発表資料

STAMP/STPAとイベントシーケンス図を用いた複数コントローラが協調するシステムにおけるハザード対策の検討支援手法の提案

国立研究開発法人　宇宙航空研究開発機構

研究開発部門　第三研究ユニット

〇髙附翔馬　梅田浩貴　植田泰士　片平真史

森崎修司（名古屋大学）

e-mail：takatsuki.shohma@jaxa.jp

本発表のターゲット

- ハザード対策の導出に課題をお持ちの方
- STAMP/STPAの適用に課題をお待ちの方
- イベントシーケンス図を使った課題解決に関心のある方

発表の概要

課題

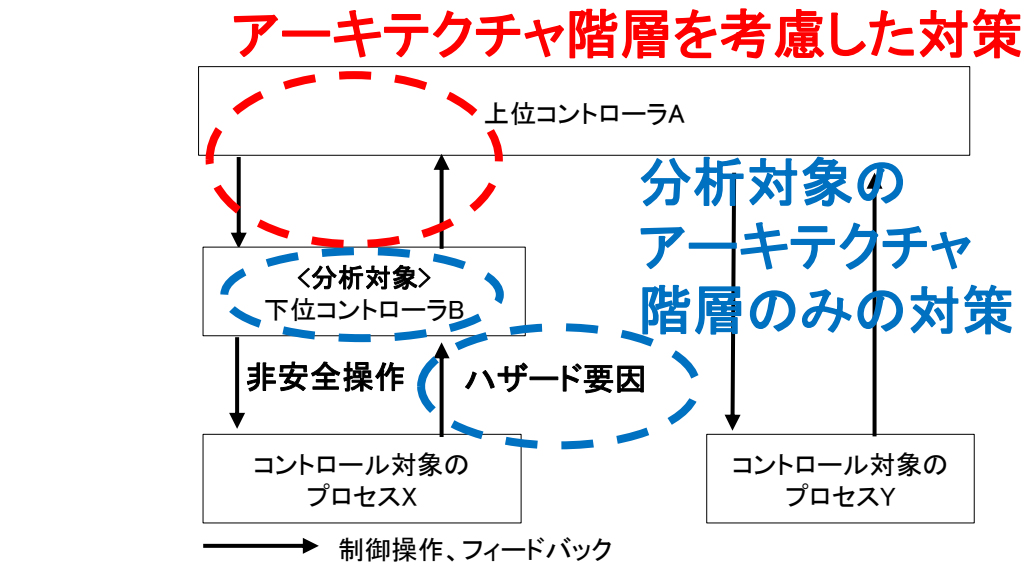
STAMP/STPAのみでは
（　）の対策が漏れる

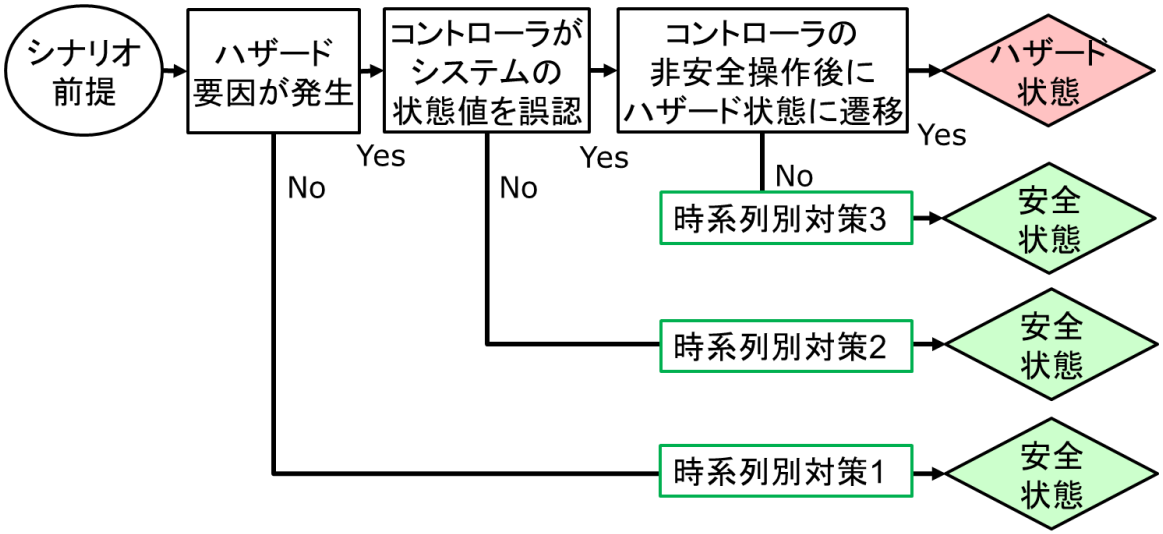
工夫

STAMP/STPA
＋
イベントシーケンス図

効果

提案手法は上記課題においてSTAMP/STPA を補強できる





目次

- 背景（前提知識等）
  - 宇宙機システムの特徴とソフトウェアの品質
  - 安全解析手法
  - STAMP/STPAによる分析
  - 取り扱うシステムの製品特性
  - 課題
- 提案手法の概要
- 提案手法の有効性確認
  - 方法
  - 結果
- まとめ

宇宙機システムの特徴とソフトウェアに求められる品質

宇宙機システムの特徴

- システム故障時の損失：大
  - 環境や人命の喪失の可能性あり
  - 損失するコスト：大
- システム故障の対応や復帰の難易度：高
  - 地球との通信は限られた期間のみ
  - 部品交換不可
- システム故障の対策の難易度：高
  - 想定外が発生しやすい
    - 動作環境が過酷（放射線によるメモリ化け発生等）
    - 過去の知見：少
      - 5年以上の長い開発期間
      - 少量多品種（研究実証向け）
  - 想定内でも実環境の試験不可

ソフトウェアに求められる品質：非常に高い

安全解析を含めた設計検証や網羅的な試験が重要

宇宙機システムの例

人工衛星

宇宙ステーション

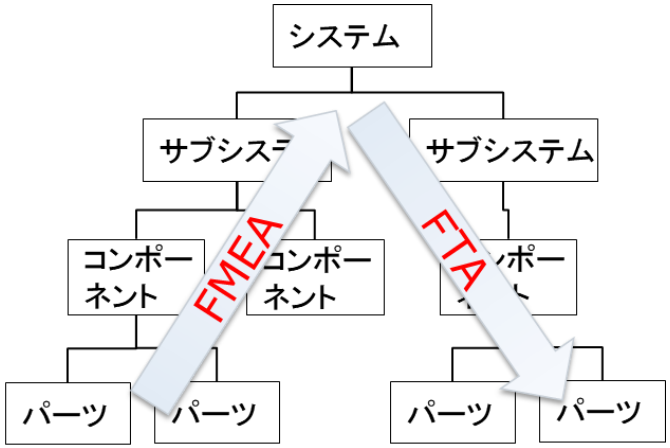
ロケット

地上管制局

安全解析手法の現在

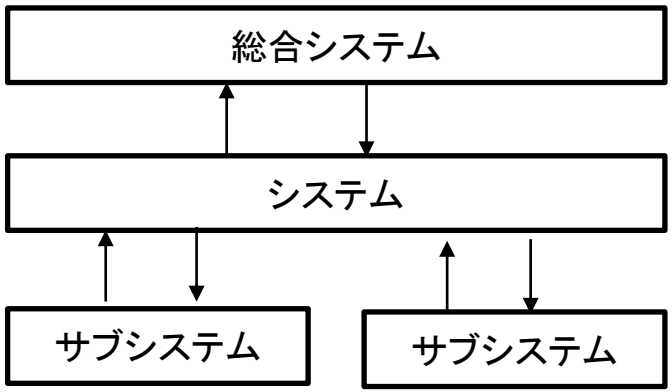
STAMP/STPAを使うことで、システム構成要素の故障がなくても発生する
システム故障を分析可能にし、より複雑で巨大なシステムを扱える

手法	FTA、FMEA	STAMP/STPA
システム故障の要因	システム構成要素の故障	コントローラ間の相互作用
故障要因としてモデル化可能な構成要素	ハードウェア	ハードウェア、ソフトウェア、人など



・トップダウンアプローチ
FTA（事象から原因推定）

・ボトムアップアプローチ
FMEA（構成要素の状態から影響分析）



STAMP/STPAの分析

システムの重大な損失につながるシナリオ（ハザードシナリオ）の
要因を因果関係を遡って分析する

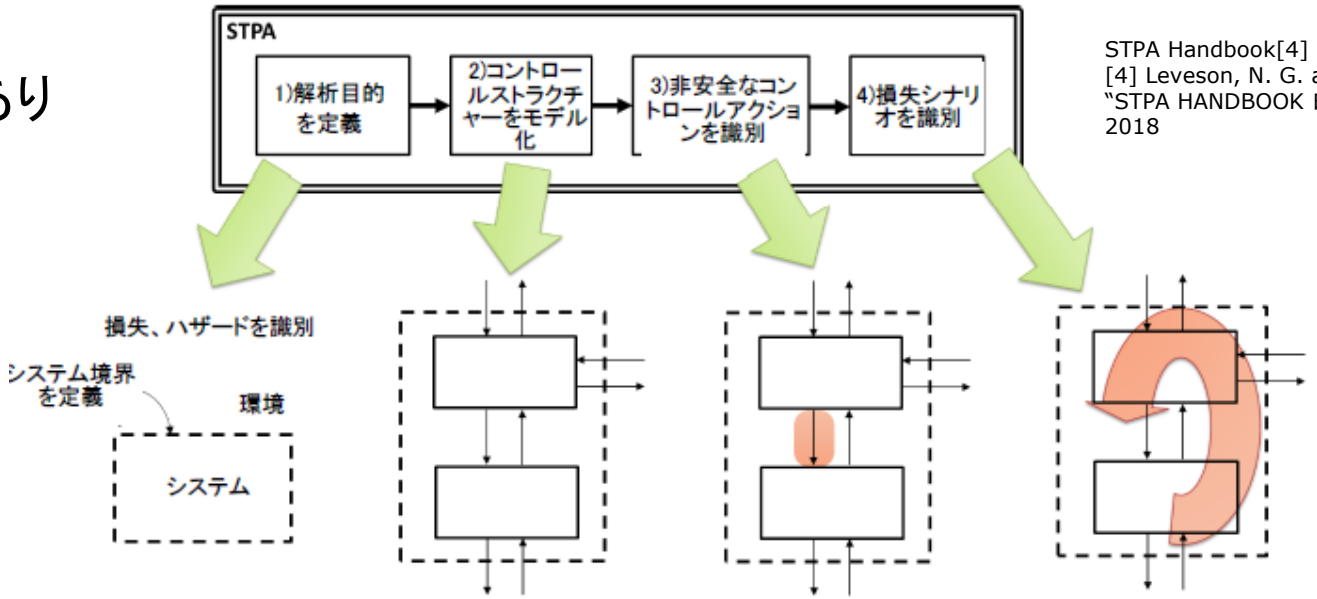
事象（イベント）の流れ

アクシデント	ハザード	非安全なコントロールアクション（UCA）	ハザード要因（HCF）
損失（Loss）を伴うシステムの事故	アクシデントにつながるシステムの状態	ハザードにつながり得る制御操作	UCAが起きる要因

分析の流れ

STAMP/STPAの限界

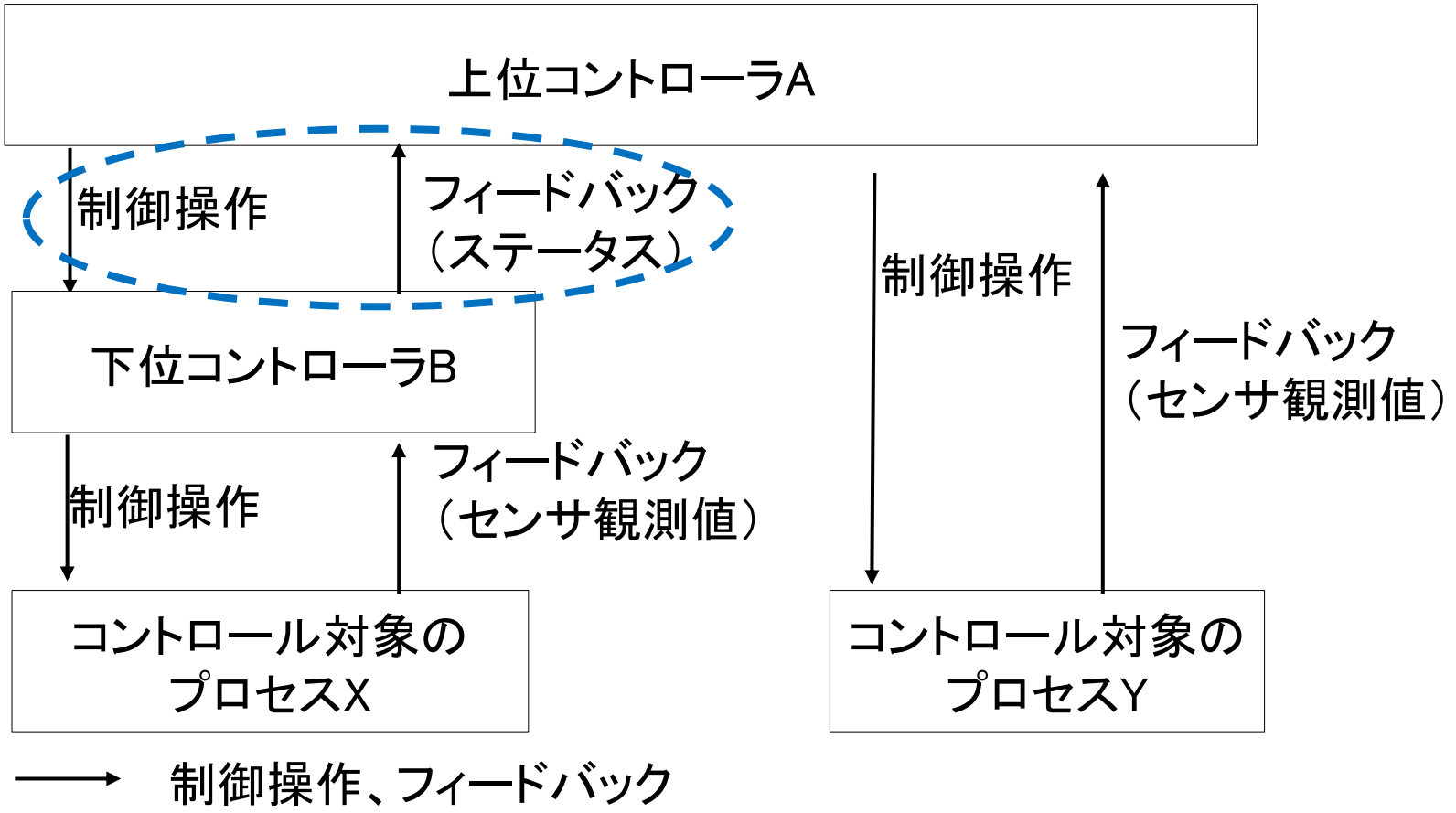
STAMP/STPAではハザードシナリオの導出までのガイドはあるが、
その対策を具体化するガイドは設定されていない

作業工程	ガイド
①ハザードシナリオの導出	あり  STPA Handbook[4] 図2.1より [4] Leveson, N. G. and Thomas, J., "STPA HANDBOOK 日本語版 Ver.0 .2", 2018
②ハザード対策シナリオの導出	なし 「どのような対策を実施すべきか？」は個々の製品特性に依存するため

取り扱うシステムの製品特性

制御構造として複数のコントローラを有し、
コントローラ間で協調してミッションの遂行や安全化を行う

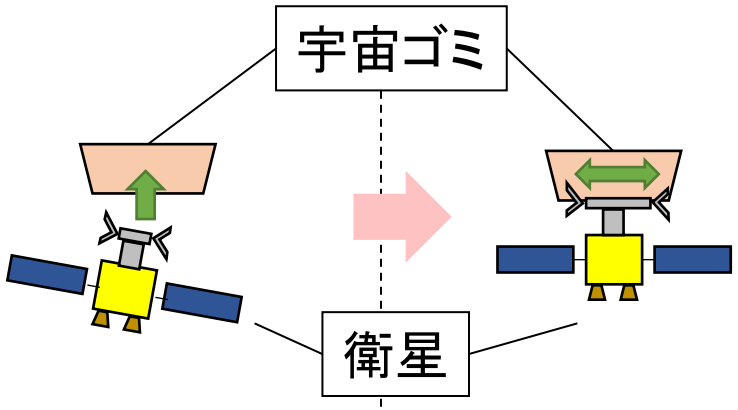
コントローラ間の相互作用（協調動作）



対象とするシステムの例（宇宙ゴミ除去衛星）

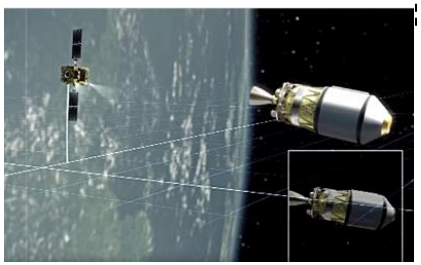
同時に制御してはいけない対象を持つ2つのコントローラが協調して、
宇宙ゴミとの衝突を回避しながら接近し、捕獲するシステム

振る舞いのイメージ（接近～捕獲）

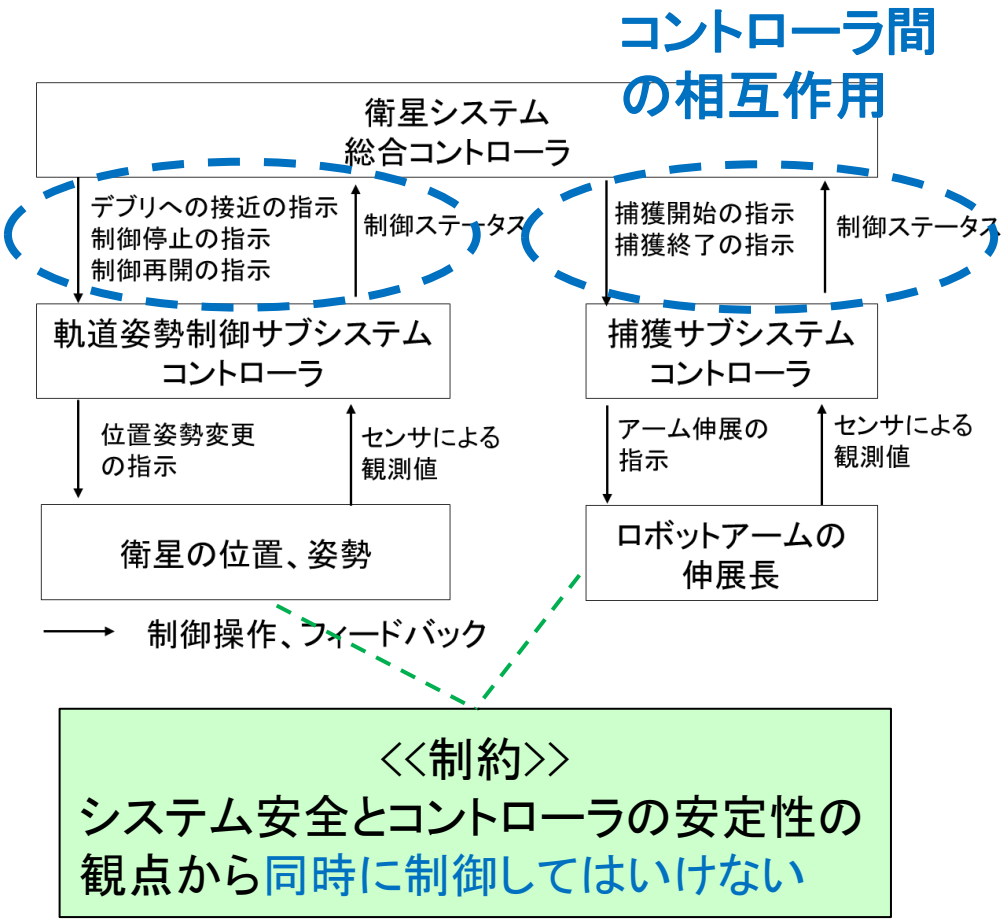


宇宙ゴミへ接近し、相対的に静止

ロボットアームを伸ばして宇宙ゴミを捕獲



制御構造

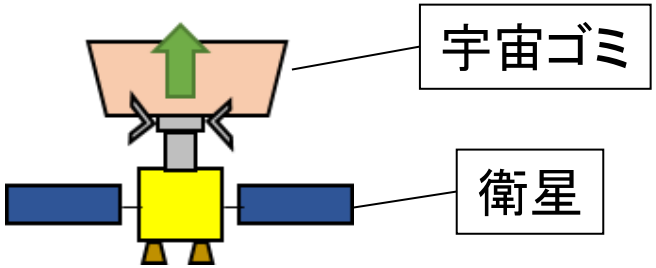


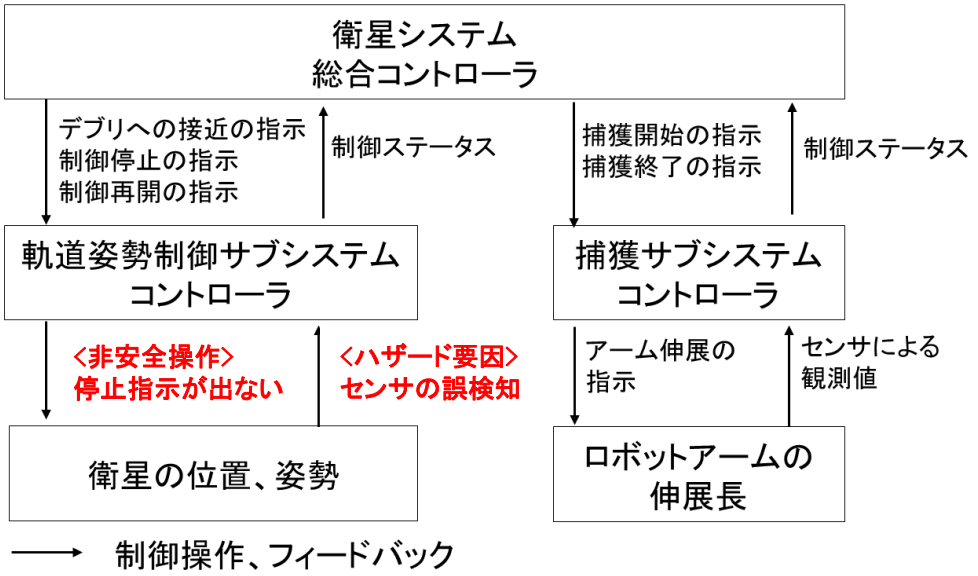
[2] Sasaki, T., Nakamura, R., Okamoto, H., Nakajima, Y., Nishishita, T., Tanishima, N., Umeda, H., Takatsuki, S. and Kobayashi, T. "Requirement Optimization of Proximity Operations for Active Debris Removal Missions Considering Both GNC and Capture System Constraints", 34th International Symposium on Space Technology and Science (ISTS), 2023

STAMP/STPA適用時に発生する課題の例

<<制約>>
宇宙ゴミとの距離が停止距離に達した場合、相対的に停止する必要あり

ハザードシナリオのイベント	例：宇宙ゴミ除去衛星
①ハザード要因が発生	距離センサから停止距離への到達が通知されない
②コントローラがシステムの状態を誤認する	コントローラがまだ接近する必要ありと誤認識
③コントローラが非安全操作を実施	コントローラが停止指示（ブレーキ）を出さない
④コントロール対象のプロセスが変化	衛星が宇宙ゴミに接近（衛星の位置が変化）
⑤システムがハザード状態に遷移	宇宙ゴミと衝突しうる距離、速度になる
⑥システム故障（アクシデント）が発生	宇宙ゴミと衝突する





STAMP/STPA適用時に発生する課題の例

ハザードシナリオに対する対策（ハザード対策シナリオ）の導出時に、
アーキテクチャ階層を考慮した対策が導出されない
（対策が分析対象のコントローラが属するシステム内に限定されがち）

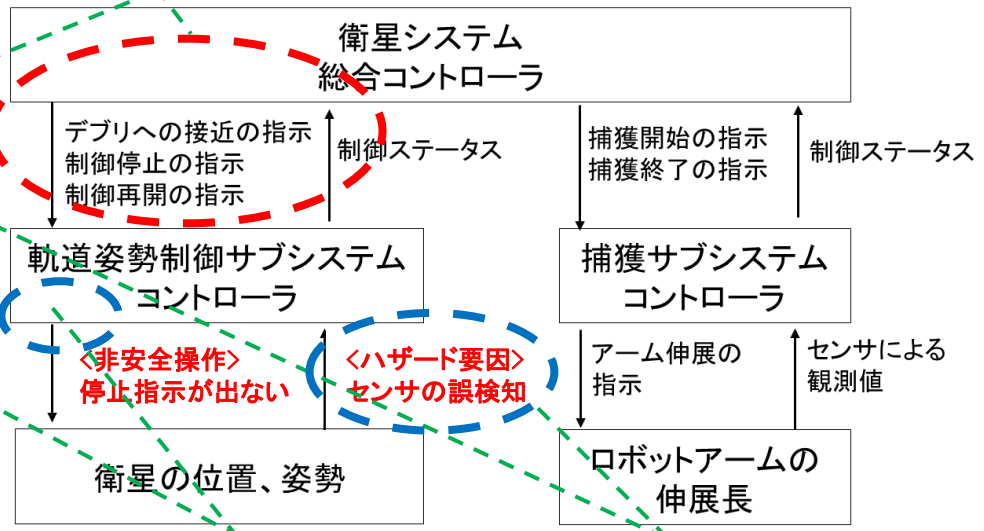
ハザードシナリオのイベント	例：宇宙ゴミ除去衛星
①ハザード要因が発生	距離センサから停止距離への到達が通知されない
②コントローラがシステムの状態を誤認する	コントローラがまだ接近する必要ありと誤認識
③コントローラが非安全操作を実施	コントローラが停止指示（ブレーキ）を出さない
④コントロール対象のプロセスが変化	衛星が宇宙ゴミに接近（衛星の位置が変化）
⑤システムがハザード状態に遷移	宇宙ゴミと衝突しうる距離、速度になる
⑥システム故障（アクシデント）が発生	宇宙ゴミと衝突する

制御構造と対策例

アーキテクチャ階層を考慮した対策

この対策が漏れる

上位コントローラが異常を検知し、誤認識中のコントローラへ停止指示を出す



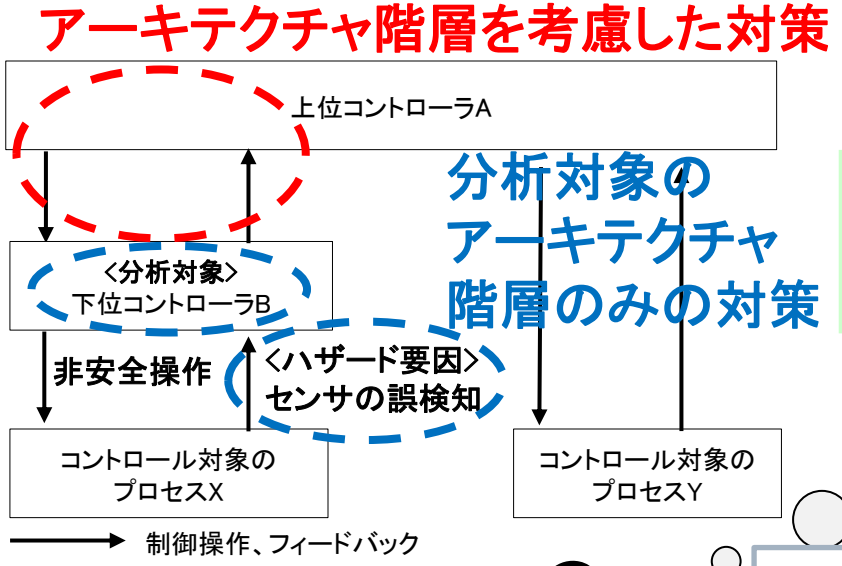
センサ値と推定値を比較して判断する

センサを冗長化

分析対象のアーキテクチャ階層のみの対策

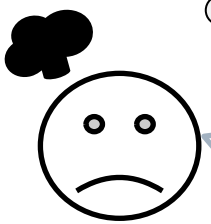
どうして課題が発生するのか？

STAMP/STPAには対策のガイドがない
→　対策の導出は作業者の力量に依存



時系列を想像

どんな順でイベントが起きるか？
対策をするタイミングはどこか？
対策実施時の前提は何か？

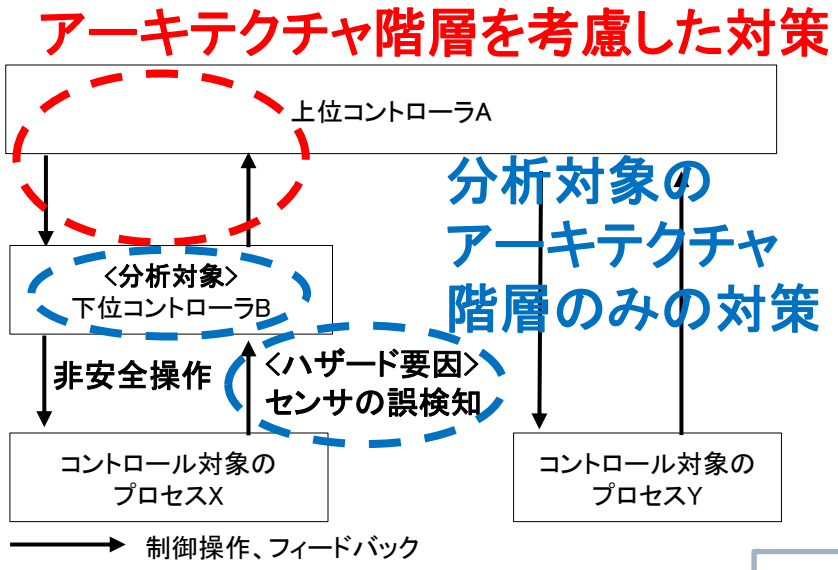


アーキテクチャ階層とイベントの時系列を頭の中で想像して、対策のタイミングや前提を把握するのは難しい

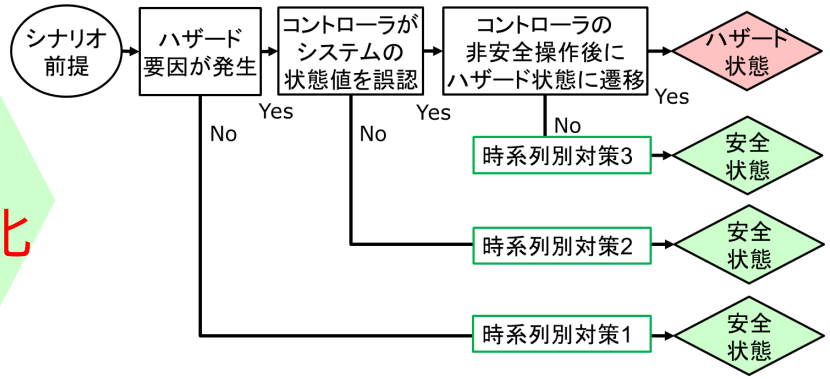
従来のハザード対策シナリオの導出方法（STAMP/STPAのみ使用）を「コントローラのアーキテクチャ階層を考慮した対策」を作業者が自然に考えられる手法プロセスに補正する必要あり

提案手法のアイデア

・対策実施時の前提を明確にするために、3つの時系列別対策に分けて導出
・イベントシーケンス図により視覚的に対策のタイミングを把握



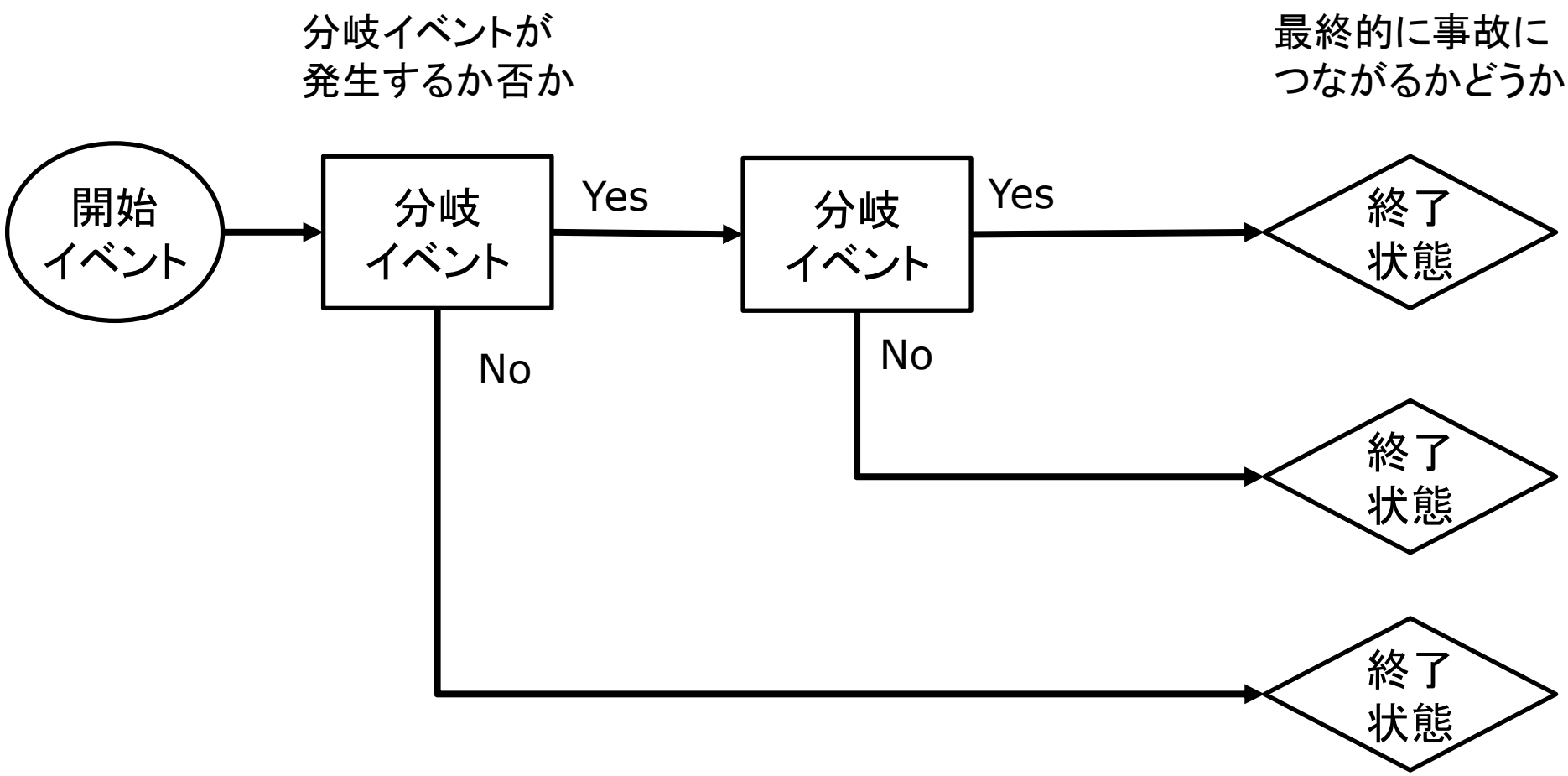
時系列
を可視化



アーキテクチャ階層とイベントの時系列を
見ながらなら対策のタイミングや前提を
把握し易い

イベントシーケンス図とは？

事故や故障によって損失につながるシーケンシャルなシナリオを表現する図
原子力や宇宙分野で分岐イベントの評価に使用されている

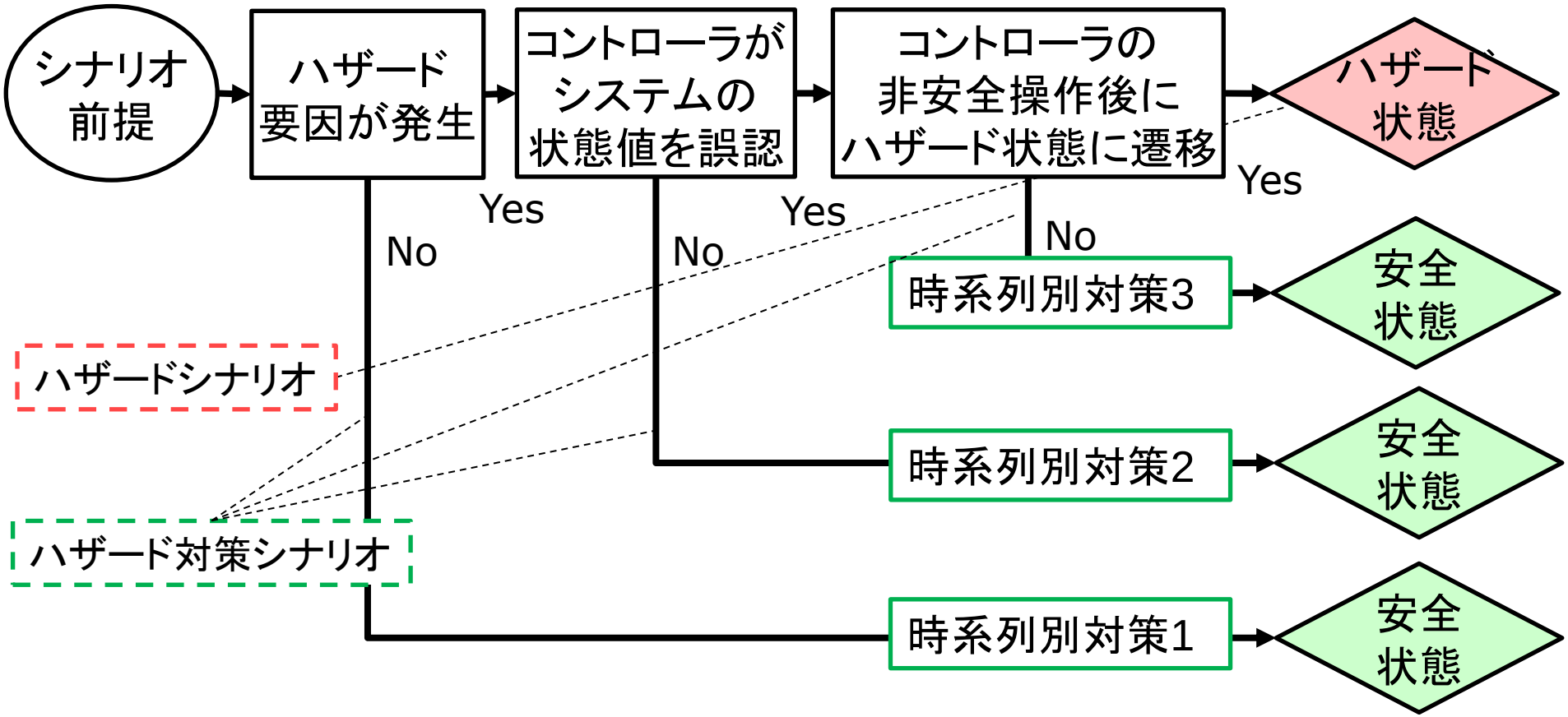


[8] National Aeronautics and Space Administration, “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners Second Edition”, NASA/SP 2011 3 421, December 2011

イベントシーケンス図を用いたハザード対策の導出

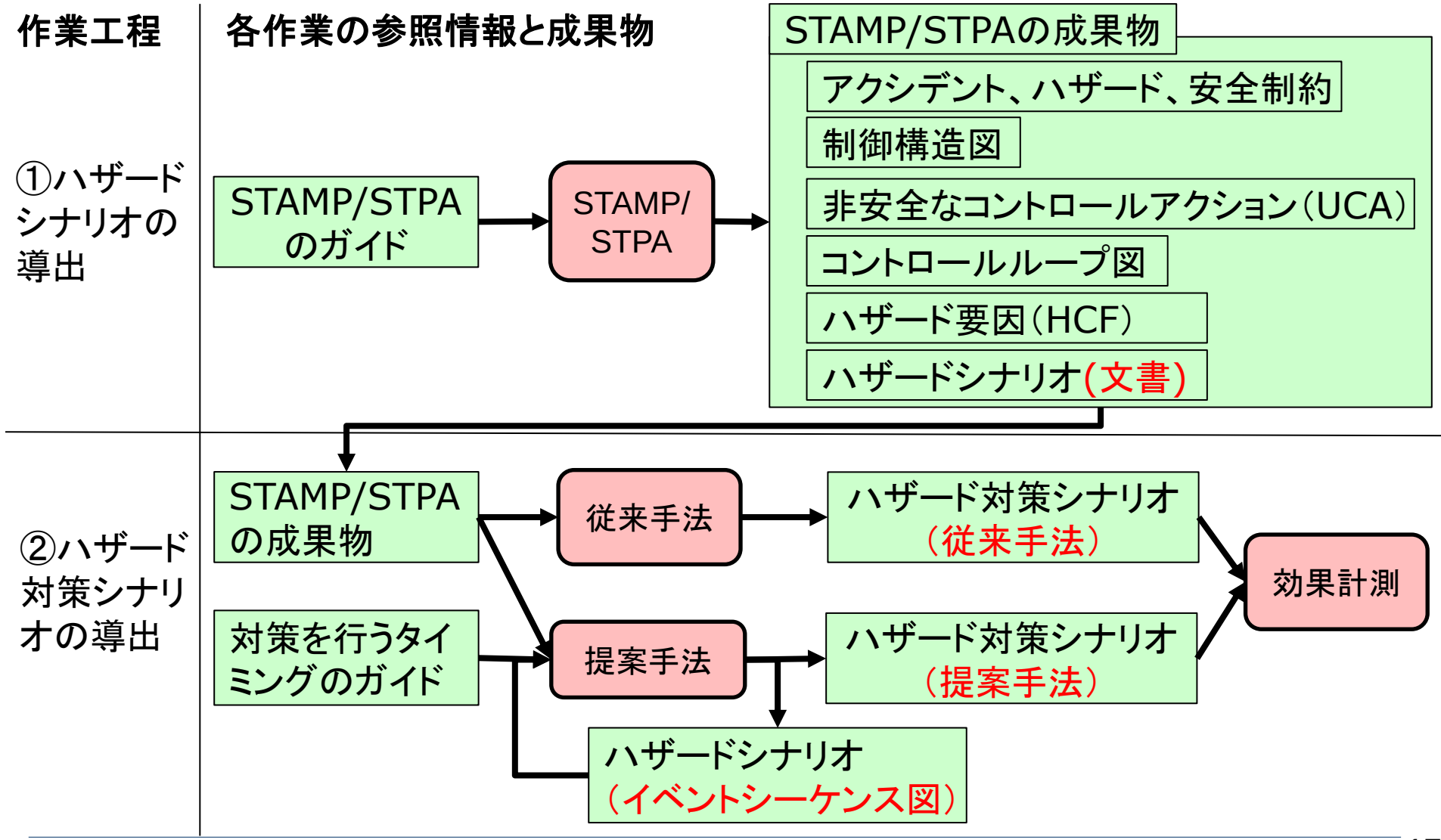
STAMP/STPAにおけるハザードシナリオのイベントに対して、
「システムが最終的に安全状態になるような対策は何か？」を思考する

【時系列別対策1】ハザード要因を除去する対策
【時系列別対策2】コントローラの非安全操作を防止する対策
【時系列別対策3】コントローラの非安全操作後の対策



有効性確認の方法：流れ

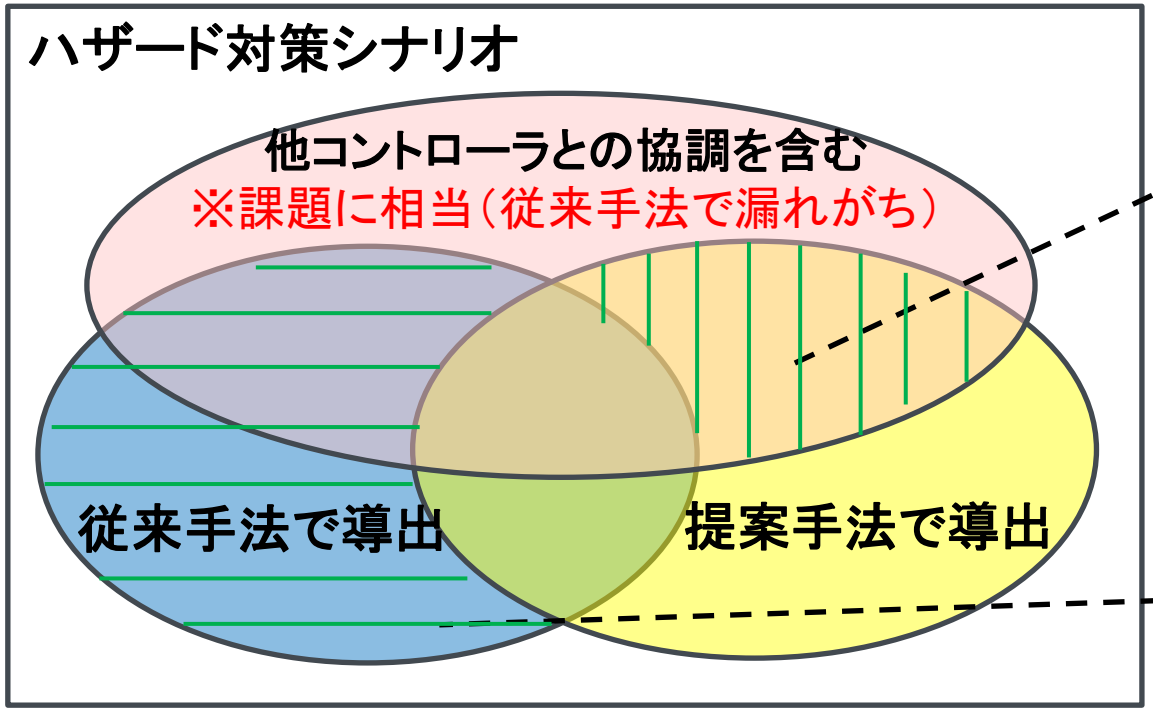
STAMP/STPAによってハザードシナリオを導出し、
その成果物をもとに、従来手法と提案手法でハザードシナリオを導出し比較



有効性確認の方法：評価指標

提案手法の有効性を評価するため、2つの項目を設定

記号	評価項目：何を評価するか？
x	従来手法で見逃しがちなハザード対策シナリオを提案手法は導出できるか？（課題に対する有効性）
y	従来手法で導出したハザード対策シナリオを提案手法は見逃していないか？（提案手法の見逃し）



評価指標x1
従来手法では見逃したが、提案手法では導出したハザード対策シナリオ数（左図：縦網かけ）
※課題に対応する「他コントローラとの協調がある」シナリオに限定

評価指標y1
従来手法では導出したが、提案手法では見逃した数（左図：横網掛け）
※「他コントローラとの協調」の有無に限定しない

（参考）有効性確認の方法：ツールによる作業支援

問い合わせ先：
takatsuki.shohma@jaxa.jp

使用する手法の学習やモデリングのコストを削減し、
分析作業に注力できるようにツールで支援

作業工程

①ハザードシナリオの導出
（STPAの基本プロセス）

- Step0：アクシデント、ハザード、安全制約の識別
- Step0：コントロールストラクチャーの構築
- Step1：非安全なコントロールアクション（UCA）の抽出
- Step2：ハザード要因（HCF）の特定

②ハザード対策シナリオの導出

支援ツール

■ツールの特徴
ExcelとPowerpointで思考を誘導する手順をツール化

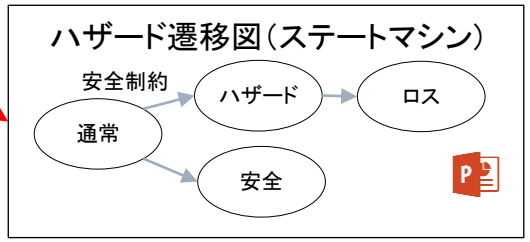
【ST-1】
ハザード定義表

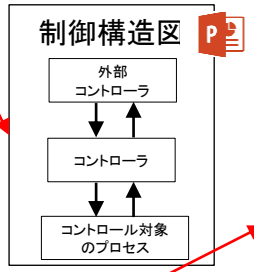
【ST-2】
制御構造定義表

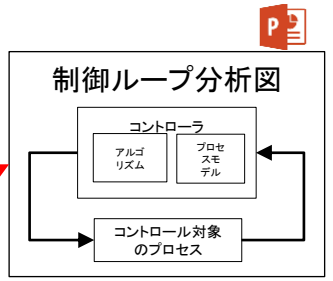
【ST-3】
非安全操作分析表

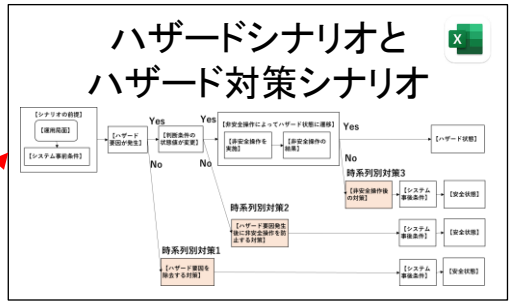
【ST-4】
制御ループ分析表

【ST-6】
ハザード対策シナリオ定義表







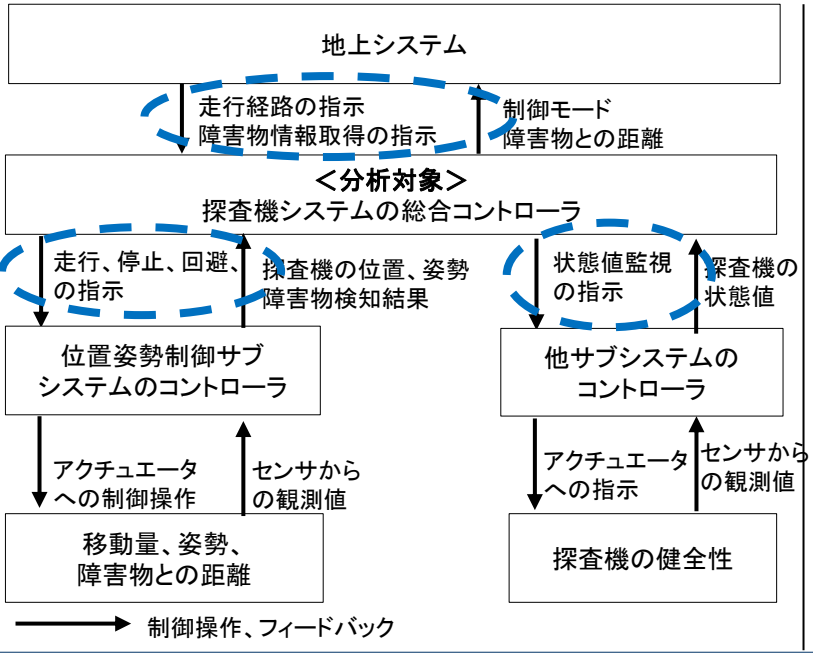


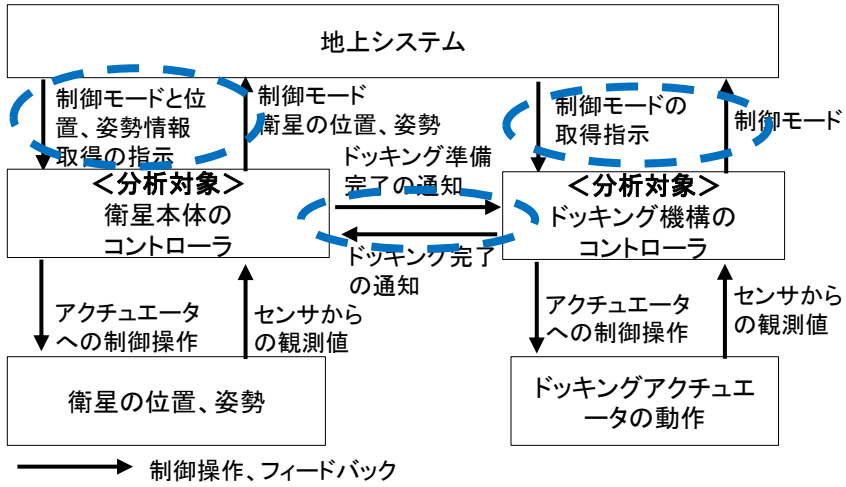
有効性確認の方法：適用対象と作業者

課題への有効性を確認するため、2つのシステムに手法を適用
システムごとにドメイン知識の異なる2人の作業者が実施

適用対象	システムA	システムB
特徴	月面上で走行し、電力を確保しつつ障害物を避けながら、探査する	相手の宇宙機との衝突を避けながら、接近しドッキング（結合）する
作業者	・ドメインエキスパートA1 ・非ドメインエキスパートA2	・ドメインエキスパートB1 ・非ドメインエキスパートB2

どちらも複数のコントローラを有し、コントローラ間で協調するシステム

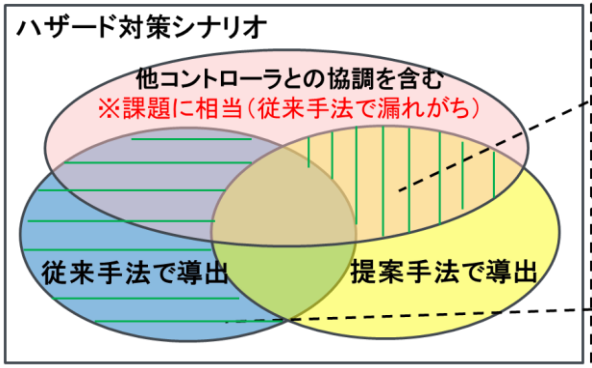




有効性確認の結果：評価項目x（課題に対する有効性）

従来手法で見逃しがちなハザード対策シナリオを提案手法は導出できるか？
- すべての作業者で導出した（課題への有効性あり）
- 導出した対策はハザードシナリオ1件あたり0.9~1.2件

項目	値			
適用対象のシステム	システムA		システムB	
作業者	ドメインエキスパートA1	非ドメインエキスパートA2	ドメインエキスパートB1	非ドメインエキスパートB2
ハザードシナリオ数	20	10	41	12
従来手法では見逃がしたが、提案手法では導出した数（評価指標x1）	18	12	37	14
ハザードシナリオ1件あたりの従来手法では見逃がしたが、提案手法では導出した数（評価指標x2）	0.90	1.20	0.90	1.17



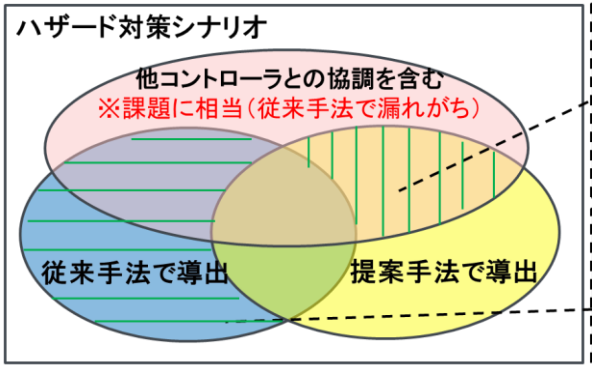
評価指標x1
従来手法では見逃したが、提案手法では導出したハザード対策シナリオ数（左図：縦網かけ）
※課題に対応する「他コントローラとの協調がある」シナリオに限定

評価指標y1
従来手法では導出したが、提案では見逃した数（左図：横網掛け）
※「他コントローラとの協調」の有無に限定しない

有効性確認の結果：評価項目y（提案手法の見逃し）

従来手法で導出したハザード対策シナリオを提案手法は見逃していないか？
- 作業者2名は提案手法による見逃しはなし、他2名では見逃しあり
- 従来手法で導出したハザード対策シナリオの75%以上を提案手法は網羅

項目	値			
適用対象のシステム	システムA		システムB	
作業者	ドメインエキスパートA1	非ドメインエキスパートA2	ドメインエキスパートB1	非ドメインエキスパートB2
ハザード対策シナリオ数(従来手法)	30	8	41	16
従来手法では導出したが、提案手法では見逃した数（評価指標y1）	7	0	0	4
従来手法で導出したハザード対策シナリオに対して提案手法が網羅した割合（評価指標y2）	76.7%	100.0%	100.0%	75.0%



評価指標x1
従来手法では見逃したが、提案手法では導出したハザード対策シナリオ数（左図：縦網かけ）
※課題に対応する「他コントローラとの協調がある」シナリオに限定

評価指標y1
従来手法では導出したが、提案では見逃した数（左図：横網掛け）
※「他コントローラとの協調」の有無に限定しない

提案手法は、課題に対して有効であったが、従来手法を完全に網羅はできていない
補強する位置づけでの実施を推奨

有効性確認の結果：手法間の記述内容の傾向

「対策を講じるタイミング」では、明確な差あり
それ以外は、STAMP/STPAの成果物の出来に依存

	両手法の比較結果
ハザード対策シナリオ	
①どのハザードシナリオか	差なし
②どんな対策か	
②a どんな条件下で	
②a1 ハザードシナリオの前提	差なし
②a2 対策を講じるタイミング	差あり：従来は曖昧なものあり 提案はすべて明確
②b 誰が（対策を行う対象）	差なし（制御構造図の粒度）
②c どのように（処理ロジック）	差なし ※同一システムの作業者間では、ドメインエキスパートの方が具体的な記述多い
②d 何をするか（達成状態）	差なし
③システムの安全状態	差なし

まとめ

- 結論
  - 提案手法は、STAMP/STPA で導出したハザードシナリオに対する対策の検討において、アーキテクチャ階層を考慮した対策の導出を補強できる
  - 既存のハザード対策の導出手法と組み合わせた実施を推奨する

- 提案手法の限界
  - 対策の記述内容は、「対策を講じるタイミング」以外は、
    STAMP/STPAで導出したハザードシナリオの出来に依存する

- 今後の展開
  - STAMP/STPAによるハザードシナリオの導出を支援する方法を検討する
  - 適応対象（システムの特性）への依存性の評価を検討する

ご清聴　ありがとうございました