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

Methodology for Deriving Countermeasures for a Hazard in a System with Multiple Controllers Cooperating with Each Other Using STAMP/STPA and Event Sequence Diagrams

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
Japan Aerospace Exploration Agency, Research and Development Directorate, Research Unit III
○髙附　翔馬　　梅田　浩貴[1)]　植田　泰士[1)]　片平　真史[1)]　　森崎　修司[2)]
○Shoma Takatsuki　Hiroki Umeda[1)]　Yasushi Ueda[1)]　Masafumi Katahira[1)]　Shuji Morisaki[2)]

Abstract　We have applied the safety analysis method STAMP/STPA to the safety design of controllers for spacecraft systems that have multiple controllers that cooperate with each other for mission execution and safety. However, it has been difficult to derive countermeasures against hazard scenarios considering the architectural hierarchy only by STAMP/STPA. Therefore, we developed a method to support deriving countermeasures by visualizing the hazard scenarios derived by STAMP/STPA in event sequence diagrams and clarifying the timing and assumptions for taking countermeasures. This paper describes the method and the results of applying the method to two actual systems.

1.　はじめに

宇宙航空開発機構（JAXA）では、下記の製品特性を有するシステムを開発している。

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。

具体的には、他の宇宙機へ接近してドッキングする宇宙機システム[1]やスペースデブリを除去するためスペースデブリへ接近し捕獲する宇宙機システム[2]である。これらのシステムの開発では、接近するためのコントローラと接近後を担うコントローラのように、複数のコントローラが協調した安全設計が必要となる。このような安全設計において、ハザードに対する対策を検討する際、従来は分析対象のシステムの対策が中心に検討されていた。しかし、複数のコントローラが協調するシステムは、各コントローラが異なる認識した状態において、それぞれがどのような動作をする必要があるかなど、他のシステムの動作も含めた対策の検討が必要となる。

上述の製品特性を有するシステムには、ハザードを引き起こす要因にシステム構成要素（コントローラ等）間の相互作用を考慮できるシステム安全解析手法「System-Theoretic Process Analysis / STAMP based Process Analysis」（以下、STAMP/STPA）[3]が有効である。しかし、STAMP/STPA では、ハザードシナリオを導出するまでのガイド[4][5]はあるが、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、それを具体化するためのガイドは設定されていない。

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
Research Unit III, Research and Development Directorate, Japan Aerospace Exploration Agency
茨城県つくば市千現 2-1-1 Tel: 050-3362-2805　e-mail:takatsuki.shohma@jaxa.jp
2-1-1 Sengen, Tsukuba, Ibaraki, Japan
1) 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
Research Unit III, Research and Development Directorate, Japan Aerospace Exploration Agency
2）名古屋大学 大学院情報学研究科
Graduate School of Informatics, Nagoya University

【キーワード：】安全設計, 安全解析, STAMP/STPA, イベントシーケンス図, ハザード対策

また、上述の製品特性に類似するシステム（複数のコントローラを有する衝突回避システム）に対して、STAMP/STPA のハザードシナリオの導出を補強する研究[6]もあるが、ハザードシナリオに対する対策の導出までは言及されていない。

本稿では、上述の製品特性を有するシステムに STAMP/STPA を適用して導出したハザードシナリオに対して、対策の検討を支援する手法を提案する。

2. STAMP/STPA の概要と適用時の課題

2.1 STAMP/STPA の概要

安全解析手法として、システム構成要素自体の故障がシステム故障の原因であると考える手法に FTA(Fault Tree Analysis)や FMEA (Failure Mode and Effects Analysis)がある。一方で、STAMP/STPA は、システム構成要素間の相互作用がシステム故障を引き起こすと考える手法である。STAMP/STPA は、システム構成要素に「ハードウェア」のような自身が故障するものだけでなく、「ソフトウェア」や「人」を含めることができる。したがって、STAMP/STPA は FTA や FMEA より複雑なシステムを扱うことが可能である[4]。また、宇宙機システムのような複雑で巨大なシステムに適用され有効性が示されている[7]。

2.2 STAMP/STPA 適用時の課題

本項では、STAMP/STPA の分析の特徴に注目して課題を述べる。

STAMP/STPA では、システムの重大な損失（アクシデント）につながるシナリオ（以下、ハザードシナリオ）の要因（以下、ハザード要因）を、その因果関係を辿って分析する。図 1 にハザードシナリオのイベントの流れと STAMP/STPA の分析の流れを示す。ハザードシナリオのイベントの流れでは、初めに、シナリオの前提のもと、ハザード要因（Hazard Causal Factors：HCF）が発生する。次に、コントローラが判断条件に用いる状態値（プロセスモデル）と実際のシステムの状態値を誤認するより、コントローラが非安全なコントロールアクション（Unsafe Control Actions：UCA、以下、非安全操作）を行う。その結果、コントロール対象のプロセスが変化する。最終的に、システムはハザード状態になり、システム故障（アクシデント）が発生する[4]。ここで、ハザードシナリオを構成するイベントを時系列順に整理すると以下になる。

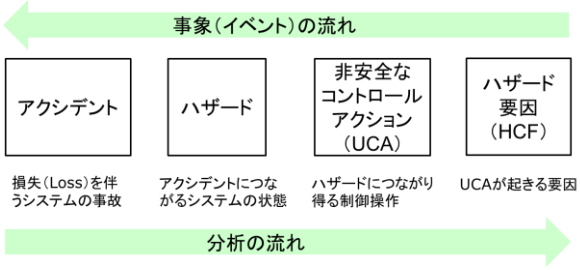

図 1 ハザードシナリオのイベントの流れと STAMP/STPA の分析の流れ

時系列順のハザードシナリオのイベント：

⓪ シナリオの前提（運用局面、システムの事前条件）
① ハザード要因が発生する
② コントローラが実際のシステムの状態を誤認する（判断条件に用いる状態値が変化する）
③ コントローラが非安全操作を行う
④ 非安全操作の結果、コントロール対象のプロセスが変化する
⑤ システムがハザード状態に遷移する
⑥ システム故障（アクシデント）が発生する

従来の STAMP/STPA では、ハザードシナリオに対する対策を時系列で分析するガイドがない。このため、ハザードシナリオに対する対策を導出する場合、作業者が頭の中でハザードシナリオのイベントを時系列順で整理しながら対策を行うタイミングを決定し、その時点のシナリオの前提を考慮して、システムが最終的にハザード状態にならないシナリオを考える必要がある。このため、従来の STAMP/STPA では、対策の内容がコンポーネントの冗長化やアルゴリズムの変更などの分析対象のコントローラが制御可能な範囲に限定されがちであった。

しかし、複数のコントローラが協調するシステムの場合、システムの安全状態を維持する対策として、1 つのコントローラが実際のシステムの状態を誤認していても、他のコントローラで対処できる可能性がある。例えば図 2 で示すとおり、分析対象のコントローラ及び制御下にあるセンサ等の構成要

素への対策（対策例 1 及び 2）だけでなく、分析対象のコントローラの制御外の要素であるアーキテクチャ階層上上位のコントローラと協調して行う対策（対策例 3）もあり得る。したがって、より適切なハザードシナリオに対する対策を採用するためには、従来のハザードシナリオに対する対策の導出方法（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がある。

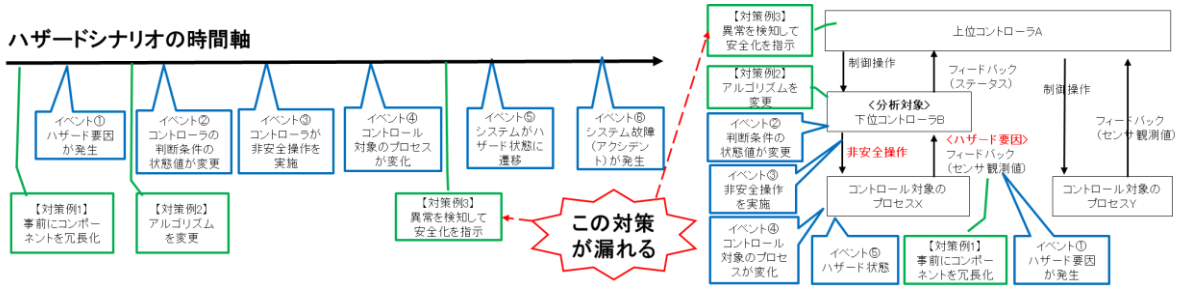

図 2 ハザードシナリオのイベントと対策の時間軸と制御構造の対応例

以上より、課題を以下のとおり整理する。

課題：ハザードシナリオに対する対策の導出時に、アーキテクチャ階層を考慮した対策が導出されない。つまり、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である。

この課題を解決するために、ハザードシナリオと対策後のシナリオを時系列で捉えることで、アーキテクチャ階層を考慮した対策の導出漏れを防ぐ方法を検討した。3 章ではこの方法について述べる。

3. 提案手法

前項の課題の解決方法として、STAMP/STPA とイベントシーケンス図(Event Sequence Diagram) [8] を用いたハザードシナリオに対する対策の導出を支援する手法（以下、提案手法）を提案する。

提案手法の工夫は 2 つある。1 つ目は、ハザードシナリオに対する対策を 3.1 項で述べる時系列別対策に区別して導出することである。対策を行うタイミングを分けて考えることで、各対策における「どのイベントまで起きたか」という前提が明確になる。その前提のもと、「各対策によってハザードシナリオが最終的にハザード状態にならないシナリオに分岐するためにはどんな対策が必要か」を思考することで、分析対象のアーキテクチャ階層のみではシステムの安全化が困難な場合に、アーキテクチャ階層上上位のコントローラ等の他アーキテクチャ階層と協調してシステムの安全化を行う対策が抽出されることがこの工夫の狙いである。2 つ目は、STAMP/STPA で導出したハザードシナリオとそのシナリオ上で時系列別対策を講じるタイミング及び対策後のシナリオをイベントシーケンス図の形式で可視化することである。作業者が頭の中でハザードシナリオのイベントを時系列で整理する必要なく、視覚的に対策を行うタイミングを把握することがこの工夫の狙いである。

提案手法では、ハザードシナリオに対する対策を「あるハザードシナリオにおいて、システムが最終的にハザード状態にならなくする（安全状態になる）対策」と定義し、ハザードシナリオに対する対策によってハザードシナリオから分岐するシナリオをハザード対策シナリオと定義する。表 1 に STAMP/STPA を用いてハザード対策シナリオを導出するまでの作業工程における参照物について、従来手法(STAMP/STPA のみ)と提案手法（STAMP/STPA + イベントシーケンス図）の比較を示す。

表 1 ハザード対策シナリオを導出するまでの作業工程で参照する情報の比較

作業工程	従来手法	提案手法
ハザードシナリオの導出	STAMP/STPA のガイド	
ハザード対策シナリオの導出	・前工程の成果物 ・ガイドなし	・前工程の成果物 ・対策を行うタイミングのガイド ・イベントシーケンス図で可視化したハザードシナリオ及びハザード対策シナリオ

3.1　時系列別対策

提案手法では、ハザードシナリオに対する対策を下記に示す3つの時系列別対策に分けて導出する。この時系列別対策の分け方の観点を述べる。

初めに、対策を「シナリオ以前に行うか、シナリオ中に行うか」の観点で区別する。時系列の境界となるイベントは、ハザードシナリオの初めのイベントを採用する。シナリオの前提を除いたハザードシナリオの初めのイベントは①「ハザード要因が発生する」(2.2項)である。したがって、シナリオ以前に行う対策、すなわち「ハザード要因の発生前に行う対策」を時系列別対策1とした。

次に、シナリオ中に行う対策を「分析対象のコントローラが判断条件に用いる状態値と実際のシステムの状態値を誤認しているかどうか」の観点で区別する。時系列の境界となるイベントは、ハザードシナリオのイベント②「コントローラが実際のシステムの状態を誤認する(判断条件に用いる状態値が変化する)」(2.2項)が該当する。したがって、シナリオ中に行う対策の内、分析対象のコントローラが実際のシステムの状態値を誤認する前に行う対策、すなわち「ハザード要因の発生後にコントローラが非安全操作をする前に行う対策」を時系列別対策2とした。一方で、シナリオ中に行う対策の内、分析対象のコントローラが実際のシステムの状態値を誤認した後に行う対策、すなわち「コントローラが非安全操作をした後に行う対策」を時系列別対策3とした。

時系列別対策1：ハザード要因の発生前に行う対策（ハザード要因を除去する対策）
時系列別対策2：ハザード要因の発生後にコントローラが非安全操作をする前に行う対策
（ハザード要因発生後に非安全操作を防止する対策）
時系列別対策3：コントローラが非安全操作をした後に行う対策（非安全操作後の対策）

3.2　ハザード対策シナリオの導出手順

提案手法では、以下の手順でハザード対策シナリオを導出する。

① ハザードシナリオを図3に示すイベントシーケンス図の形式で、各イベント(2.2項「ハザードシナリオを構成するイベントの順序」を参照)の時系列を可視化し、対策のタイミングを明確にする。
② 時系列別対策毎にシステムが最終的にハザード状態にならない(安全状態になる)対策を記述する。
③ ①～②をハザードシナリオごとに実施する。

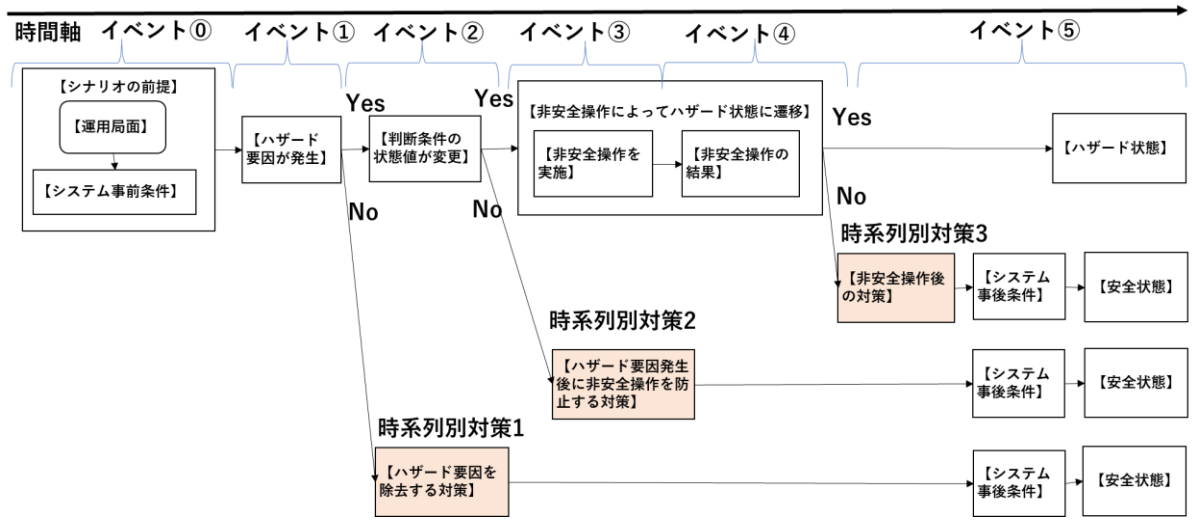

図3 イベントシーケンス図を用いたハザードシナリオと時系列別対策によるシナリオ分岐

4.　提案手法の有効性確認

本項では提案手法の有効性確認の内容を述べる。

4.1　有効性確認の方法と評価指標

初めに、後述する本稿で手法を適用したシステムに対して、STAMP/STPAによってハザー

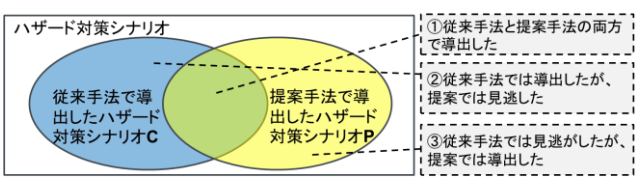

図4 両手法で導出したハザード対策シナリオの概念

ドシナリオを導出する。次に、従来手法と提案手法でハザード対策シナリオを導出する。ただし、参照する STAMP/STPA の成果物は両手法で共通とする。最後に、表 3 に示す評価指標を計測する。

表 3 評価項目と評価指標

記号	評価項目：何を評価するか？	記号	評価指標
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）	x1	従来手法では見逃したが、提案手法では導出した（※）「他コントローラとの協調の記述がある」ハザード対策シナリオ数　※図 4 の③に該当
		x2	評価指標 a1 のハザードシナリオ 1 件あたりの値
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？	y1	従来手法では導出したが、提案では見逃した数 ※図 4 の②に該当
		y2	従来手法で導出したハザード対策シナリオに対する提案手法で導出したハザード対策シナリオの網羅率

(1) 手法を適用したシステム

本稿で手法を適用したシステムは 2 つある。1 つは月面上で電力を確保しつつ障害物を避けながら探査を行うシステム（以下、システム A）である。図 5 にシステム A の月面探査の運用局面における制御構造を示す。もう 1 つは相手の宇宙機システムへ自動でドッキングを行うシステム（以下、システム B）である。図 6 にシステム B の自動ドッキングの運用局面における制御構造を示す。どちらのシステムも制御構造に複数のコントローラを有しコントローラ間で協調する（制御操作やフィードバックがある）システムであり、本稿で扱う製品特性（1 項「製品特性」）を有している。

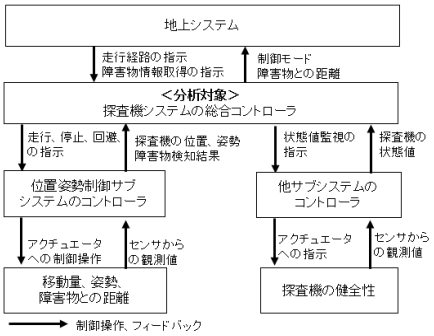

図 5 制御構造図（システム A）

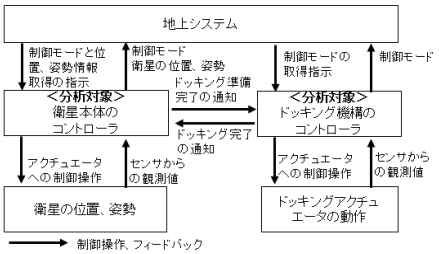

図 6 制御構造図（システム B）

(2) 作業者

作業者のドメイン知識の差による傾向を評価するため、本稿で手法を適用したシステムごとに、そのシステムのドメインにおける業務知識や経験が豊富な技術者（以下、ドメインエキスパート）とそうでない技術者（以下、非ドメインエキスパート）を 1 名ずつ用意した。以降では、システム A に対する作業者を「ドメインエキスパート A1」及び「非ドメインエキスパート A2」とし、システム B に対する作業者を「ドメインエキスパート B1」及び「非ドメインエキスパート B2」とする。

(3) 提案手法の適用上の課題と作業支援ツール

従来手法と比べた提案手法の適用上の課題は、作業者へイベントシーケンス図の記法の教育が必要であることと作業時の作図コストの増加がある。この課題を解決するため、我々は「ハザード対策シナリオ定義表」と「ハザードシナリオ定義表からイベントシーケンス図を自動生成する機能」からなるツール（以下、本ツール）を作成した。本ツールを使用することで、作業者が提案手法を適用する際に、イベントシーケンス図の記法の教育を必要とせず、またイベントシーケンス図の作図コストの増加を可能な限り低くした。本稿おいて、実際に提案手法を適用した際の作業手順を以下に示す。

- 分析フォーマットへ STAMP/STPA によって導出したハザードシナリオの内容を記入する
- 本ツールを用いて分析フォーマットからイベントシーケンス図を自動生成する
- イベントシーケンス図を参照して、分析フォーマットへ各時系列別対策の内容を記入する

- 再度、本ツールを用いて分析フォーマットからイベントシーケンス図を自動生成する
- 必要に応じて、分析フォーマットの対策の各時系列別対策の内容を修正・追記する

4.2 有効性確認の結果

表 4～6 に提案手法の有効性確認の結果を示す。

表 4 両手法で導出したハザード対策シナリオ数の内訳

No	項目		値											
1	適用対象のシステム		システムA						システムB					
2	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		
3	ハザードシナリオ数		20			10			41			12		
4	ハザード対策シナリオ導出の手法		従来	提案		従来	提案		従来	提案		従来	提案	
5	ハザード対策シナリオ数	【時系列別対策1】ハザード要因を除去する対策	30	63	22	8	27	9	41	105	31	16	41	12
6		【時系列別対策2】ハザード要因発生後に非安全操作を防止する対策			20			8			37			12
7		【時系列別対策3】非安全操作後の対策			21			10			37			17
8	ハザード対策シナリオ数（他コントローラとの協調の記述がある）	【時系列別対策1】ハザード要因を除去する対策	12	29	4	3	15	5	7	44	7	6	19	2
9		【時系列別対策2】ハザード要因発生後に非安全操作を防止する対策			8			0			0			1
10		【時系列別対策3】非安全操作後の対策			17			10			37			16

表 5 両手法におけるハザード対策シナリオの対応関係

No	項目	記号	値			
1	適用対象のシステム	-	システムA		システムB	
2	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
3	ハザードシナリオ数	n(ハザードシナリオ)	20	10	41	12
4	従来手法で導出したハザード対策シナリオ数	n(従来)	30	8	41	16
5	提案手法で導出したハザード対策シナリオ数	n(提案)	63	27	105	41
6	従来手法と提案手法の両方で導出した数	n(従来 ∩ 提案)	23	8	41	12
7	従来手法で導出したハザード対策シナリオに対する提案手法で導出したハザード対策シナリオの網羅率（評価指標y2）	n(従来 ∩ 提案) / n(従来)	**76.7%**	**100.0%**	**100.0%**	**75.0%**
8	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）	n(従来) - n(従来 ∩ 提案)	**7**	**0**	**0**	**4**
9	従来手法では見逃がしたが、提案手法では導出した数	n(提案) - n(従来 ∩ 提案)	40	19	64	29

表 6 両手法のハザード対策シナリオの対応関係（他コントローラとの協調の記述あり）

No	項目	記号	値			
1	適用対象のシステム	-	システムA		システムB	
2	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
3	ハザードシナリオ数	n(ハザードシナリオ)	20	10	41	12
4	従来手法で導出したハザード対策シナリオ数	n(従来)	12	3	7	6
5	提案手法で導出したハザード対策シナリオ数	n(提案)	29	15	44	19
6	従来手法と提案手法の両方で導出した数	n(従来 ∩ 提案)	11	3	7	5
7	従来手法で導出したハザード対策シナリオに対する提案手法で導出したハザード対策シナリオの網羅率	n(従来 ∩ 提案) / n(従来)	91.7%	100.0%	100.0%	83.3%
8	従来手法では導出したが、提案手法では見逃した数	n(従来) - n(従来 ∩ 提案)	1	0	0	1
9	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）	n(提案) - n(従来 ∩ 提案)	**18**	**12**	**37**	**14**
10	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）	(n(提案) - n(従来 ∩ 提案)) / n(ハザードシナリオ)	**0.90**	**1.20**	**0.90**	**1.17**

4.3 考察

(1) 評価項目 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？

表 6 に注目する。評価指標 x1（No 列:9）がすべての作業者において 1 以上であることから、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が導出できたことがわかる。また、評価指標 x2（No 列:10）からすべての作業者において、ハザードシナリオ 1 件あたり 0.9～1.2 件の当該シナリオが導出できていることがわかる。ここで、本稿で手法を適用したシステムごとに作業者のドメイン知識の観点で比較する。評価指標 x2（No 列:10）は、ドメインエキスパート（A1, B1）の値 0.90 よりも非ドメインエキスパート(A2, B2)の値 1.17～1.20 の方が高い。この結果が有意であると仮定すると、ドメイン知識が少ない作業者の方が提案手法が有効であることを意味する。この作業者のドメイン知識の差による傾向を調査するためには、他システムへ適用した事例を増やす必要がある。

(2) 評価項目 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？

表 5 に注目する。評価指標 y2（No 列:7）からすべての作業者で従来手法で導出したハザード対策シナリオの内、75%以上を提案手法で導出していることがわかる。

また、評価指標 y1 (No 列:8) からドメインエキスパート A1 と非ドメインエキスパート B2 において、提案手法による従来手法で導出したハザード対策シナリオの見逃しが、それぞれ 7 件、4 件あることがわかる。ここで、表 7 に「従来手法では導出したが、提案手法では見逃したハザード対策シナリオ」の内訳を示す。ドメインエキスパート A1 では、「対策を講じる対象にコントローラを含む」方のハザード対策シナリオが多く、一方で、非ドメインエキスパート B2 では、「対策を講じる対象にコントローラを含まない」方のハザード対策シナリオが多かった。これは、作業者の業務ドメインの違いによる影響と考える。ドメインエキスパート A1 はソフトウェア開発が主の業務であり、非ドメインエキスパート B2 はハードウェアを含めたシステム開発が主の業務である。従来手法のハザード対策シナリオの導出作業では、提案手法のガイドにとらわれず、普段の業務で使用している対策を導出する思考プロセスを各作業者が行ったため、作業者自身の業務ドメインに合致する内容のハザード対策シナリオが提案手法に比べて比較的多く導出された、と考える。

表 7 「従来手法では導出したが、提案手法では見逃したハザード対策シナリオ」の内訳

No	項目	値			
1	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B2	
2	従来手法では導出したが、提案手法では見逃したハザード対策シナリオ数（**評価指標y1**）	7		4	
3	対策を講じる対象にコントローラか含まれるか？含まないか（機器の冗長化や構造の変更などのハードウェアのみ）？	コントローラを含む	コントローラを含まない	コントローラを含む	コントローラを含まない
4	従来手法では導出したが、提案手法では見逃したハザード対策シナリオの内、No3に該当するシナリオ数　※括弧の中は「他コントローラとの協調の記述がある」シナリオ数	6 (1)	1	1 (1)	3

(3) ハザード対策シナリオの記述の曖昧さ

従来手法と提案手法で導出したハザード対策シナリオの記述の曖昧さについて定性的に述べる。ここで、ハザード対策シナリオの記述内容ごとに曖昧さの傾向を従来手法と提案手法で比較した結果を表 8 に示す。ハザード対策シナリオの記述の曖昧さにおける従来手法と提案手法の傾向の差は、「対策を講じるタイミング（②a2)」のみ明確に見られた。これは、提案手法が、対策を講じるタイミングをガイドしているためと考える。また、ドメインエキスパートと非ドメインエキスパートの記述の曖昧さは、「どのように（②c)」と「何をするか（②d)」で見られた。

以上より、STAMP/STPA のみでは考慮が難しいハザード対策シナリオが提案手法の適用により増加したことから提案手法の有効性を示唆できた。有効性をより検証する項目として、作業者のドメイン知識の差の他に適用するシステムの規模、作業工数が考えられる。また、提案手法は「ハザード対策シナリオの導出」の前工程である「ハザードシナリオの導出」工程で STAMP/STPA の成果物が十分に特定できていない場合は有効でない、という限界がある。

表 8 ハザード対策シナリオの記述の曖昧さにおける従来手法と提案手法の比較

記号	記述内容	曖昧さの傾向の比較
①	どのハザードシナリオ	両手法の差なし（共通の成果物を使用）
②	どんな対策	N/A
②a	どんな条件下で	N/A
②a1	ハザードシナリオのシナリオ前提	両手法の差なし（共通の成果物を使用）
②a2	対策を講じるタイミング	従来手法は曖昧なものあり。 提案手法はすべて明確。
②b	誰が（対策を行う対象）	両手法の差なし（共通の成果物を使用） ※STAMP/STPA で特定する制御構造図の粒度
②c	どのように（処理ロジック）	両手法の差なし。 ただし、ドメインエキスパートの方が非ドメインエキスパートよりも具体的な記述が多い。
②b	何をするか（達成状態）	
③	安全状態	両手法の差なし（共通の成果物を使用）

5. まとめ

本稿では、「複数のコントローラが協調するシステム」において、STAMP/STPA で導出したハザードシナリオに対する対策の検討を支援する手法を提案し、有効性を示した。提案手法により、ハザードシナリオに対する対策の検討時に、漏れがちであったアーキテクチャ階層を考慮した（他コントローラと協調する）対策シナリオを増やすことができる。しかし、提案手法のみでは作業者が使い慣れた手法で導出できていたハザード対策シナリオを見逃す可能性もあるため、提案手法を使い慣れた手法に組み合わせて使用することを推奨する。

6. 参考文献

[1] Tomita, Y., Umeda, H., Kawatsu, K., Iwai, S., Usuku, K., Tsujita, D., Nomoto, H., Takatsuki, S., Horikawa, M., Uchiyama, T. and Maeda, M., “Behavior Analysis and Integration of HTV-X Automated Docking Demonstration Mission with Model Based Systems Engineering Approach”, 33rd International Symposium on Space Technology and Science (ISTS), 2022.
[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.
[3] Leveson, N. G., “Engineering a Safer World”, MIT Press, Cambridge, pp.171-249, 2012.
[4] Leveson, N. G. and Thomas, J. P., “STPA HANDBOOK 日本語版 Ver.0.2”, 2018,
[5] 独立行政法人情報処理推進機構（IPA）, “はじめての STAMP/STPA～システム思考に基づく新しい安全性解析手法～”, 2016, https://www.ipa.go.jp/sec/reports/20160428.html(参照 2023-08-14).
[6] Takatsuki, S., Umeda, H., Kobayashi, T., Sasaki, T., Ueda, Y., Katahira, M. and Morisaki, S., “Hazard Scenarios Analysis Method Using STAMP/STPA and Sequence Diagrams in A Collision Avoidance System with Multiple Controllers”, 12th IAASS Conference, 2023.
[7] Ishimatsu, T., Leveson, N. G., Thomas, J. P., Fleming, C. H., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H. and Hoshino, N., “Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis”, Journal of Spacecraft and Rockets, Vol. 51, No. 2, pp. 509-522, 2014.
[8] National Aeronautics and Space Administration, “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners Second Edition”, NASA/SP-2011-3421, December 2011