STAMP/STPA とシーケンス図を用いたコントローラ間の相互作用があるシステムにおける安全設計手法の提案

Safety Design Methodology for Systems with Controller Interaction Using STAMP/STPA and 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 applied the safety analysis method "STAMP/STPA" to the safety design of a controller for a spacecraft system with a product characteristic that "each controller has a feedback loop and interferes with each other's feedback loop due to communication between controllers and physical actions of actuators". However, it was found that it is difficult to identify hazard causal factors by only using control loops to analyze the external system components and the constraints on the time and sequence of their behavior. Therefore, we attempted to improve the analysis by adding SysML sequence diagrams to STAMP/STPA. 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、宇宙機システムの開発で安全設計を実施しているが、これは複数のコントローラが協調して他システム等と衝突を回避すること等を目的としている。特にコントローラとコントロール対象が複数あり、互いに協調動作する場合（図 1）、制御操作である各アクチュエータの動作状態とその影響（位置や姿勢等）及び、フィードバックである複数のセンサ間の特性やコントローラ間の通信等を考慮する必要がある。宇宙機システムの安全設計において、これらの内容が漏れることはシステム運用時の重大な損失につながるシナリオ（以降、ハザードシナリオ）が漏れることであるため、これらの考慮漏れを防ぐ必要がある。

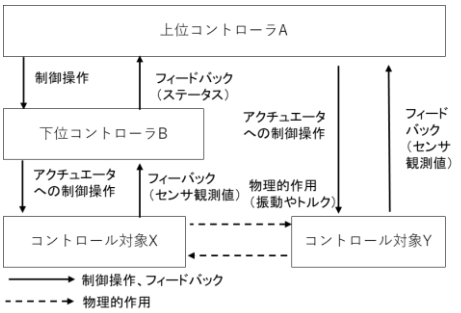

図 1 対象とする製品特性を有するシステムの制御構造の例

製品特性：各コントローラがフィードバックループを持ち、コントローラ間の通信やアクチュエータの物理的作用により互いのフィードバックループに干渉し合う。

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：】STAMP/STPA, 安全設計, MBSE, SysML, シーケンス図

システム構成要素間の相互作用に着目した安全解析手法として STAMP/STPA[1]~[3] (Systems Theoretic Accident Model and Processes / System-Theoretic Process Analysis)がある。STAMP/STPA を上述の製品特性を有するシステムへ適用したところ、外部システムの構成要素や振る舞いの順序や時間に関する分析が漏れがちであった。そこで、STAMP/STPA に SysML のシーケンス図[4]を加えて分析することで改善を試みた。

本論文では、上述の製品特性を有するシステムのコントローラの安全設計において、STAMP/STPA を補強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、システム故障の原因はシステム構成要素の故障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、システム故障の原因はシステム構成要素間の相互作用であると考え、システムが自身の実際の状態とシステムが想定する状態（プロセスモデル）を誤認識することで、「非安全なコントロールアクション」(以降、UCA) を行うことがシステム故障の原因とする解析手法である。

STAMP/STPA のメリットは、システム構成要素に「ハードウェア」のような自身が故障し得るものだけでなく、「ソフトウェア」や「人」を含めることができる点にある。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り、人工衛星のような宇宙機システムに対して有効性が示されている[5]。

2.2 STAMP/STPA 適用時の課題

STAMP/STPA のハザード誘発要因（以降、HCF）を特定する工程においては、図 2 で示すコントロールループとガイドワードが用いられる[2]。

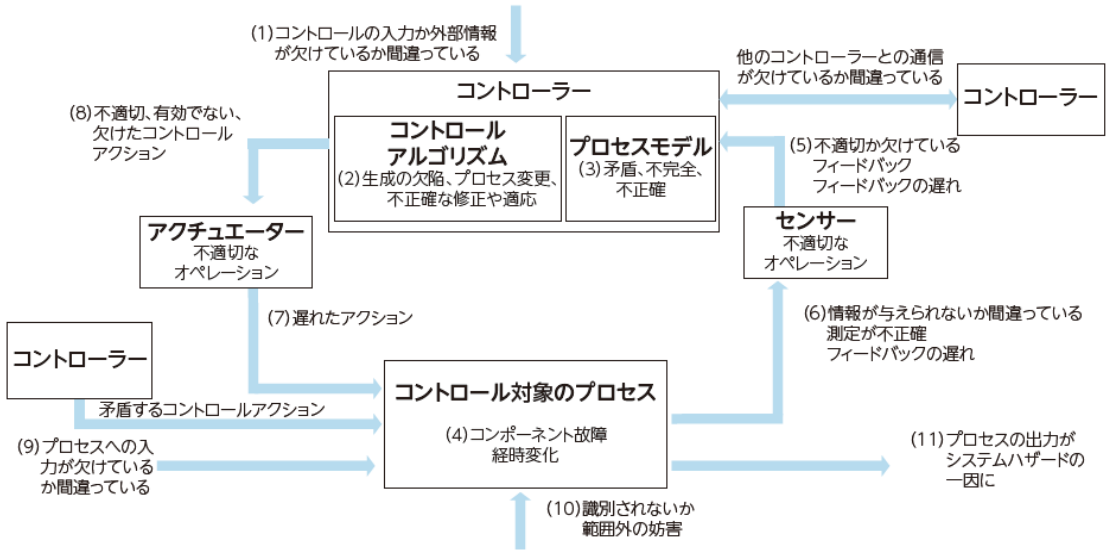

図 2 HCF を特定する工程で使用するコントロールループとガイドワード

「1.はじめに」の「製品特性」を有するシステムに STAMP/STPA を適応した場合、HCF を特定する工程で以下の課題が発生した。

【課題 1】外部コントローラからの制御指示とコントロール対象の観測値を組み合せた分析が漏れる
【課題 2】外部コントローラが制御するアクチュエータの物理的作用の影響の分析が漏れる
【課題 3】制御指示や観測値取得の「順序」やアクチュエータの「動作時間」などの時間に関する制約に関する分析が漏れる

これらの考慮漏れにより特定すべき HCF が漏れ、さらにハザードシナリオの漏れにつながるため、上述の課題で挙げた考慮漏れを防ぐことが必要である。

本課題の詳細について、従来手法である STAMP/STPA のコントロールループと提案手法で使用するシーケンス図を用いて説明する。図 3 にハザードに繋がる UCA に対してその要因を分析するコントロールループ（従来）とそのときの振る舞いをシーケンス図（提案）で示す。

STAMP/STPA では、HCF を特定する手順として、コントロールループ上で UCA の要因を時系列で因果関係を遡る手順となっている。つまり、図 3 のコントロールループで要因①～⑤の順で UCA との因果関係を分析するため、「UCA を含むループ」の分析が主となる。

しかし、「1. はじめに」の「製品特性」を有するシステムでは、分析対象のコントロールループ以外のコントロールループの構成要素（外部コントローラや外部アクチュエータ等）の影響を考慮する必要がある。この影響の分析は「UCA を含むループ」のみでは不十分であり、「UCA を含むループ」から１つ前のループを遡る且つ、外部コントローラが属するコントロールループを含めることが重要である。従来のコントロールループでは 2 つ以上のループを分析するガイドはないことから、外部コントローラからの制御指示や外部アクチュエータの物理的作用による影響とコントローラ自身の制御操作を同時に考慮した分析が漏れやすい（課題 1、課題 2）。また、従来のコントロールループのみの分析では、「振る舞いの順序や時間に関する制約」を記述するルールがなく、またそれらを記述できても表現が 1 つの操作情報として記述される。このため、他の制御操作との関係を明確にできず、「振る舞いの順序や時間に関する制約」を考慮した分析が漏れやすい（課題 3）。

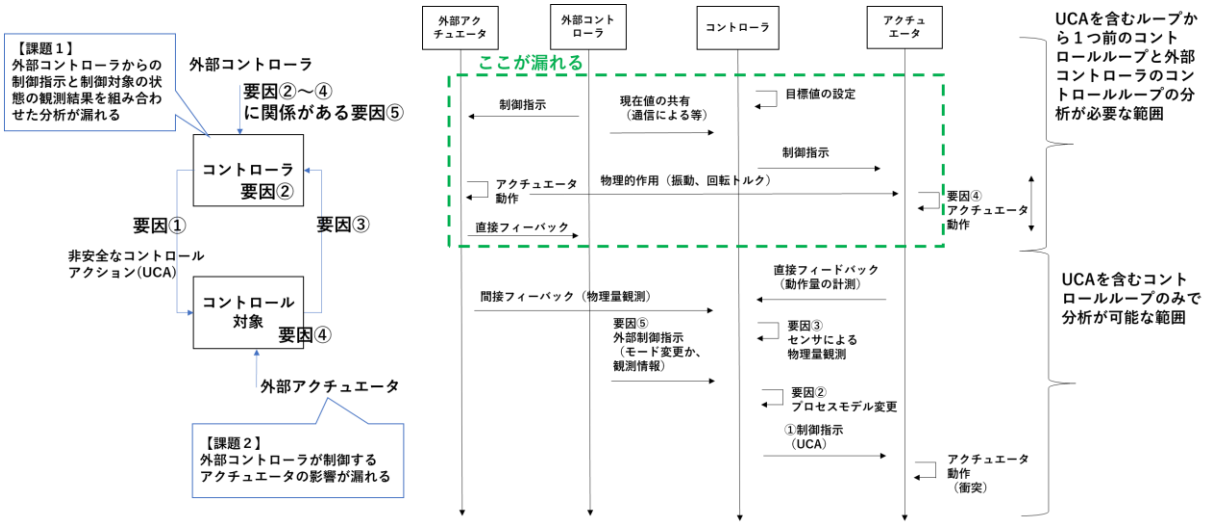

図 3 外部システムの構成要素に起因する課題（課題 1 と課題 2）における
コントロールループ（従来）とシーケンス図（提案）の対応

3. 提案手法

3.1 概要

前項で挙げた課題を解決するために、本研究では従来手法(STAMP/STPA)の Step2 で行うコントロールループを用いた HCF の分析において、システム外部構成要素と時間や順序の制約を入れたシーケンス図（以降、制約付きシーケンス図）を加えた分析を行うことを提案する。従来手法(STAMP/STPA)の分析手順と提案手法の関係を図 4 に示す。

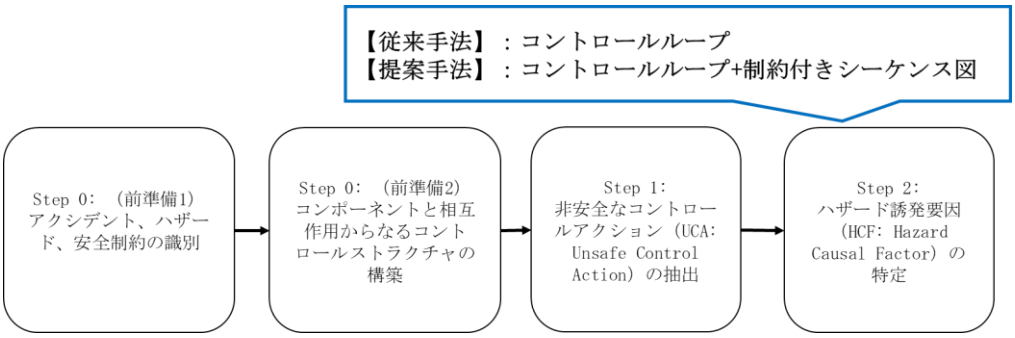

図 4 STAMP/STPA の分析工程と提案手法の関係

3.2 制約付きシーケンス図

制約付きシーケンス図の作成方針を表 1 に示す。

表 1 制約付きシーケンス図の作成方針

No.	項目	方針
1	構成要素の抽出	分析対象のコントローラを中心とした以下の構成要素とする。 ・ 分析対象のコントローラのコントロールループに登場する構成要素（コントローラ、センサ、アクチュエータ、外部環境） ・ 分析対象のコントローラと入出力関係のある外部システムの構成要素とその構成要素が属するコントロールループに登場する構成要素 ※コントローラ以外の構成要素はライフラインとしての表現でなくても、コントローラの自己メッセージとしての表現も可とする。
2	シーケンスの範囲	・ コントローラの UCA からコントロールループを遡った直近のコントローラの通常の操作（1 つ前のループ） ・ プロセスモデル（自身が認識する状態値）が更新される範囲
3	時間に関する制約	以下を該当するメッセージに対して記述する。 ・ アクチュエータの動作：所要時間、開始/停止の条件 ・ センサや通信の受信/送信：周期
4	順序に関する制約	以下を該当するメッセージに対して記述する。 ・コントローラのプロセスモデルの更新のための制御操作に順序がある場合、その順序に関する制約(操作の同期性や特定状況下で順番等)を記述する。
5	プロセスモデルの有効期限	制御ループが 2 重構造である場合、その上位下位コントローラ間の情報の同期周期と各プロセスモデル（自身が認識する状態値）の有効時間を記述する。
6	物理的作用	制御対象の物理量に着目して、外部システムのアクチュエータや外部環境によって発生するセンサ上の制約とアクチュエータへ影響を記述する。

特にシーケンス図のメッセージの記述方針に関する表 1 の No3～6 の記述例を図 5～9 以下に示す。各図の赤字部分が表 1 の方針に該当する記述である。

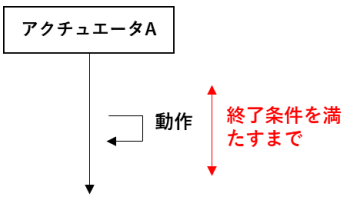

図 5 時間に関する制約の記述例
（アクチュエータの動作）

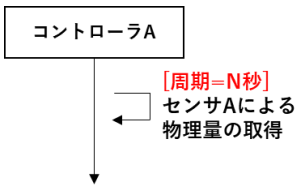

図 6 時間に関する制約の記述例
（センサの周期）

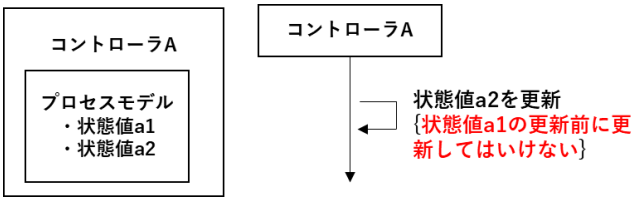

図 7 順序に関する制約の記述例

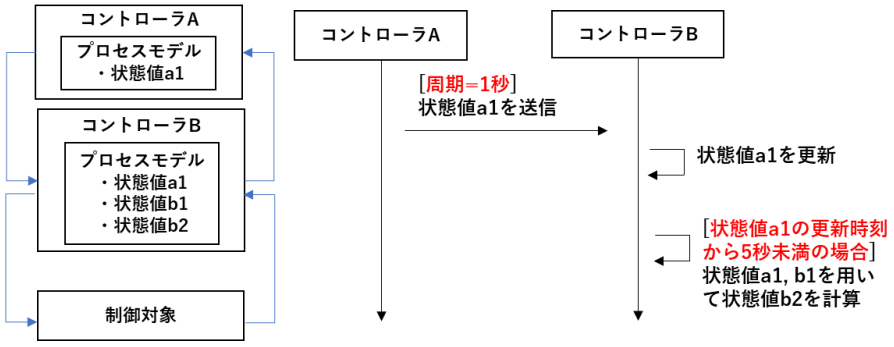

図 8 順序に関する制約の記述例

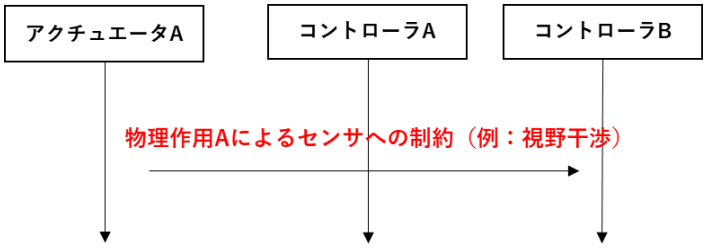

図 9 物理的作用の記述例

4. 提案手法の有効性確認

4.1 有効性確認の方法

製品特性「各コントローラが別々のフィードバックループを持ち、コントローラ間の通信やアクチュエータの物理的作用により互いのフィードバックループに干渉し合う」を有するシステム A、システム B に対して、従来手法（STAMP/STPA）と提案手法（STAMP/STPA +シーケンス図）でハザードシナリオの数を比較した。具体的な手順を以下に示す。

(1) 有効性確認の手順

1. 従来手法（STAMP/STPA）でハザードシナリオを作成する
2. 3.2 項記載の作成方針で「制約付きシーケンス図」を作成する
3. 「制約付きシーケンス図」を用いて再度、ハザードシナリオを作成する
4. 提案手法によりハザードシナリオが新規に作成されるか、また新規作成されたハザードシナリオが「従来手法の本質的な見落としかどうか」、「従来手法の本質的な見落としがどの課題に対応するか」確認する

(2) 手法を適用したシステム

システム A とシステム B の制御構造を図 10 と図 11 に示す。

システム A は、宇宙機 A と宇宙機 B が相対位置を保ちながら衝突しないように航行するシステムである。宇宙機 A が制御上の上位であり、宇宙機 A と宇宙機 B はどちらも自身のアクチュエータ（スラスタ）により相対位置を制御する特徴がある。また、宇宙機Ａと宇宙機Ｂは互いに通信により定期的に自身の位置、速度等の情報を相手に送信し、受信側はその値に基づき制御量の目標値を計算する。

システム B は、1 つの宇宙機内に姿勢を制御するコントローラ（姿勢制御コントローラ）と姿勢制御コントローラや構造物の展開収縮を制御するコントローラ（総合コントローラ）があり、協調して宇宙機が破損しないようにそれぞれのコントロール対象を制御するシステムである。どちらのコントローラも 1 つの宇宙機の物理的な状態を制御しているため、自身のアクチュエータが発生させた物理的作用（振動やセンサ視野への干渉）が相手のフィードバックループへ影響する特徴がある。

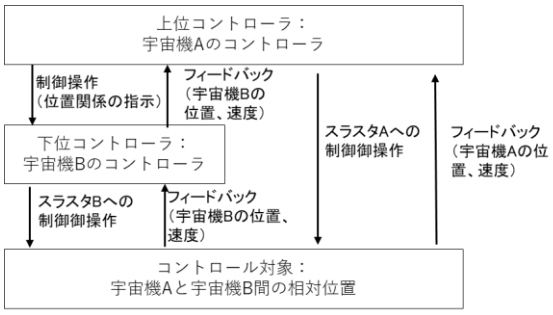

図 10 制御構造図（システム A）

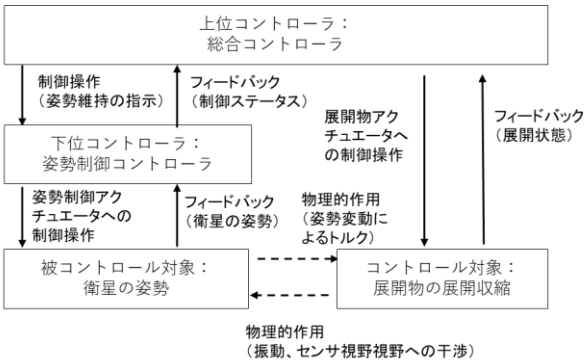

図 11 制御構造図（システム B）

4.2 有効性確認の結果

有効性の確認結果及び各内訳で使用する分類とその定義を表 2～5 に示す。

表 2 提案手法適用後のハザードシナリオの分類と定義

分類	定義
変更なし	提案手法適法前とシナリオの記述に変更がない。
記述が詳細化	UCA が発生する状況や入出力情報が具体化された。
新規（本質的な見落とし）	上記以外。従来手法での本質的な見落としと見なす。

表 3 提案手法適用による新規のハザードシナリオの分類と定義

分類	定義
外部コントローラとの相互作用漏れ（課題 1）	外部システムのコントローラからの制御指示等の相互作用が含まれる。
外部アクチュエータの影響漏れ（課題 2）	外部システムのアクチュエータによる物理的作用が含まれる。
順序・時間に関する制約の漏れ（課題 3）	上記以外でコントローラ、アクチュエータ、センサの振る舞いに順序や時間に関する記載がある。

表 4 ハザードシナリオの内訳(システム A)

ハザードシナリオ数		提案手法適用後のハザードシナリオの内訳		提案手法適用による新規ハザードシナリオの内訳	
提案手法適用前	15				
提案手法適用後	34	変更なし	12		
		記述が詳細化	3		
		新規（本質的な見落とし）	19	外部コントローラとの相互作用漏れ（課題 1）	11
				外部アクチュエータの影響漏れ（課題 2）	0
				順序・時間に関する制約の漏れ（課題 3）	8

表 5 ハザードシナリオの内訳(システム B)

ハザードシナリオ数		提案手法適用後のハザードシナリオの内訳		提案手法適用による新規ハザードシナリオの内訳	
提案手法適用前	66				
提案手法適用後	74	変更なし	59		
		記述が詳細化	9		
		新規（本質的な見落とし）	6	外部コントローラとの相互作用漏れ（課題 1）	1
				外部アクチュエータの影響漏れ（課題 2）	4
				順序・時間に関する制約の漏れ（課題 3）	1

4.3 考察

特に「提案手法適用による新規シナリオの内訳」に注目して考察する。

・シナリオの質

提案手法適用前である従来手法（STAMP/STPA）の分析の時点でシステムの重大な損失に繋がるハザードを特定している。提案手法ではこのハザードに繋がる HCF が他にないかを制約付きシーケンス図を加えて分析する。したがって、提案手法により新規作成されたハザードシナリオはすべてシステムの重大損失に繋がる重要なシナリオである。

・システム A

表 4 の「提案手法適用による新規シナリオの内訳」から「外部コントローラとの相互作用漏れ」と「時間・順序制約の漏れ」のシナリオが作成されたことがわかる。これは、システム A は制御ループが 2 重構造を持ち情報の同期処理を多く行う特徴があり、制約付きシーケンス図にそれらの周期やプロセスモデルの更新周期を記述した効果である。一方で、「外部アクチュエータの影響漏れ」のシナリオは 0 件であったが、図 10 のとおりシステム A は外部アクチュエータが物理的な影響を及ぼさないシステムのため妥当である。

・システム B

提案手法適用による新規シナリオの中では、「外部アクチュエータの影響漏れ」が比較的多く作成された。これは図 11 のとおりシステム B は外部アクチュエータが物理的な影響を及ぼすシステムであり、その影響を考慮したためである。

以上より、STAMP/STPA のみでは考慮が難しいハザード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ためには、適用するシステムの規模や分析者を複数用意し実験を行う必要がある。一方で、本手法はシーケンス図に記述する制約を抽出できないと有効でない、という限界がある。

5. まとめ

STAMP/STPA の HCF の特定を補強する手法として SysML のシーケンス図を用いる方法を提案した。本手法により、外部システムのコントローラとの相互作用やアクチュエータの影響及び振る舞いの順序や時間に関する制約を考慮したハザードシナリオを増やすことができる。しかし、シーケンス図に表現する制約が少ないと本手法の効果が薄くなると考える。この制約の抽出は分析者のドメイン知識への依存が大きい。したがって、ドメイン知識が乏しい技術者が本手法を有効活用するためには、今後の検討が必要である。

6. 参考文献

[1] Leveson, N. G.、Engineering a Safer World、MIT Press、Cambridge、pp.171-249、2012
[2] Leveson, N. G. and Thomas, J. P.、 STPA HANDBOOK 日本語版 Ver.0.2、2018、http://psas.scripts.mit.edu/home/get_file2.php?name=STPA_handbook_japanese.pdf(参照 2022-08-02)
[3] 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 2022-08-18）
[4] Object Management Group、 OMG Systems Modeling Language（OMG SysML）Version 1.4、2015
[5] 山田将史, 仲瀬寛輝, 小木曽望, 南部陽介、STPA を用いた超小型人工衛星のレジリエントな運用モデルの構築、航空宇宙技術論文、Vol.21、pp.31-39, 2022