第 3 回 STAMP ワークショップ発表概要

タイトル

STAMP/STPA による自動制御システムの安全解析

Application of STAMP/STPA to Automatic Control System in Safety Analysis

著者・発表者

有人宇宙システム株式会社　道浦 康貴

Japan Manned Space Systems Corporation　Yasutaka Michiura

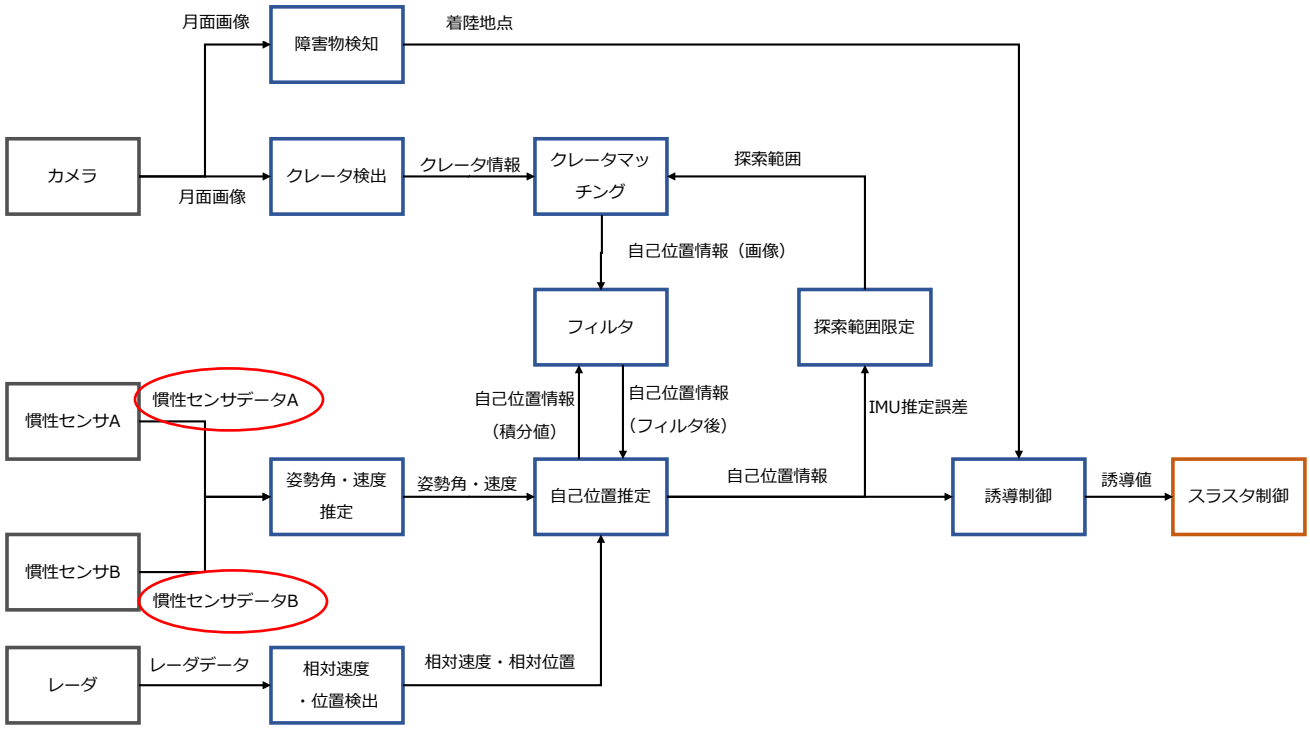
概要

近年、宇宙機／航空機／自動車などのシステムは大規模、複雑になり、かつ、自動制御されるという特徴がある。このようなシステムを STAMP/STPA を用いて分析する時、いくつかの課題が明確になってきた。今回のプレゼンでは、宇宙機の事例を基に、STAMP/STPA 分析の課題とその解決案を紹介する。

課題 1： 4 つのガイドワード分析の盲点

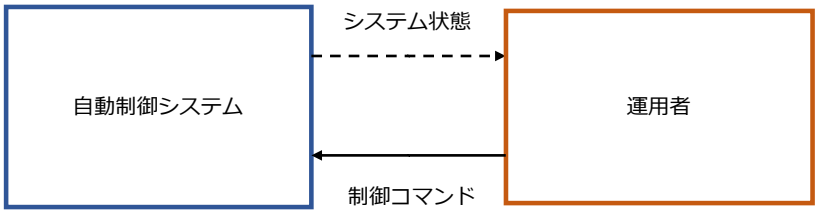
Step.1 では、Control Action（CA）毎に 4 つのガイドワードを適用して Unsafe Control Action（UCA）を識別するが、自動制御システムのような複雑なシステムを分析する場合、CA 毎にガイドワード用いた分析のみだと、識別することができないハザードシナリオがある。

例えば、下図のような Control Structure の場合、慣性センサデータ A / B のいずれかが提供されなくてもハザードには至らない。これは、機能が冗長化されていることから、片方の CA が提供されなくても、システムとして対応可能な設計になっているためである。しかし、両方の CA が共に提供されないと、機能が成立せずハザードに至る。このようなハザードシナリオを識別するためには、複数の CA の振る舞いを考慮した分析が必要となる。



課題 2：存在しない CA の識別

自動制御システムの場合、正常動作時には、運用者の介在を必要としなくても、異常が発生した時は、運用者の介在を必要とする場合がある。このような時、運用者がシステムを適切に操作するためには、自動制御システムの状態を知ることが必要となる。例えば、Step.1 では、CA が提供されない状況を分析することは可能であるが、下図のように、そもそも設計上、CA（システム状態）が存在しないような時は、ガイドワードによる分析は実施できない。



上述した課題 1、2 を解決するためには、個別の CA だけに着目して分析するだけではなく、Control Structure の構造からシステムの特徴を捉え、ハザードシナリオを識別するという作業が必要となる。

キーワード

(1) STAMP/STPA

(2) Automatic control system

(3) Human-machine system

(4) Hazard analysis

(5) Spacecraft