX時代の
コンピュータシステムへの対応が必要
さらには、AIへの対応も必要

現在の解析技法が確立されたのは50年以上も前
現在のシステムは、ハードウェア主体からDX時代の制御システムへ

トラディショナルな安全性解析技法

解析技法		概要
FMEA	Failure modes and effects analysis (故障モード影響解析)	✓ 構成要素の故障モードとその**上位アイテムへの影響を解析**する**ボトムアップ**の解析技法 ✓ 1940年代にアメリカ陸軍が正式に導入以降、様々な分野で活用される代表的解析技法
FTA	Fault tree analysis (故障の木解析)	✓ 事故/故障等の望ましく事象に対し、その**要因**を探る**トップダウン**の解析技法 ✓ 米国ベル研が開発以降、事前解析のみならず、トラブル発生後に原因を探るためにも活用される代表的技法
HAZOP	Hazard and operability study	✓ プラントの運転状態の「**設計意図からのずれ**」、すなわちプロセス異常に着目する技法 ✓ 「設計意図からのずれ」を洩れなく洗い出すため**ガイドワード**を活用(no, reverse, other than, more, less, as well as, part of, early, late, before, after)
ETA	Event tree analysis (事象の木解析)	✓ システムの異常状態を出発点として、システムに組み込まれたいくつかの安全防護機能バリアの成功、失敗の分岐を経て、最終的な結果事象に到達する**事故シーケンスを特定する**技法
CCA	Cause-consequence analysis (原因-結果分析)	✓ FTA と ETA を組み合わせた技法 ✓ イベントツリーを展開させながら、同時に事故シーケンスを展開し、同時に起因事象および各安全防護機能の失敗事象をトップ事象とするフォールトツリーを作成 ✓ 事故シーケンスが特定され、同時に**各事故シーケンスの原因解析**を行うことが可能

トラディショナルな「ハードウエア中心」「動作が確定的」「事故は構成要素の故障に帰着できる」ことを前提とした技法では、相互作用が複雑なシステムにおける安全解析手法としては不十分である

解析技法の概要説明は、
IEC/ISO 31010 Risk management – Risk assessment techniques より

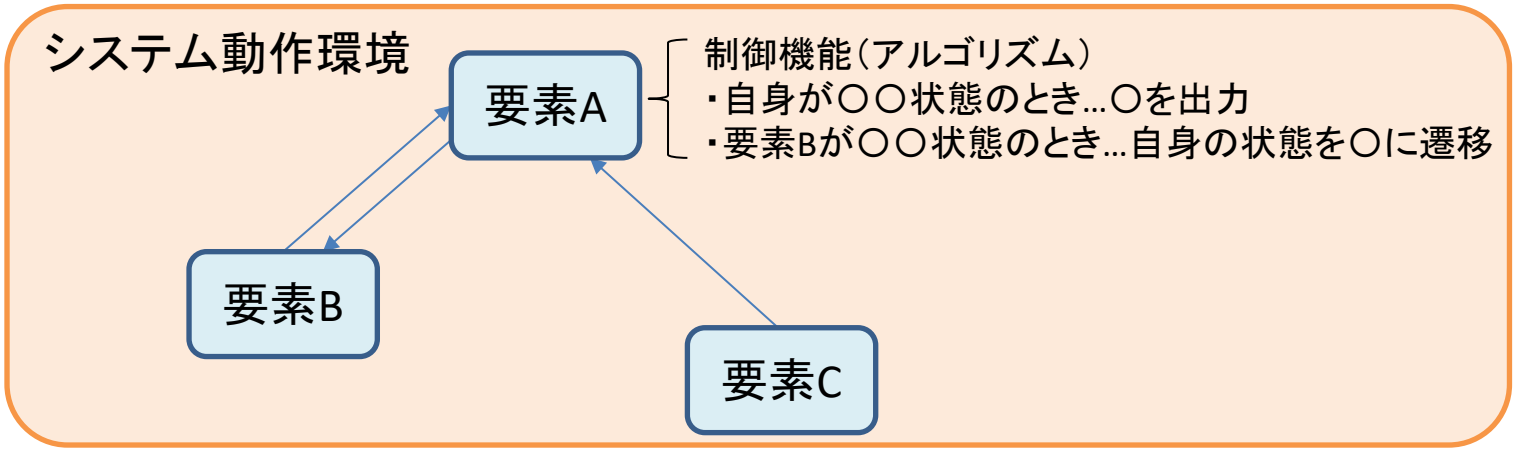
システム安全解析技術の動向

- 安全性を確保するための要求分析、設計手法が必要
  - 機能安全(Functional Safety)
    - システム安全を担保する安全機能を開発上流から識別する
    - 安全機能：危険を検知し安全状態に移行する機能、等
    - 安全機能はクリティカル機能として冗長性設計、他の非クリティカル機能との分離設計などを行う
  - 各産業の機能安全
    - 制御システム全般（IEC61508）
    - 自動車（ISO26262）
    - 航空機（DO-178）
    - 協働ロボット（ISO/TS 15066）
  - 課題：
    - クリティカル機能だけしっかり作ればよいのか？（結局信頼性？）
    - 非クリティカル機能は本当に安全に影響しないのか？
    - 冗長・分離することによるリスクは発生しないか？（2020/10 東証システム不具合）
    - システムの動作環境はどこまで分析されているか？
      - 機器故障・オペミスのような明確な変動だけでなく、目に見えない（特にソフトウェア）の変動をとらえているか

システム安全解析技術の動向

- 個の要素だけでなくシステム全体としての分析が必要
  - VUCA：Volatility（変動）、Uncertainty（不確実）、Complexity（複雑）、Ambiguity（曖昧）な今日のシステム

- システム理論：システム構成要素、入出力情報、制御アルゴリズム
  - システムで不変なもの、変化するものは何か？
    - Context（状況）：システムの動作環境の変化（温度・圧力、機器異常など）
    - Architecture（連携）：要素同士の入出力情報の変化（欠落、誤情報、遅延など）
    - Formation（配置）：隣接する要素の数や距離の変化
    - Function（機能）：上記の変動に対する機能自体の役割の変化
  - システムは要素同士が連携して変動に対応できるか？



JAMSSの安全解析技術

ソフトウエアの安全解析を行う専門組織であるIV&V（Independent Verification & Validation: 独立検証）部門では1996年以来、システム理論に基づく安全性解析手法をJAXA・MITと共に研究し、システム／ソフトウェアの安全要求・安全制約の抽出を実施。

- 活用している解析手法
  - ハザード(*)が自明であり、安全制御の仕組みが検討されているシステムの安全性解析
    - **STAMP/STPA**（Systems-Theoretic Accident Model and Process/Systems-Theoretic Process Analysis）
  - ハザードが自明ではない、機能間の主・従もなく制御の仕組みが曖昧なシステムの安全性解析
    - **FRAM**(Functional Resonance Analysis Method)

(*) ハザード：現在主流の安全解析において必須の概念。起こってほしくない事象（火災、衝突etc）のこと。

JAMSSの他産業における分析の実績

a. 安全・セキュリティの分析

以下の分野において、システムモデル解析（STPA、FRAM）による安全・セキュリティのリスク分析を実施し、安全設計を改善した。

- 宇宙（宇宙ステーション、ロケット、人工衛星）
- 原子力（プラント制御）
- 自動車（自動運転、配車サービス）
- 鉄道（運行制御、踏切制御）
- 航空機（飛行制御）
- 船舶（自動運転）

b. 組織の最適化

以下の分野において、組織モデル解析（FRAM）による組織最適化の分析を実施し、組織のプロセスを改善した。

- 宇宙（ロケット打ち上げ組織改善）
- 原子力（品質保証プロセス改善）
- 自動車（サプライヤの組織改善）
- 機械システム（顧客から発注時の業務フロー改善）

システム安全技術の一覧

No.	技術名称	概要
1	STPA	MITのLeveson教授による安全解析手法(STPA：System-Theoretic Process Analysis)により、システムの安全上の課題を分析
2	FRAM	南デンマーク大学のHollnagel教授によるレジリエンス解析手法(FRAM: Functional Resonance Analysis Method)を用い、システムの安全上の課題を分析
3	CAST	Leveson教授による不具合分析手法(CAST: Causal Analysis using System Theory)により、過去の事故･不具合の根本原因を分析
4	STPA-SEC	Leveson教授によるサイバーセキュリティ解析手法(STPA-SEC)により、システムのサイバーセキュリティ上の課題を分析
5	PRA(確率論的リスク評価)	従来型PRAによるシステム安全設計、運用性評価 動的PRAによるシステム運用のシナリオに依存した故障のモデル化
6	組織の最適化分析	FRAMやCASTを組織を対象にして実施し、組織の弱点を分析
7	Reliable AI	JAMSSの特許技術である人工知能(AI)安全検証技術により、AIシステムの安全上の課題を分析
8	安全を考慮したアジャイル開発	SafeScrumを応用したJAMSS独自の開発手法により、 安全を考慮したソフトウェアのアジャイル開発プロセスをメーカ内に構築

2. 安全解析手法(STPA：System-Theoretic Process Analysis)

2.1 STPA概要

STPA概要

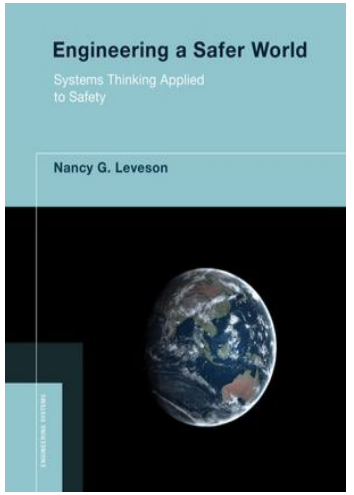
●STAMP（Systems-Theoretic Accident Model and Process）：
システム理論に基づく事故モデル

●STPA（Systems-Theoretic Process Analysis）：STAMP(システム理論)に基づく安全解析手法

マサチューセッツ工科大学(MIT)のNancy.G.Leveson教授が、
“Engineering a Safer World”の中で提唱

STPAは、複数のコントローラが介在する
複雑なシステムに対する安全解析手法

システムを構成するサブシステムやコンポーネントにおける不具合の有無に関わらず、サブシステムやコンポーネントの組み合わせによって発生する不具合に対する安全解析手法



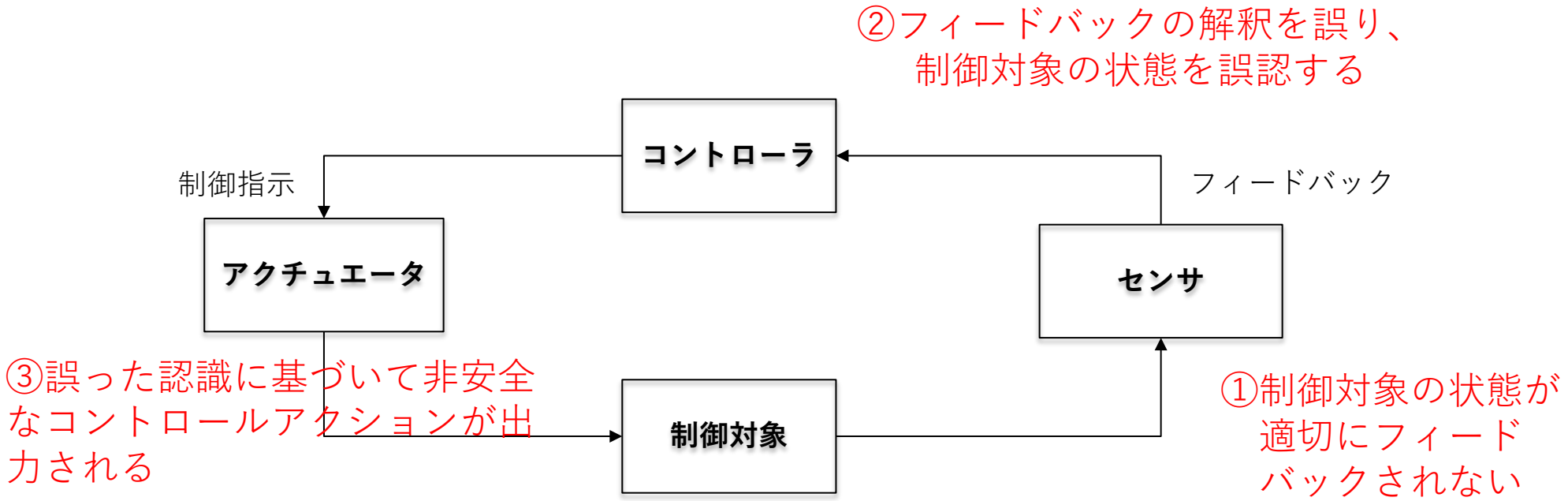
Nancy.G.Leveson著
“Engineering a Safer World”

STPA概要

従来安全解析手法とSTAMP/STPAの違い

安全解析手法	概要	特徴
従来安全解析手法 (FTA, FMEA)	✓ 主にシステム末端の物理的な構成要素と故障モードが決まる**詳細設計の段階**から適用。	✓ 主に**機器故障**をハザード発生要因として識別。
STAMP/STPA	✓ 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。	✓ 非安全な相互作用によるハザード発生要因に着目

コンポーネント間の非安全な相互作用とは



STPA概要

Step 1: 解析目的の定義

・システム境界の定義
・損失の識別
・ハザードの識別

Step 2: 制御構造のモデル化

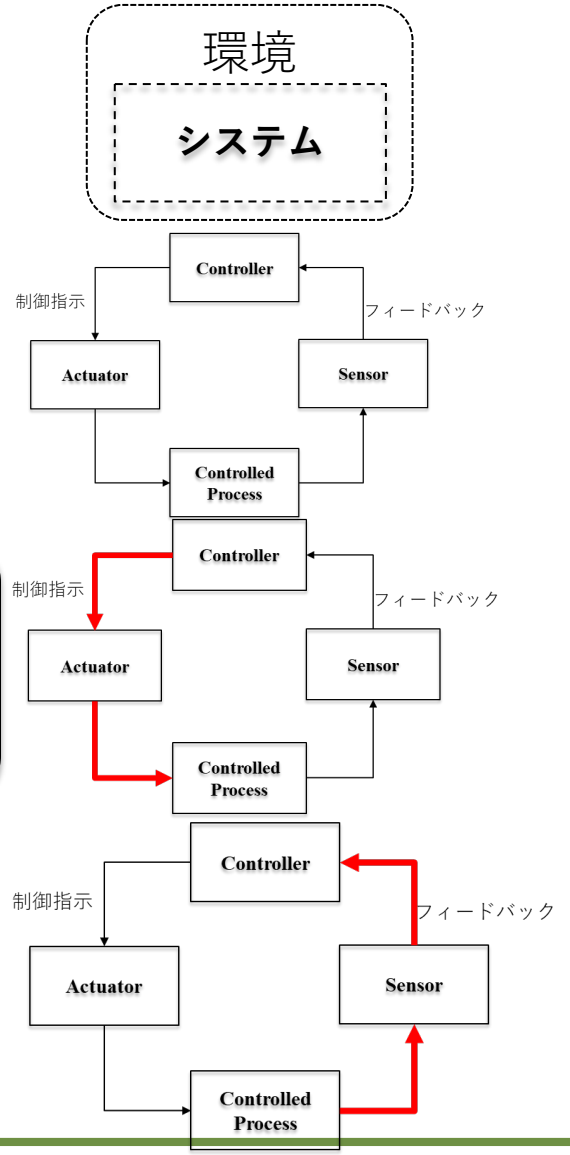
・コントローラ、アクチュエータ、センサ、制御対象プロセスの構造をモデル化

Step 3: 非安全なコントロールアクション(Unsafe Control Action)の識別

・ガイドワードを用いて特定の条件下で危険を引き起こす可能性のある制御アクションを分析

Step 4: 損失シナリオの識別

・危険な制御アクションがどのように発生するかを因果シナリオで特定



2.2 STPA適用事例

STPA 適用事例
STPA Step.1：安全制約の識別

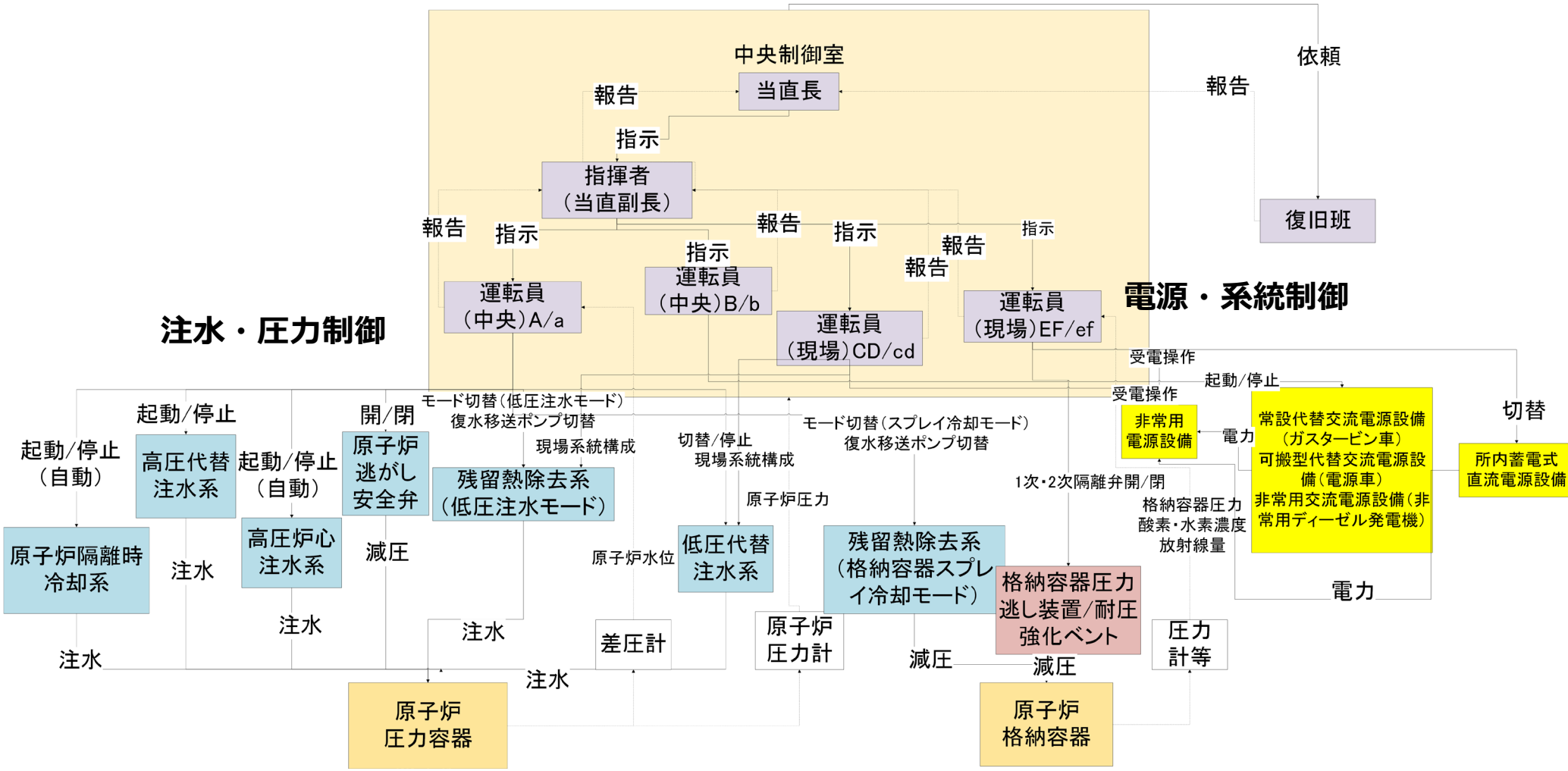
適用対象：公開情報である『重大事故等対策の有効性評価（BWR のSBO）』に記載されたシステム構成及び事故対応シーケンス

ハザードID	ハザード	安全制約
H1	原子炉を冷却できず、炉心損傷の可能性が高まる	原子炉の冷却手段が確保されている
H2	原子炉格納容器を冷却・徐熱できず、破損の可能性が高まる	原子炉格納容器の冷却、徐熱手段が確保されている

※本研究は、原子力規制庁の原子力規制研究技術基盤構築事業費補助金
（原子力規制研究の強化に向けた技術基盤構築事業）の補助を受けて実施したものである。

STPA 適用事例

STPA Step.2：事故対策に関わる制御構造図



STPA 適用事例

- 結果の詳細は、当日報告

STPA 適用事例
分析結果に対する考察

解析結果全般に対する専門家コメント：

- STPAの試行結果は、既存のハザード解析よりも詳細かつ具体的なケースを分析できている
- 分析が詳細である分、対策の検討や有効性評価がしやすいメリットがある
- 一方、識別されたシナリオは全く新しい知見は少なく、一定以上の経験がある関係者であれば『そういったこともあり得る』と経験的に理解しているシナリオにとどまっている

考察：

- STPAの試行によって確認された効果は、現状では『経験知・暗黙知として認識されていたシナリオが形式知化された』ことにあると考えられる（入力となる情報をより詳細にした）
- 識別されたシナリオを他の安全・信頼性に関する活動（PRA、実践的な訓練）への入力として活用することで形式知化したことへの価値が見いだせる可能性がある

- PRA技術の前提となるHRA分析結果と組み合わせることで、より詳細なシナリオを対象とした定量化を行う
  1. **STPAで識別したハザードシナリオに対して確率的な評価を実施し、既存のシナリオに対する評価結果と比較した際の有効性について評価する**
  2. **Error Forcing Contextの識別にSTPAを使用した場合の有効性についても評価する**

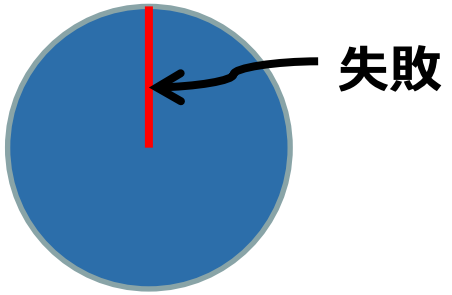
3. レジリエンス解析手法(FRAM: Functional Resonance Analysis Method)

3.1 FRAM概要

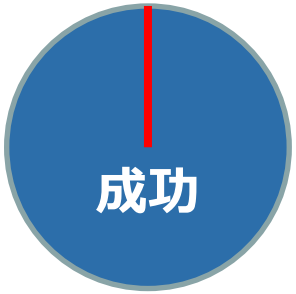
FRAM概要
従来の安全解析手法との比較

FTA：
ハザードの原因を故障に求める

STAMP：
ハザードの原因をコンポーネント間のインタラクションが「遅れる」「間違う」「途中で止まる」「提供されない」等、故障以外の要因から求める
⇒『失敗』に着目した解析



FRAM：
はじめからシステムの失敗事象を定義せず、なぜシステムが成功するのかを分析し、その反面からリスクを識別する
⇒『成功』に着目した解析



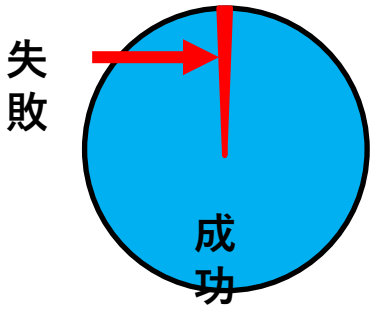
FRAMの特徴

FRAM (Functional Resonance Analysis Method：機能共鳴分析手法)：

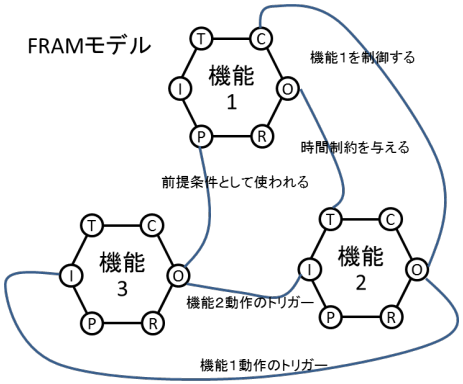
- 失敗要因だけではなく、システムが何故成功できるのかを考え、**成功要因を分析**
- FRAMは、成功要因を起点として、その裏に潜む**リスク要因を識別**

分析の特徴：

- 機能間のインタラクションをモデル化
- 成功要因を可視化
- リスク要因を可視化



・世の中のシステムのほとんどは**成功**
・**成功要因をきっかけ**として**リスク要因の分析**に
つなげる手順を整理



要素	説明
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	機能の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

3.2 FRAM適用事例

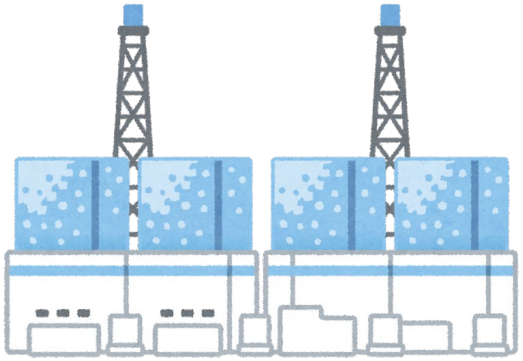
FRAM適用事例
FRAM適用対象と目的

FRAM適用対象：

- 原子力発電施設の緊急時対策訓練にFRAMを適用

目的：

- FRAMモデルの特徴を基に、成功要因の背後に潜在するリスク要因の識別が可能であるか検討



※本研究は、原子力規制庁の令和6年度原子力規制研究技術基盤構築事業費補助金
（原子力規制研究の強化に向けた技術基盤構築事業）の補助を受けて実施したものである。

FRAM適用事例
Step.1:機能の把握

Step.1:機能の把握

Step.2:FRAMモデルの作成

Step.3:特徴の識別

Step.4:成功要因の識別

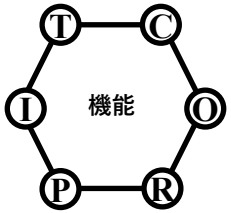
Step.5:リスク要因の識別

- 緊急時対策訓練に関する計画書を基に、FRAMモデル作成に必要となる機能を抽出
- 不明点は、原子力発電施設関係者への質問を通して、機能の振る舞いを補足

文書確認

専門家への質問

FRAMの機能整理



要素	説明
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	機能の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

FRAM適用事例
Step.2:FRAMモデルの作成

- Step.1で把握した機能を基にFRAMモデルを作成
- FRAMモデルの分析結果の一例をStep.3以降で示す

FRAMモデルは
当日報告

FRAM適用事例
Step.3：特徴の識別

Step.1:機能の把握

Step.2:FRAMモデルの作成

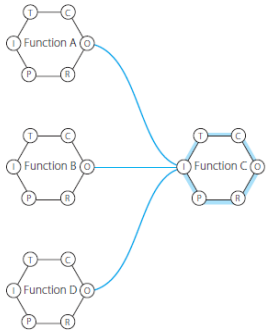
Step.3:特徴の識別

Step.4:成功要因の識別

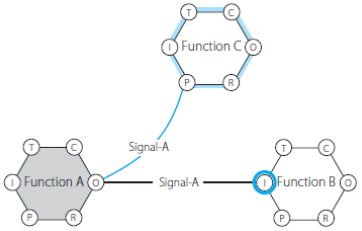
Step.5:リスク要因の識別

- 作成したFRAMモデルの特徴を識別（以下特徴の例）
- **特徴毎の観点に従い分析**（本発表ではループ構造に着目）

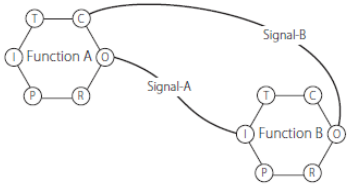
1. 同一種類の複数入力（ツリー型）



2. 複数の機能に出力（スター型）



3. ループ構造（リング型）



[参考文献] FRAM（機能共鳴分析手法）による成功学に基づく安全工学, SEC journal Vol.14 No.1 Aug. 2018

FRAM適用事例

結果の詳細は、当日報告

FRAM適用事例
まとめ・課題

- 本研究では、緊急時対策訓練にFRAMを適用することで、成功要因の背後に潜在するリスク要因を識別できることが示され、組織のレジリエンス能力向上のために訓練すべき点が確認された。
- 今後の課題は、識別したリスクの妥当性を検証するとともに、リスク低減策の導出方法について検討を進め、事故対応訓練シナリオの定量的評価の方法を検討する。

STPA補足

STAMP/STPAの利用動向

- **海外の動向**
  - ISO26262(自動車機能安全) にて、STAMP/STPAを推奨(2018)
  - DO-356（航空機セキュリティ）にて、STPA-SEC（STPAのセキュリティ版）を推奨(2018)
- **国内の動向**
  - JAXA-MIT*-JAMSSで、STAMP/STPAの共同研究（2009-）
    ***STAMP/STPA提唱者のN.Leveson教授との共同研究**
  - JAXA宇宙機開発において、STAMP/STPAを推進（2014-）
  - 第1回STAMPワークショップ** @九州大 (2016.12.5-7)：130名
    ****JAMSSは共催**（現在までに4回開催）
  - IPA(情報処理推進機構)にて、開発企業向け小冊子「はじめてのSTAMP」発行(2016)
  - JasPar(車載ソフト標準化機関)にて、STAMP/STPAを推奨(2017)

STAMP/STPAの分析手順

非安全なコントロールアクションの識別によるハザードシナリオの分析

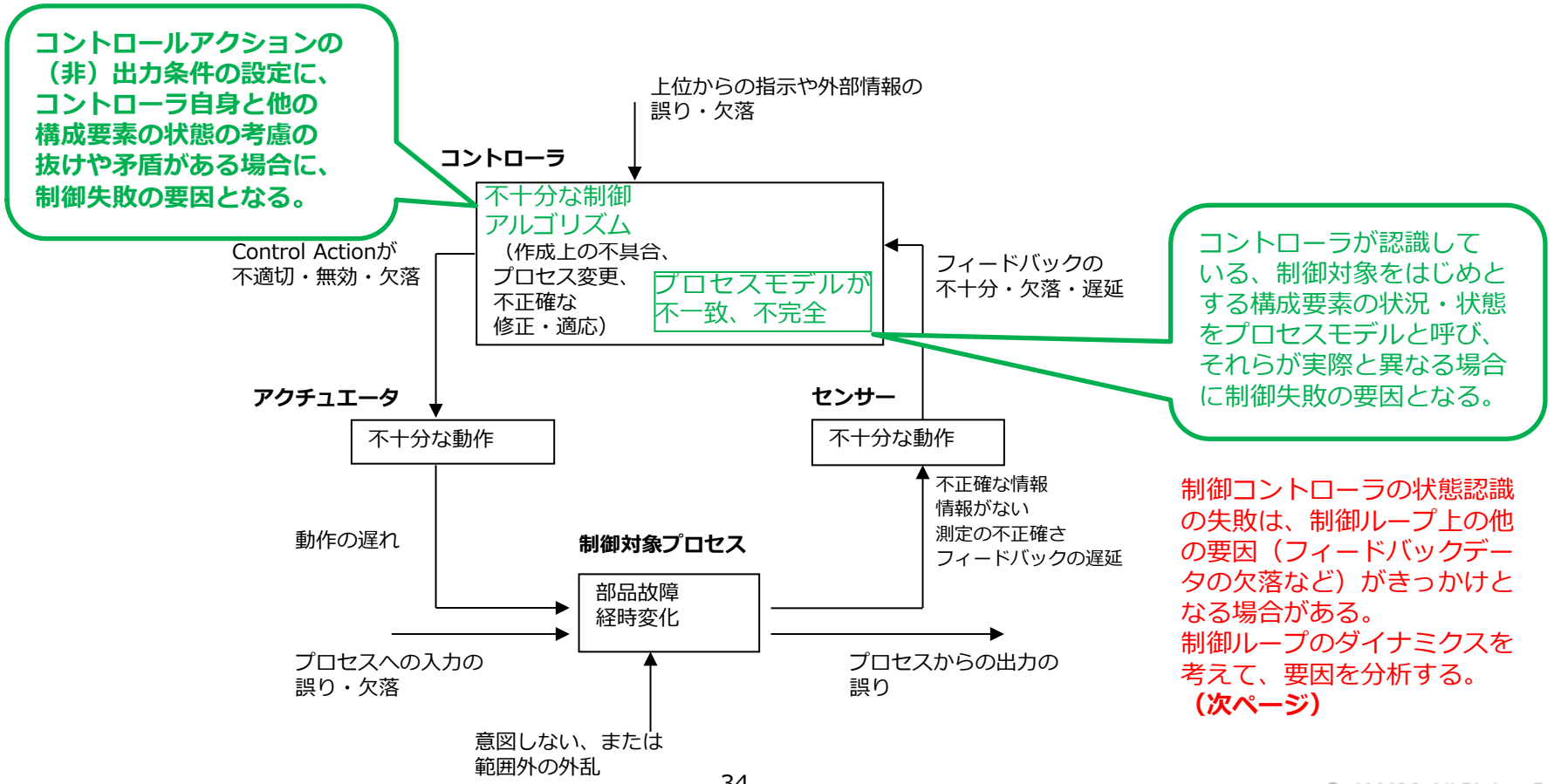
- 全てのコントロールアクションに対して、４つのガイドワードを使ってハザードにつながる非安全なコントロールアクション（Unsafe Control Actions：UCA）を分析する
  - ① “Not Provided”
    必要なときに提供されないとハザードに至る
  - ② “Incorrectly Provided”
    不適切に提供される（不必要なとき、あるいは誤った内容）とハザードに至る
  - ③ “Provided Too Early, Too Late, or Out of Sequence”
    提供開始タイミングを間違うとハザードに至る
  - ④ “Stopped Too Soon, or Applied Too Long”
    提供終了タイミングを間違うとハザードに至る

<table>
<tr><td colspan="3">提供される</td><td rowspan="4">提供されない</td></tr>
<tr><td colspan="2">正しいものが提供される</td><td rowspan="3">間違ったものが提供される</td></tr>
<tr><td>正しいものが正しいタイミングで提供される</td><td rowspan="2">正しいものが間違った開始タイミングで提供される</td></tr>
<tr><td>正しいものが正しいタイミングで最後まで正しく提供される</td><td>正しいものが間違った終了タイミングで提供される</td></tr>
</table>

STAMP/STPAの分析手順

制御ループ図の分析によるハザード要因の分析

- 非安全なコントロールアクション毎に、関係する制御コントローラと制御対象との間の制御ループを分析し、ガイドワードを参照しながら詳細なハザード要因を分析する
- **特に制御コントローラによる状態認識の失敗に起因する要因を導き出す**

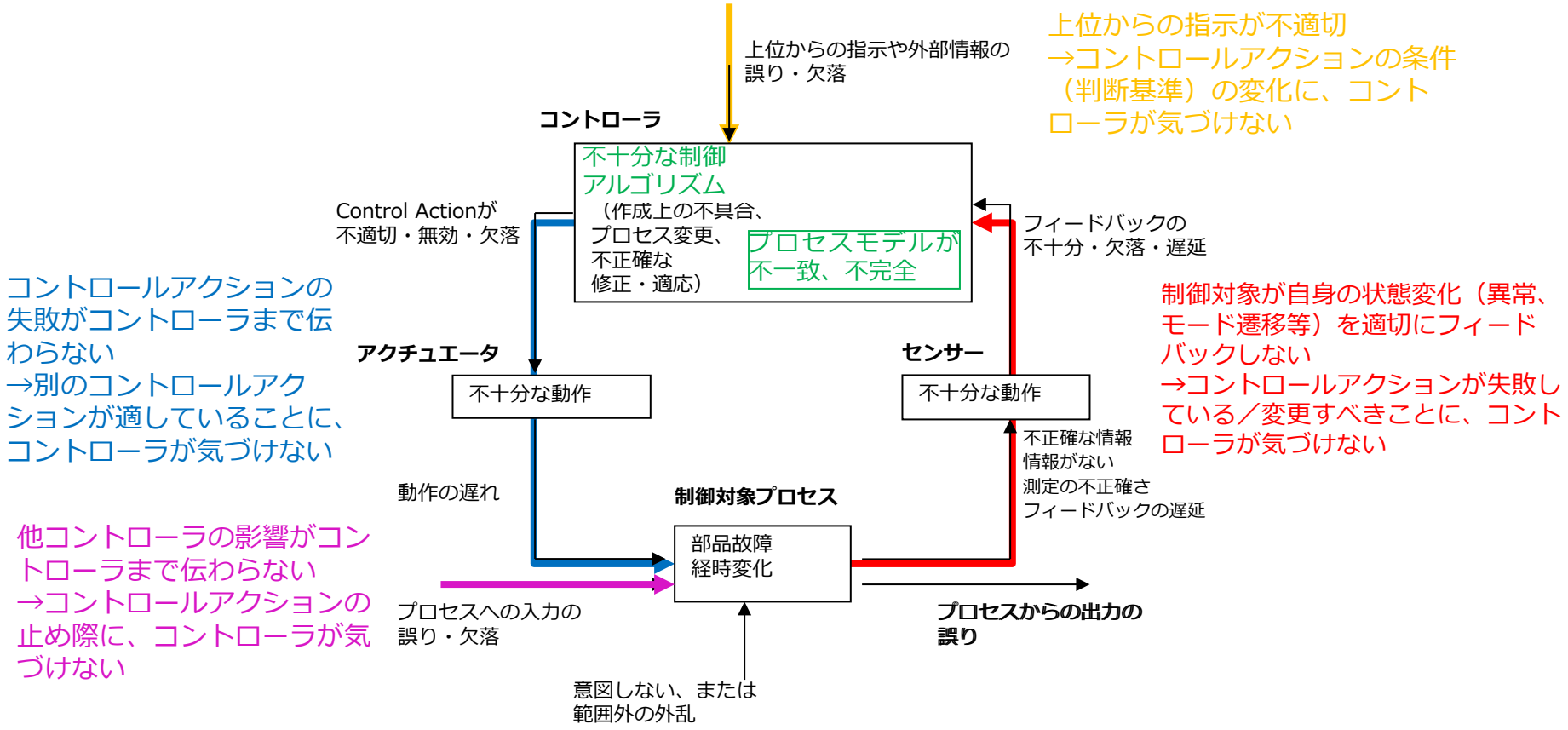


制御コントローラの状態認識の失敗は、制御ループ上の他の要因（フィードバックデータの欠落など）がきっかけとなる場合がある。
制御ループのダイナミクスを考えて、要因を分析する。
（次ページ）

STAMP/STPAの分析手順

制御ループ図の分析によるハザード要因の分析

- **制御コントローラによる状態認識の失敗につながる制御ループ上の要因の例**



セキュリティリスク分析の手法

●従来のセキュリティ分析手法

・セキュリティ脅威を洗い出し、各脅威（システム脆弱性の悪用）に対する対策を実施
・攻撃パターンの識別後に対策を行うため、新たな攻撃パターンに対して後手になる

●新しいセキュリティ分析手法

弊社は従来のボトムアップアプローチではなく、新しい観点からのトップダウンアプローチを採用した以下の分析を実施することで、高レベルでセキュリティと安全性を統合したシステムの構築を実現

STPA-SEC：

STAMP/STPA （システム理論に基づく安全解析手法）にセキュリティ脆弱性のヒントワードを追加し、同時多発的に発生しうる複数の制御ループ上の要因を組み合わせたハザードシナリオを分析

レジリエントセキュリティ分析：

異常検知と攻撃後の被害を最小限にするため、どのようなセキュリティ脅威があったとしても、安全を確保するために必要なシステム機能を提供する方法を検討