STAMP/STPAによる
自動制御システムの安全解析

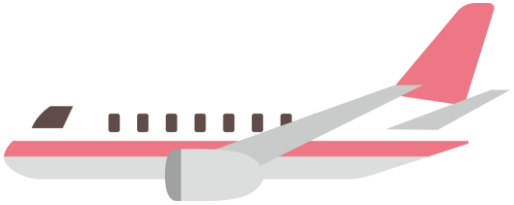
2018年12月3日

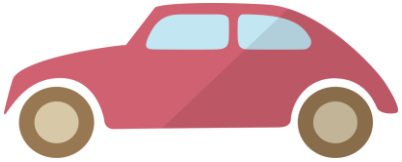
有人宇宙システム株式会社
IV&V研究センター
道浦 康貴
michiura.yasutaka@jamss.co.jp

はじめに

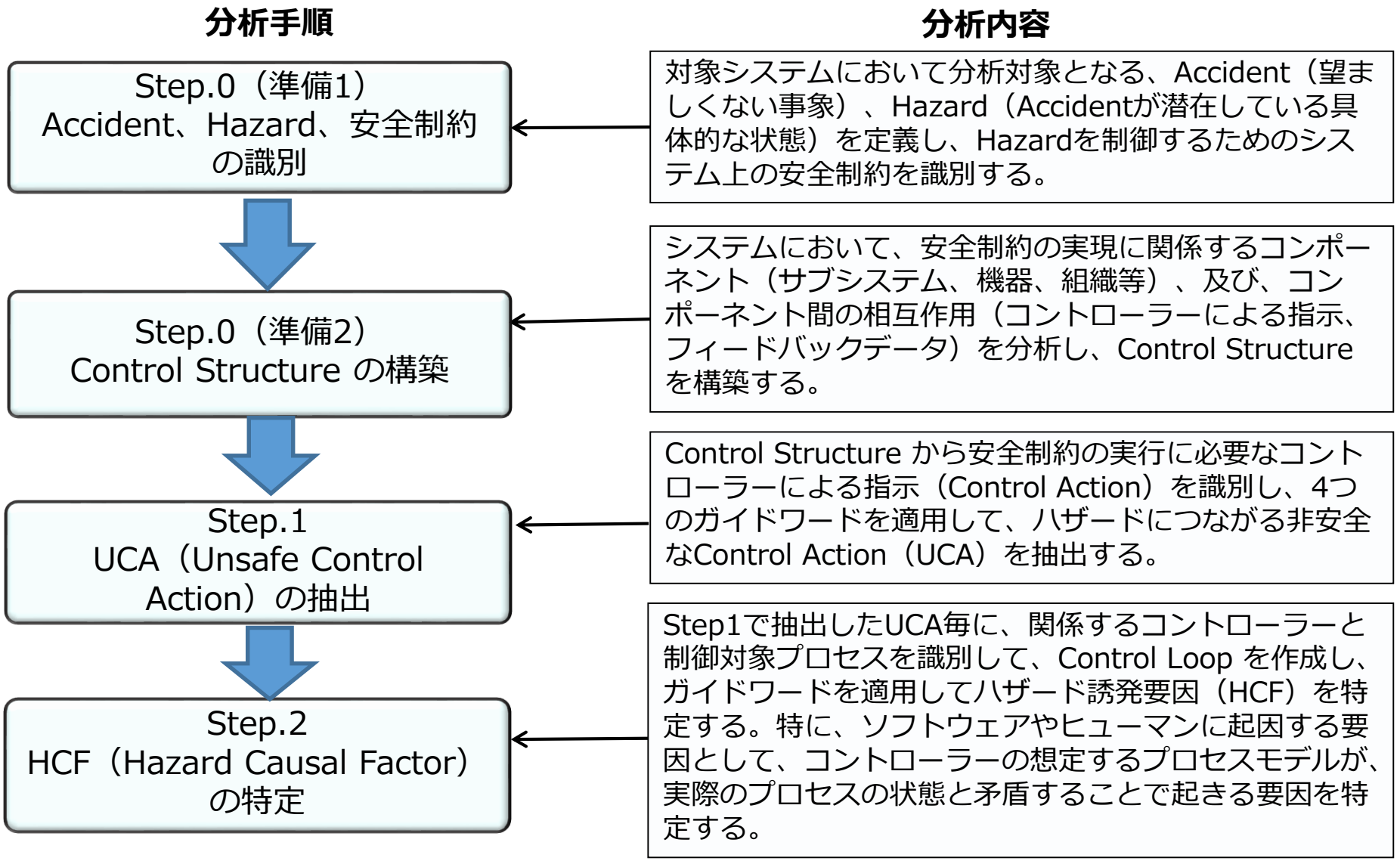
近年、宇宙機／航空機／自動車などのシステムは大規模、複雑になり、かつ、自動制御されるという特徴がある。このようなシステムをSTAMP/STPAを用いて分析する時、いくつかの課題が明確になってきた。今回の発表では、宇宙機の事例を基に、STAMP/STPA分析の課題とその解決案を紹介する。

©JAXA



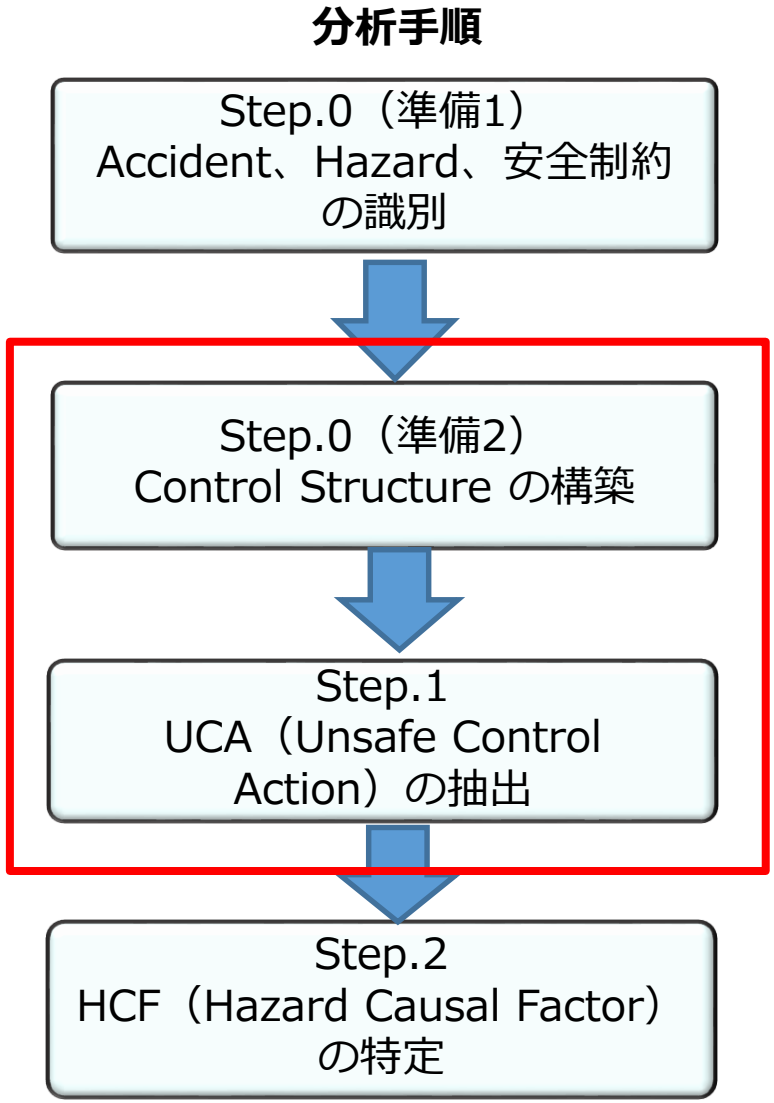


STAMP／STPAの分析手順（「IPA, はじめてのSTAMP/STPA」より）



[出典]IPA, はじめてのSTAMP/STPA（実践編）p.1

STAMP／STPA分析の課題



STAMP/STPAの工程における２つの課題を取り上げ、その解決策を紹介

課題1：複数のControl Actionの分析

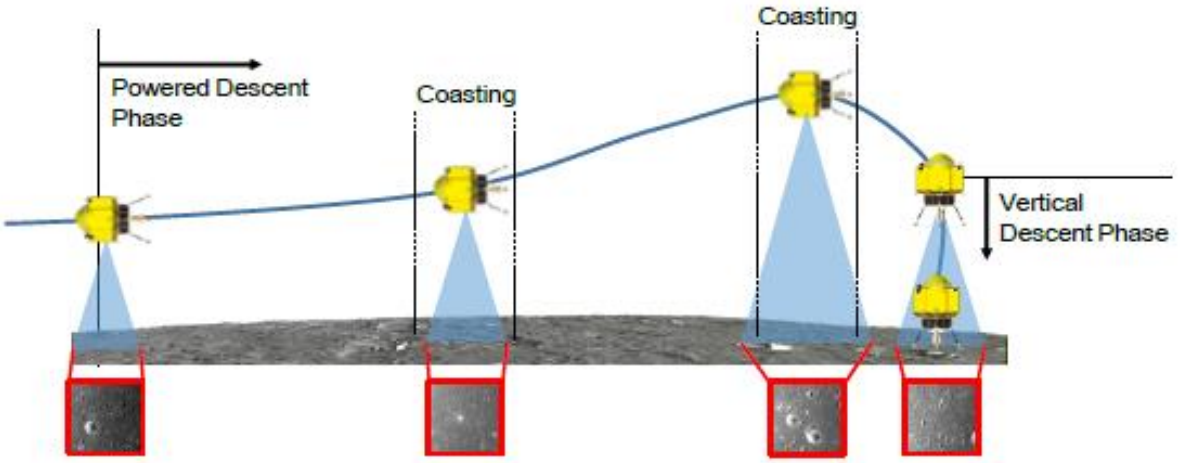
課題2：存在しないControl Actionの識別

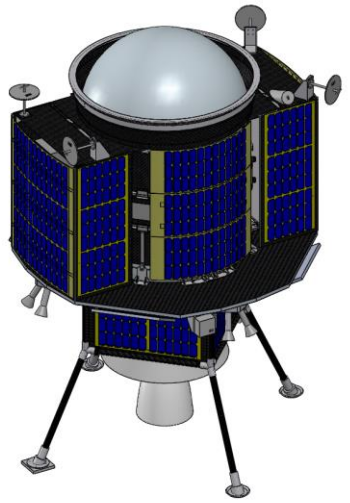
STAMP／STPA分析対象

『第61回宇宙科学技術連合講演会』の発表論文を基に、STAMP／STPA分析を実施した結果の一部を紹介

小型月着陸実証機（SLIM※）：

- 宇宙航空研究開発機構（JAXA）が開発する月面への高精度着陸技術の実証機
- カメラで月面画像を取得し、クレータ情報を抽出
- 抽出したクレータ情報と、月面の地図情報を照合し、高精度に自己位置を推定





©JAXA

[出典]石田貴行 et al. ,クレータを特徴点とした画像照合航法の実装に向けた最適化と精度評価, 2017,日本航空宇宙学会

※SLIM：Smart Lander for Investigating Moon

Step.0 Accident、Hazard、安全制約の識別

SLIMは、高精度な着陸を実施するために自身の位置を正しく推定する必要があることから、STPAの分析対象ハザードとして下記を定義する。

アクシデント：

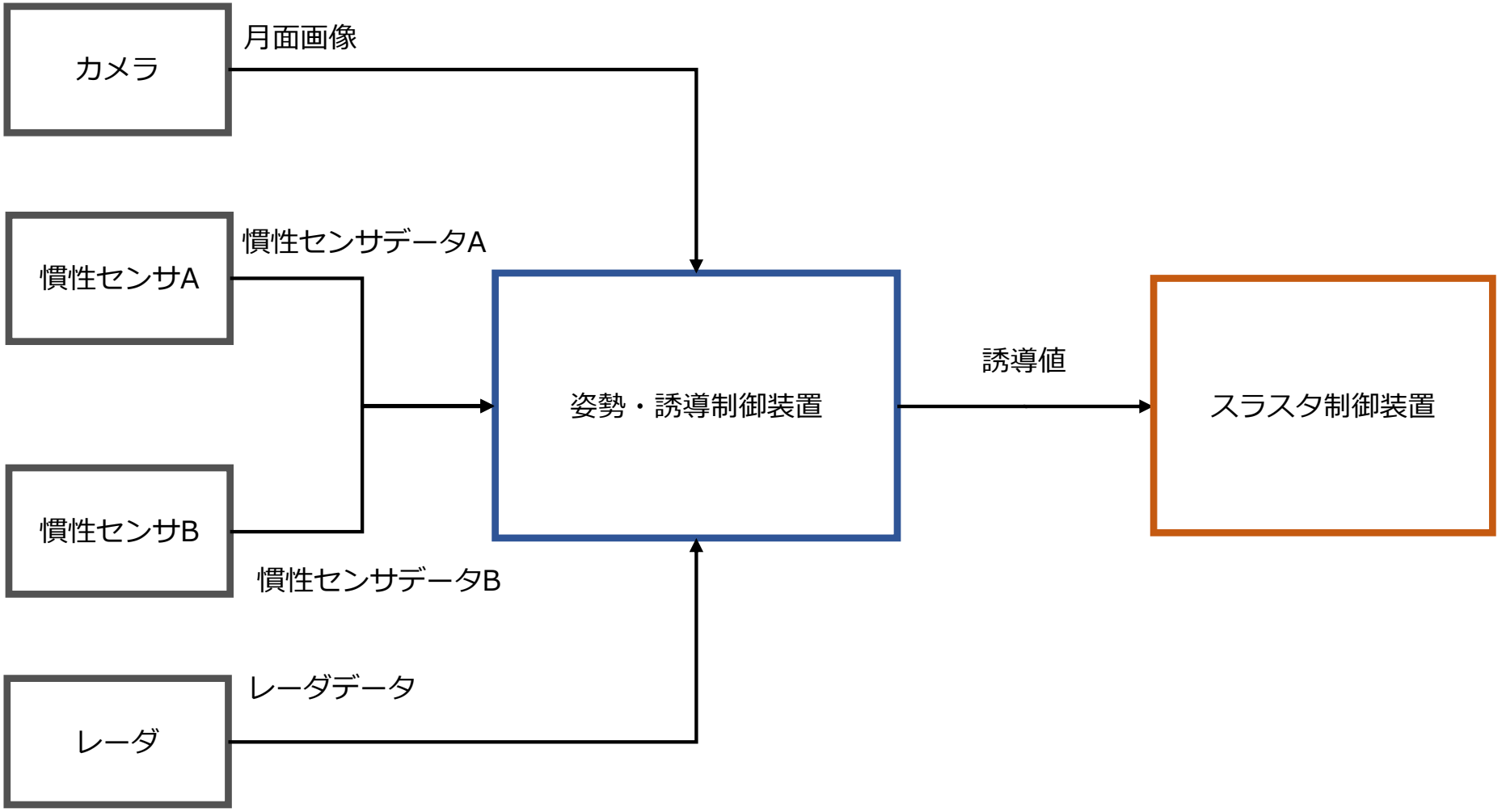
高精度（100mオーダ）の着陸を実施できない。

ハザード：

着陸時に、SLIMが自己位置を正しく推定できない。（H1)

Step.0 Control Structure の構築

コンポーネント間のインタラクションを描いた場合：



Step.1 UCA（Unsafe Control Action）の抽出

非安全なControl Actionの識別：

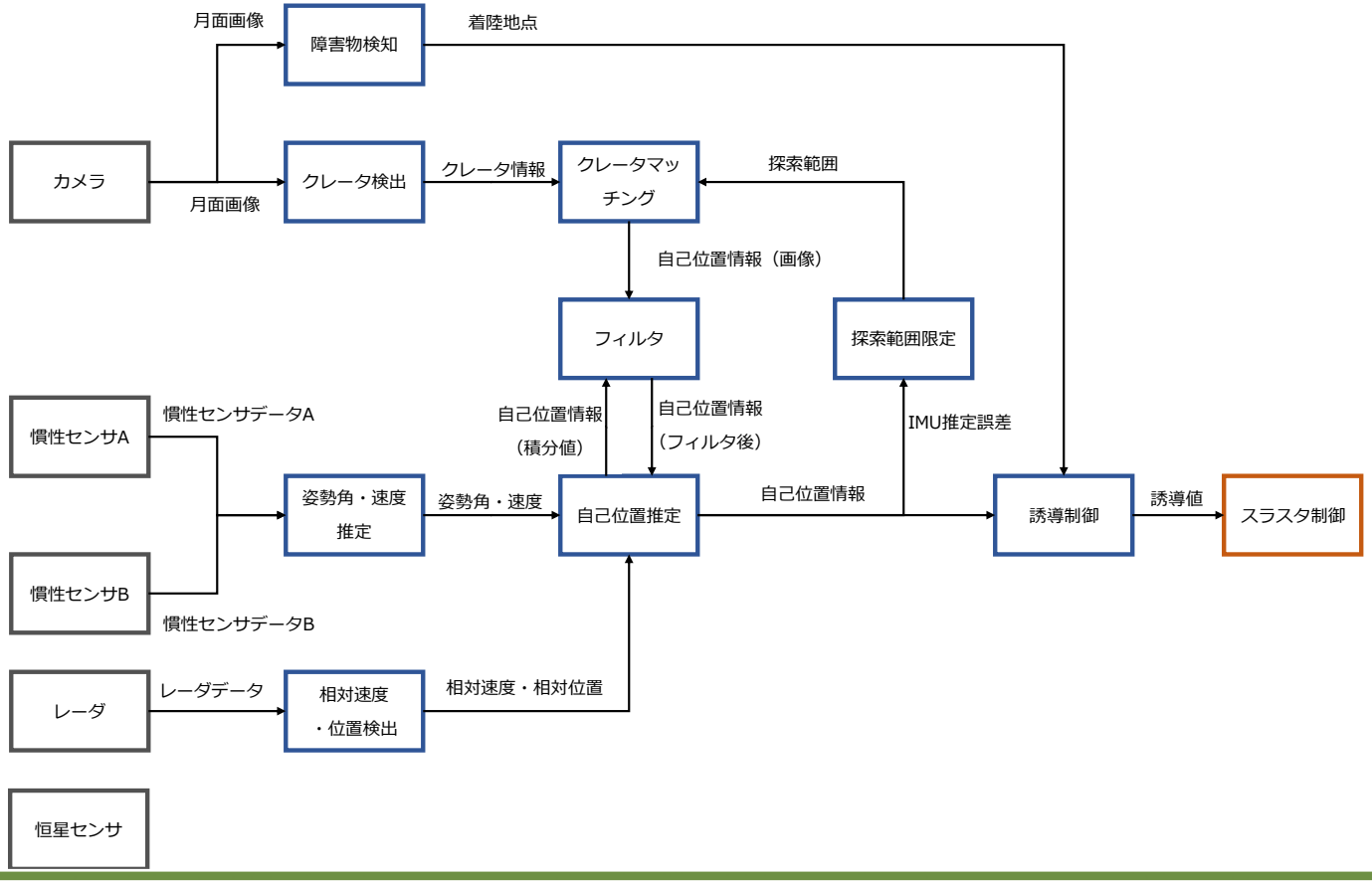
#	CA	From	To	Not Providing	Incorrectly Providing	Too early / Too Late	Stop too soon/Applying too long
1	月面画像	カメラ	姿勢・誘導制御装置	UCA1: 月面画像が無く、高精度の自己位置を算出できない	UCA2： 誤った月面画像により、自己位置を算出し誤る	UCA3： 月面画像の入力が遅くなり、自己位置を算出し誤る	UCA4： 月面画像の入力が停止し、自己位置を算出し誤る
2	慣性センサデータA	慣性センサA	同上	・・・			
3	慣性センサデータB	慣性センサB	同上				

UCAは識別できるが、いずれも抽象度が高く、
この後、UCAの生じる状況・原因を詳細に考えなければならない

姿勢・誘導制御装置の機能の振る舞いを考えなければ
ハザード発生要因の分析は困難

Control Structure の粒度

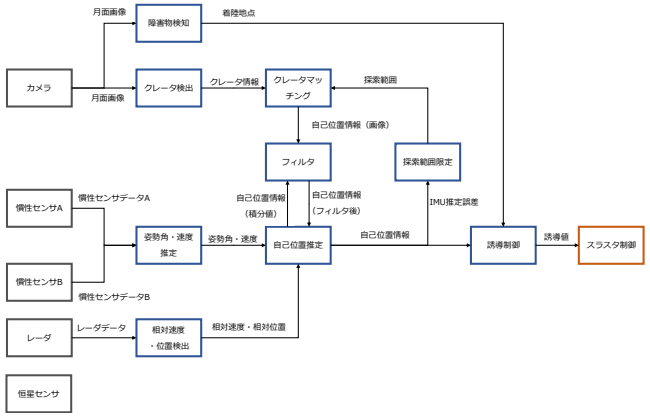
分析すべきハザードは**「SLIMが自己位置を正しく推定できない。」**である。
このハザードの発生要因を分析するためには、**「SLIMが自己位置を推定する構造」**が明確になるように、Control Structureを作成する必要がある。



課題１.
複数のControl Actionの分析
（４つのガイドワード分析の盲点）

課題1. 複数のControl Actionの分析

Step.1において、Unsafe Control Action（UCA）を抽出し、 Control Action毎に4つのガイドワードに沿って、ハザードシナリオを識別する



#	CA	From	To	Not Providing	Incorrectly Providing	Too early / Too Late	Stop too soon/Applying too long
1	月面画像	カメラ	姿勢・誘導制御装置	UCA1: 月面画像が無く、高精度の自己位置を算出できない	UCA2：誤った月面画像により、自己位置を算出し誤る	UCA3：	
2	慣性センサAデータ	慣性センサA	同上	・・・			
3	慣性センサBデータ	慣性センサB	同上				
4	XXX	YYY	ZZZ				
5	XXX	YYY	ZZZ				

識別した全てのControl Action毎に４つのガイドワードを適用してハザードシナリオを識別

実際に分析を行うと、

- Control Actionが多数存在する場合、表を埋めるのは大変な作業
  ⇒作業の目的が表を埋めることになりがちなので注意が必要
- 個別のControl Actionの影響は4つのガイドワードに沿って分析できるが、
  複数のControl Actionの振る舞いはどのように分析すれば良いか？

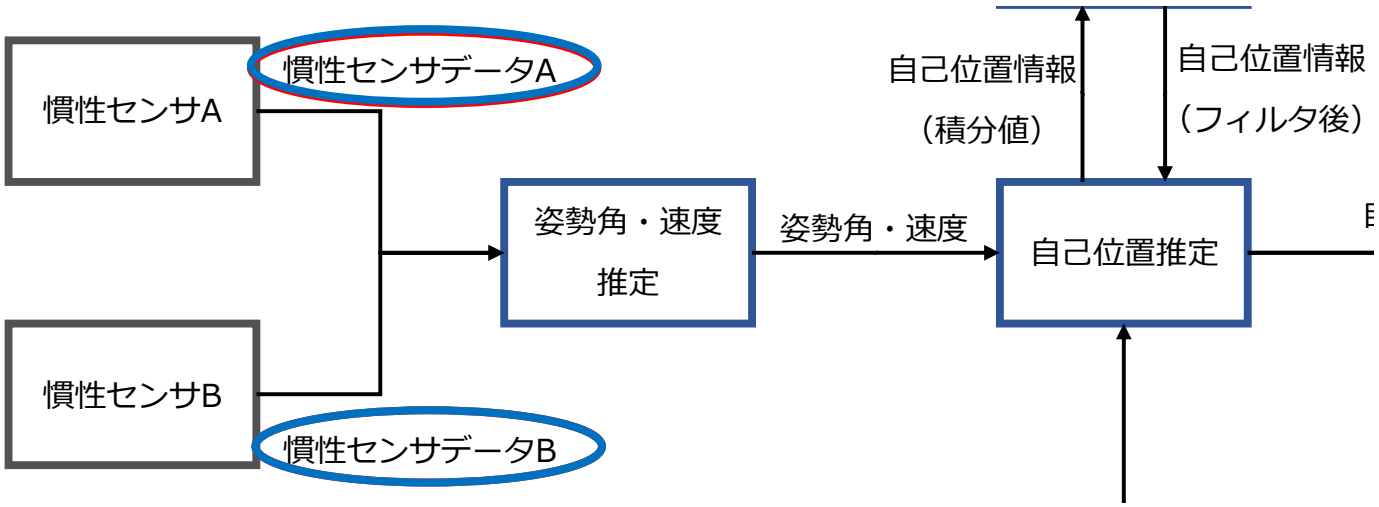
複数のControl Actionの振る舞い

課題1:複数のControl Actionの分析

慣性センサデータAが提供されなくてもハザードには至らない。

慣性センサデータBが提供されなくてもハザードには至らない。

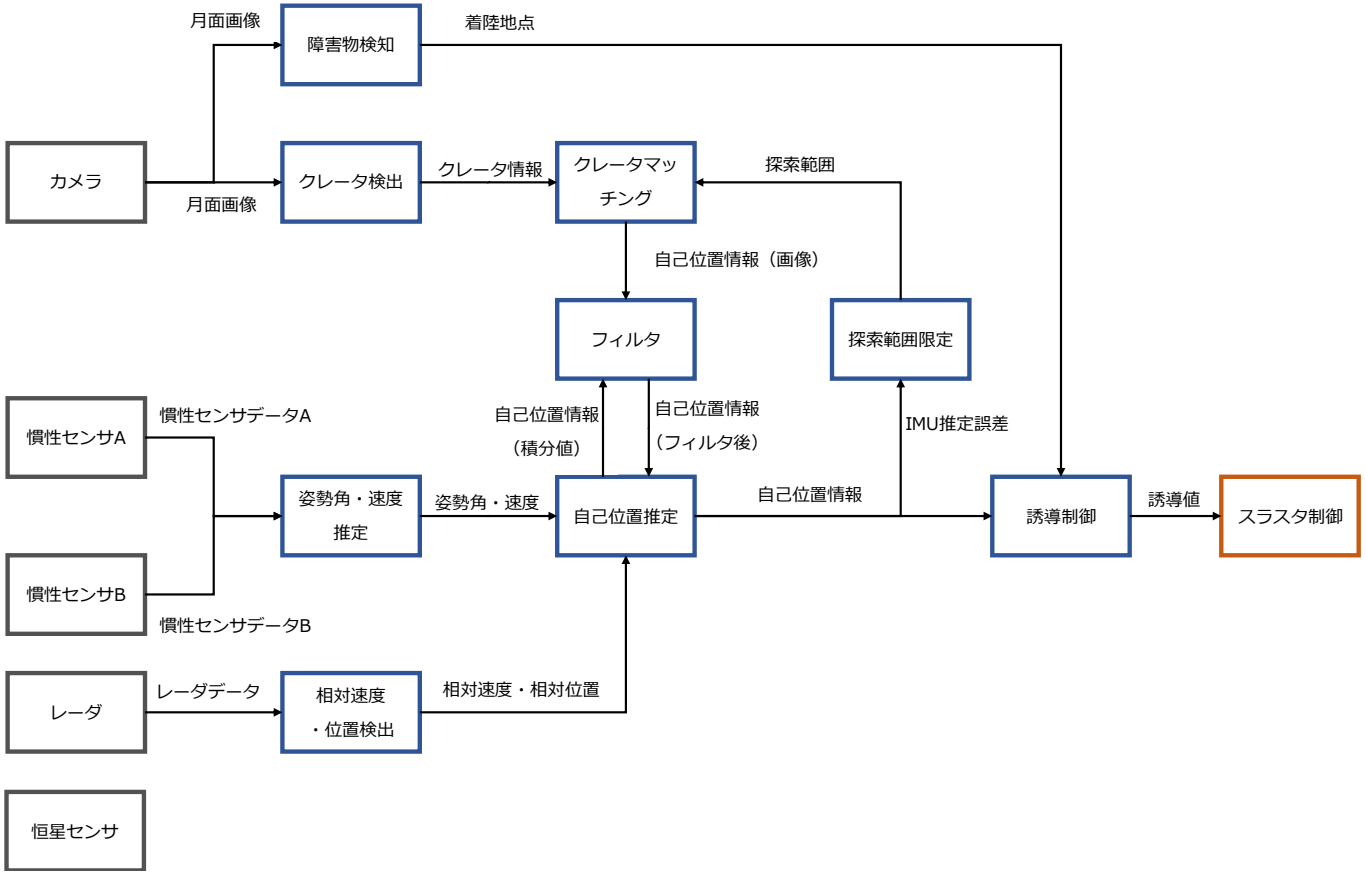
しかし、両方のセンサデータが提供されないと、ハザードに至る。



複数のControl Actionの振る舞いを考えなければ
識別できないハザード発生要因が存在

複数のControl Actionの分析方法

では、どのようにして複数のControl Actionの振る舞いを分析すれば良いか。



多数のCAをどのように組み合わせて考えれば良いか

複数のControl Actionの分析方法

対策案：

複数のControl Actionの組み合わせを考慮したマトリクスを用いて分析する。

検討結果：

例えば、Control Actionが5個ある場合、

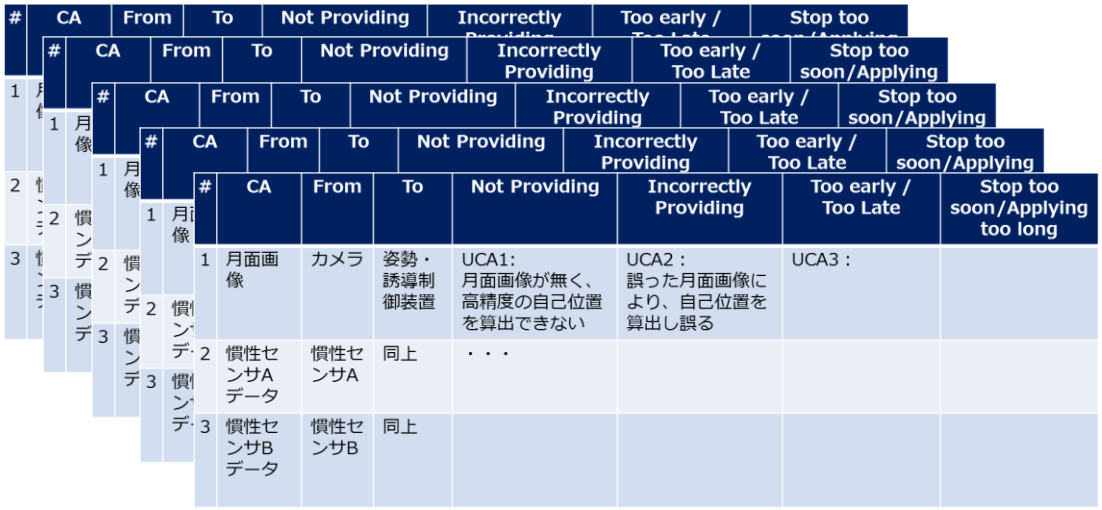
その組み合わせは、

AB,ABC,ABCD,ABCDE

AC,ACD,ACDE

・・・

・・・



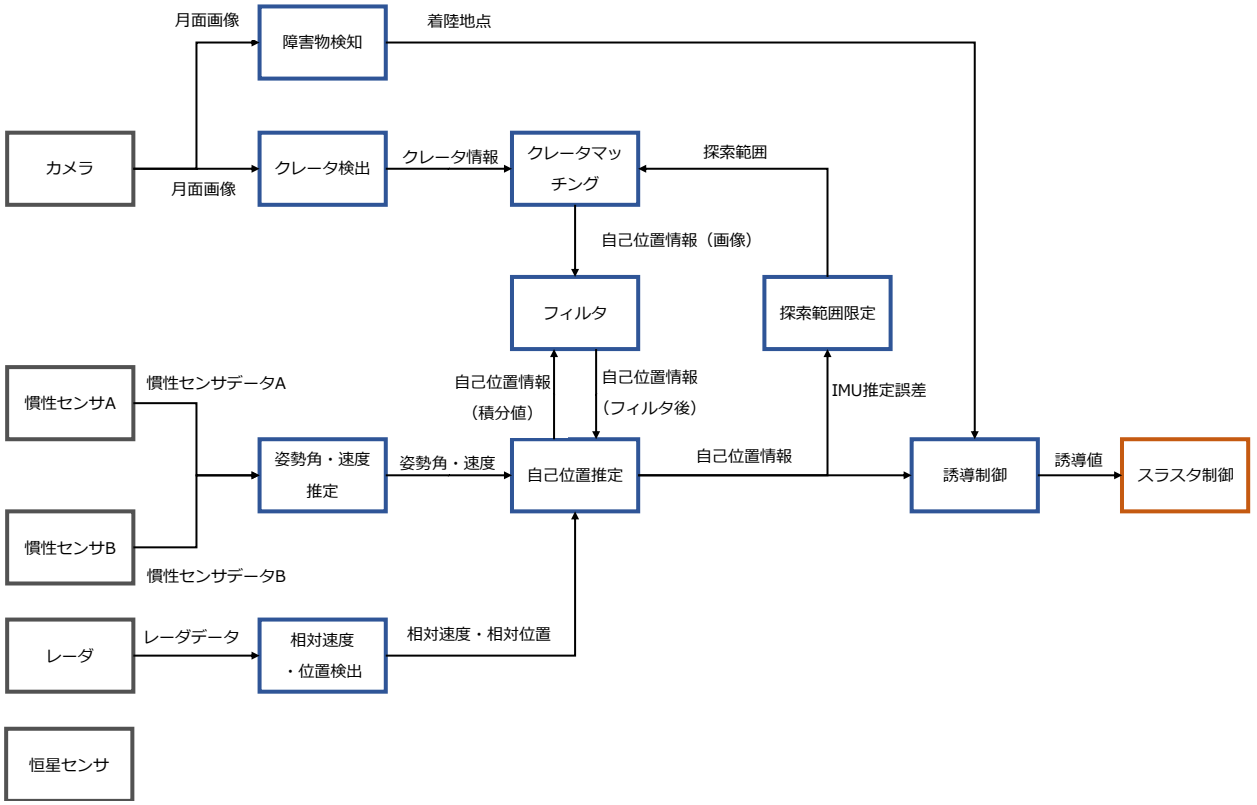
#	CA	From	To	Not Providing	Incorrectly Providing	Too early / Too Late	Stop too soon/Applying too long
1	月面画像	カメラ	姿勢・誘導制御装置	UCA1: 月面画像が無く、高精度の自己位置を算出できない	UCA2：誤った月面画像により、自己位置を算出し誤る	UCA3：	
2	慣性センサAデータ	慣性センサA	同上	・・・			
3	慣性センサBデータ	慣性センサB	同上				

マトリクスを用いて機械的に分析することは現実的に困難

複数のControl Actionの分析方法

分析すべきハザードは**「SLIMが自己位置を正しく推定できない」**である。

Step.1の分析すべきCAを考える段階では、負の要因を意識し過ぎず、**「何故、 SLIMが100mオーダの高精度な自己位置推定ができるのか」**といった、システムが成功している特徴を的確に捉えることが重要。



構造解析の着眼点

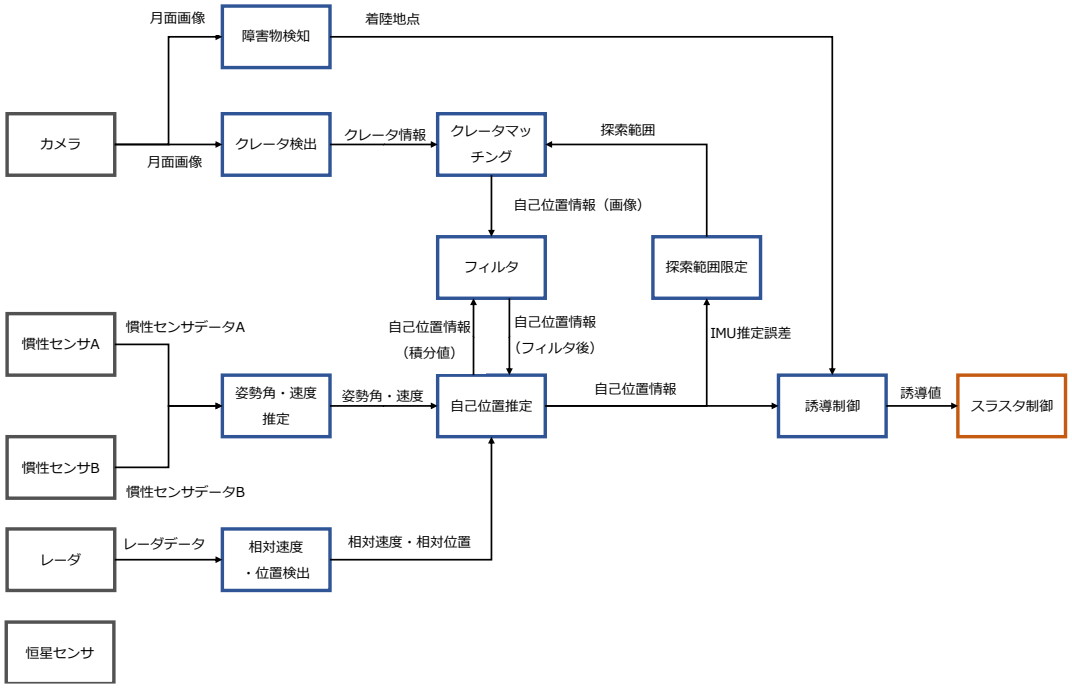
着眼点：

・安全制約を満たすための特徴は？
　⇒100mオーダの精度を出すために実施
　　していることは？

・新規性の高いインタラクションは？

・故障／異常発生時にどのように対応
　しているか？

・Control Structure上、特徴的なControl
　Actionのインタラクションはあるか？



システムの成功要因と構造の特徴に着目

例1：構造解析によるハザードシナリオ識別

特徴：

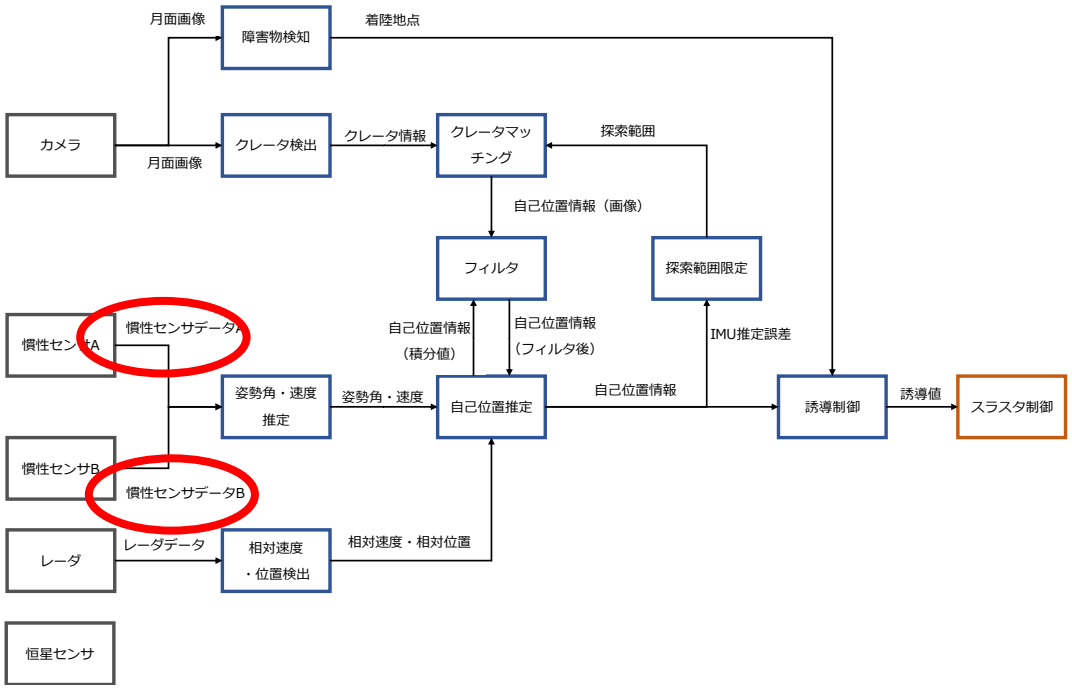
姿勢角・速度推定機能は、同種の２つのデータを入力している。

成功要因：

慣性センサAと慣性センサBの冗長構成により、片方のセンサが故障しても、ミッションを継続可能

ハザードシナリオ：

慣性センサAからBに切り替わった時、自己位置推定の結果が大きく変わり、自己位置を正しく推定できなくなる



システムを成功させるために実施していることに着目

例2：構造解析によるハザードシナリオ識別

特徴：

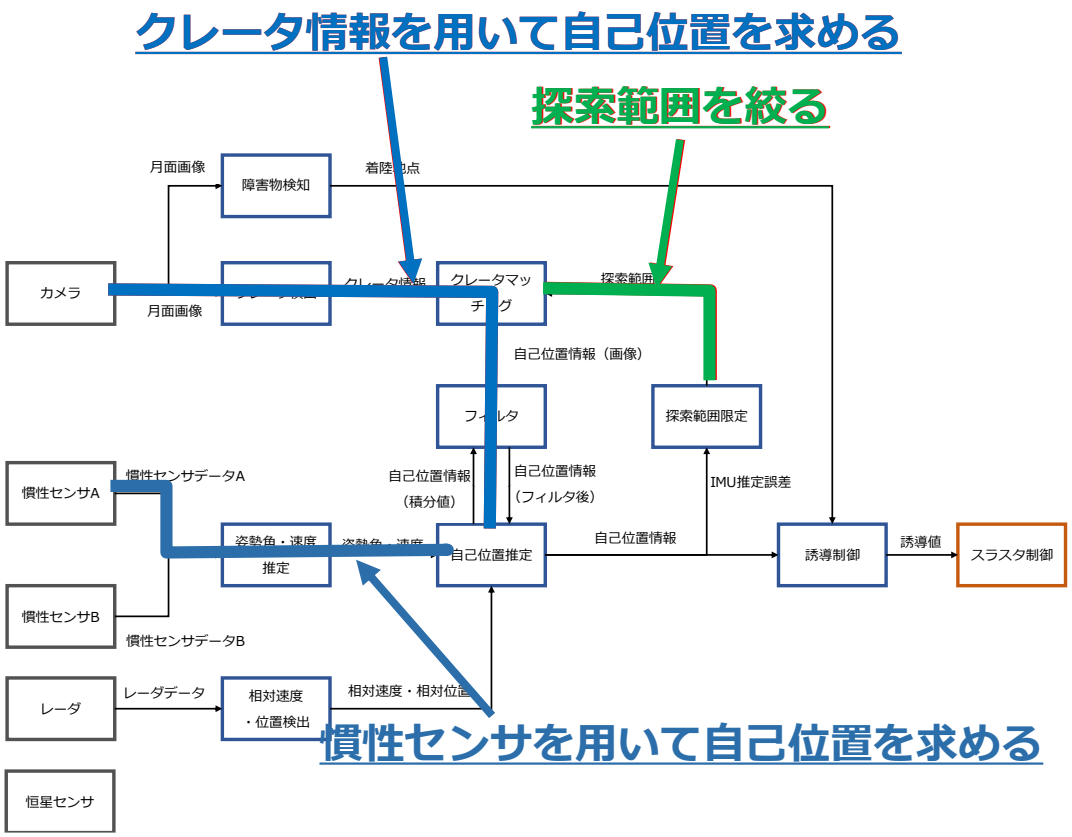
SLIMはクレータ情報と慣性センサ情報から自己位置を推定する

成功要因：

SLIMはクレータの**探索範囲を絞る**ことで、計算時間を削減し、効率的に自己位置を求めている。

ハザードシナリオ：

探索範囲を絞り過ぎた場合、クレータマッチングを行うことができず、自己位置を正しく推定できなくなる



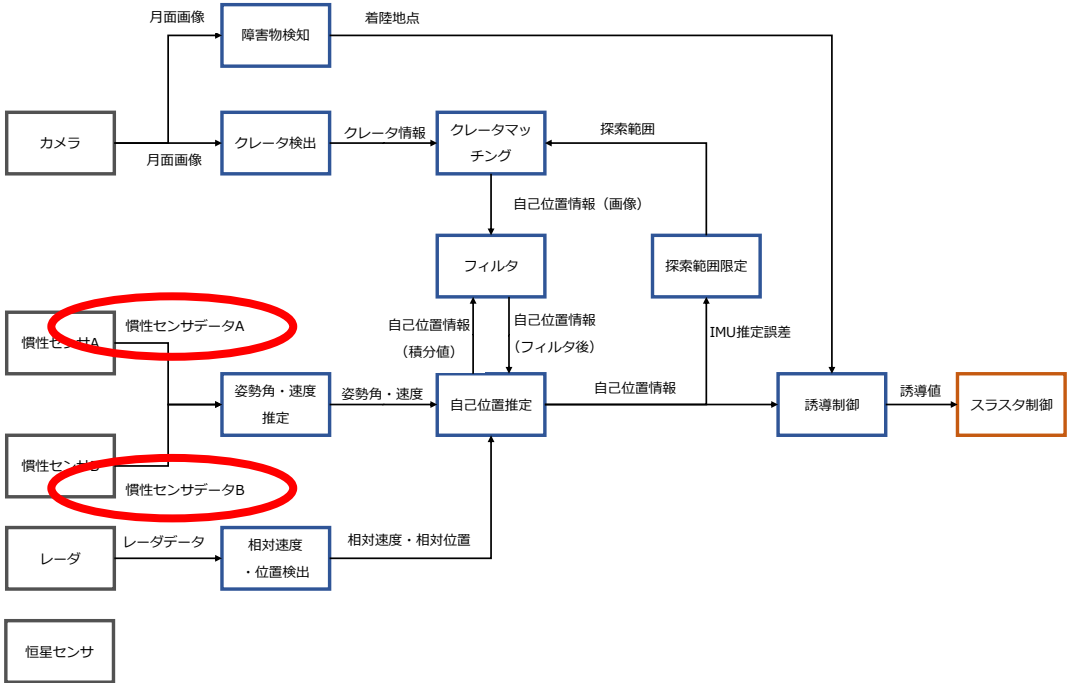
探索範囲の絞り方次第でハザードに至る可能性が生じる

４つのガイドワード分析だけでなく、Control Structure全体を俯瞰して関連するControl Actionの影響を分析することが必要

Step.1で実施すべき分析

特徴の識別には様々な着眼点がある。例えば、今回は複数のControl Actionが機能に入力されているところを識別した。

他にもControl Actionの振る舞いの特徴をよく捉えることが肝要となる。



４つのガイドワード分析　＋　構造解析による複数CAの分析

課題2.
存在しないControl Actionの識別

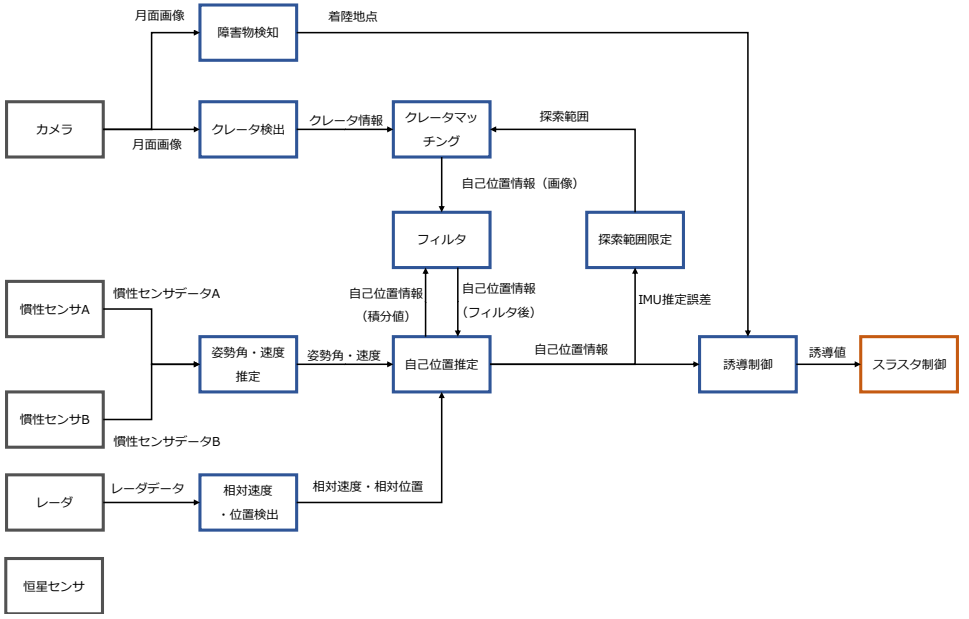
課題2. 存在しないControl Actionの識別

ここまでの分析において、
単一のControl Actionと、複数のControl Actionを分析し、ハザード発生要因を特定した。
しかし、自動制御システムの場合、他にもハザード発生要因が潜在していることがある

単一のControl Actionの分析

#	CA	From	To	Not Providing	Incorrectly Providing	Too early / Too Late	Stop too soon/Applying too long
1	月面画像	カメラ	姿勢・誘導制御装置	UCA1: 月面画像が無く、高精度の自己位置を算出できない	UCA2： 誤った月面画像により、自己位置を算出し誤る	UCA3：	
2	慣性センサAデータ	慣性センサA	同上	・・・			
3	慣性センサBデータ	慣性センサB	同上				

複数のControl Actionの分析



課題2. 存在しないControl Actionの識別

Step.1のNot Providingの分析では、
Control Actionが提供されない場合に、ハザードに至るシナリオを分析するが、
Control Actionというデータが実在していなければ分析することはできない

#	CA	From	To	Not Providing	Incorrectly Providing	Too early / Too Late	Stop too soon/Applying too long
1	月面画像	カメラ	姿勢・誘導制御装置	UCA1: 月面画像が無く、高精度の自己位置を算出できない	UCA2： 誤った月面画像により、自己位置を算出し誤る	UCA3：	
2	慣性センサAデータ	慣性センサA	同上	・・・			
3	慣性センサBデータ	慣性センサB	同上				

Control Actionが存在しないためハザードに至るシナリオは分析できない

例3：構造解析によるハザードシナリオ識別

特徴：

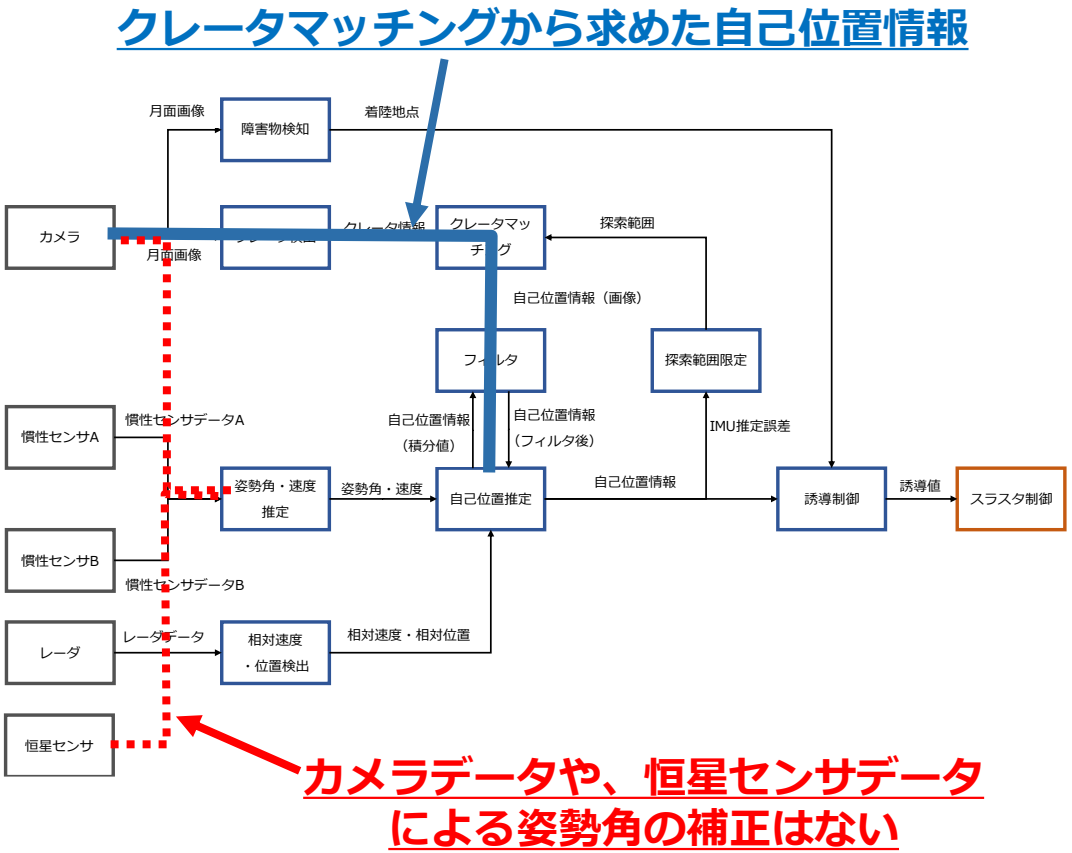
クレータマッチングを行うためには、正しい姿勢で月面を撮像したデータが必要

構造解析：

- クレータマッチングから求めた自己位置情報を補正することができる
- 慣性センサデータには誤差が生じるが、姿勢角を補正するControl Actionは存在していない

ハザードシナリオ：

姿勢角の誤差が大きくなると、月面を正しく撮像できずにクレータマッチングの精度が低下し、自己位置を推定できなくなる



構造解析から、補正を行う機能／行わない機能が明確になる

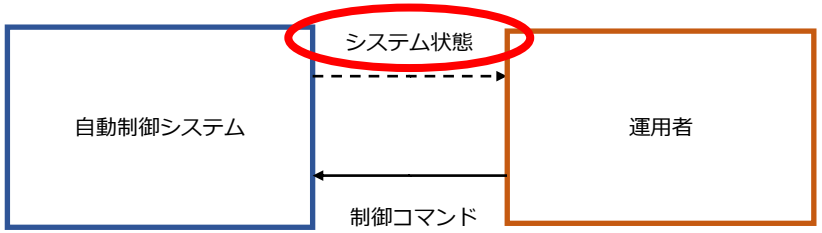
自動制御システムと人との間のインタラクション

自動制御システムと人との間のインタラクションにControl Actionが存在しないことから、問題が発生するケースが散見される。

例えば、航空機の自動化に伴う事故は、主に状況認識（situation awareness）の失敗が原因で発生している。M.R.Endsleyらは、この状況認識には３つのレベルがあると整理しているが、大半は、レベル１が満たされないことにより、事故に至っていると言われている。

・レベル１：何かが起こっていることに気づく
・レベル２：その原因を特定できる
・レベル３：これからの事態の推移が予測できる

よく訓練されたパイロットですら、
何が起こったのかが分からなかったことが、原因の大半を占める



人に対して適切なインタラクション（Control Action）がそもそも存在しないことが問題

自動制御システムと人との間のインタラクション

自動制御システムと人との間では、そもそもControl Actionが無いことがハザードの発生要因になっていることがある。

「システム状態」というCAが存在すれば、そのCAが提供されない時の分析は、既存のガイドワードを用いた分析で識別できる

#	CA	From	To	Not Providing
1	制御コマンド	運用者	自動制御システム	・・・
2	システム状態	自動制御システム	運用者	・・・

「システム状態」というCAがそもそも存在しない場合、ハザードシナリオを識別することはできない。

これらを回避するためには、システムの構造をよく理解し、かつ、運用者が必要とするインタラクションを考えなければならない。

自動制御システムでは、
システムの構造から特徴を把握し、運用者とのインタラクションの明確化が必要

まとめ

- 自動制御システムを分析する際には、システムの振る舞いが明確になる粒度でControl Structureを描くことが重要
- システムの構造を解析し、特徴を捉えて複数のControl Actionの振る舞いを考えることが必要
- 人が介入する自動制御システムの場合、自動制御システムの振る舞いを明確化し、人にとってどのようなインタラクションが必要となるのかを考えることが重要（Control Actionの抜けを防止）