自動制御システムの安全性解析の最新手法 - FRAMの基礎と適用方法 -

2017年12月13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

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になるだけでなく、システムが自動制御されるという特徴がある。そのような、自動制御システムに対して、どうすれば安全を確保できるか、その一つの考え方を紹介する。

©JAXA

目次

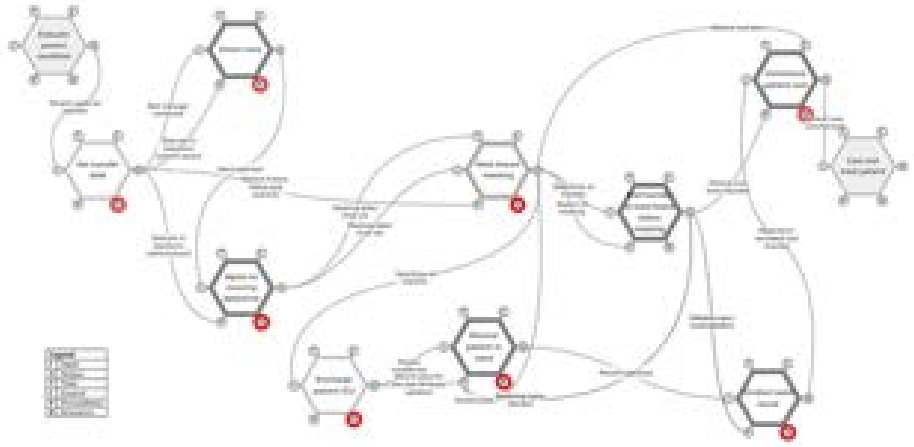
１．FRAMとは
２．FRAMの考え方
　- 宇宙機（人工衛星）の例 -
　- 鉄道（踏切制御論理）の例 –
３．まとめ
４．自動制御システムの課題

1. FRAMとは

FRAM

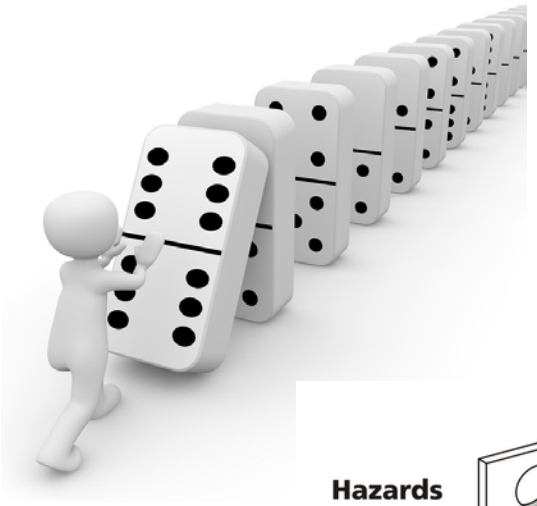
FRAM（*Functional Resonance Analysis Method:*機能共鳴分析手法）：

・南デンマーク大学のホルナゲル教授が提唱した安全解析手法
・事故は、失敗や不全ではなく、成功からも発生すると提唱



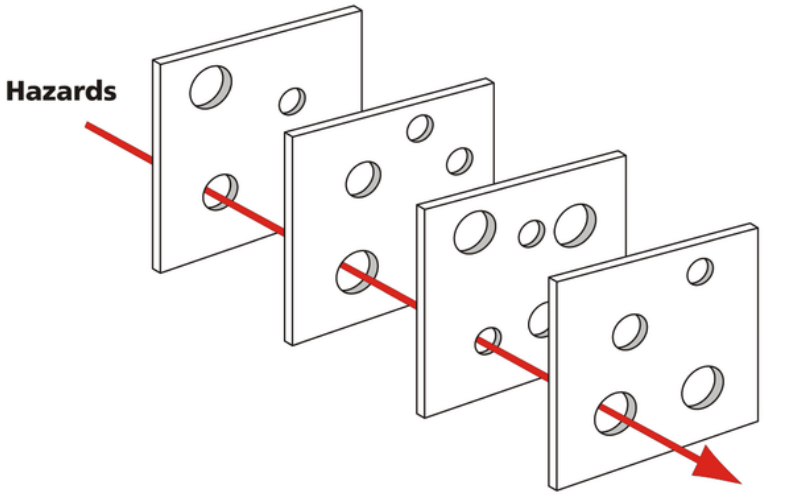
事故モデルの変遷

ドミノモデル：
単一の根本原因から
事故は生まれる



(※1)

スイスチーズモデル：
いくつかのレイヤー、コンポーネントの
異常の組合せから事故は生まれる



(※2)

悪い原因から悪い結果が生まれると定義する安全工学

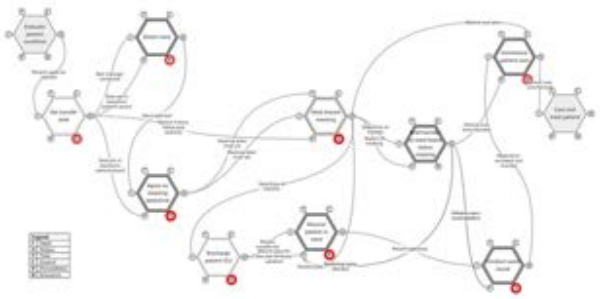
[出典](※1)pixabay, https://pixabay.com/de/mikado-domino-steine-zahlen-1013878/
(※2)Davidmack, https://commons.wikimedia.org/wiki/File:Swiss_cheese_model_of_accident_causation.png

事故モデルの変遷

FRAMモデル（機能共鳴モデル）：

・システムが大規模・複雑になると、複数の機能のインタラクションから、成功と失敗が生まれる

・FRAMにおける安全分析とは、複数の機能が互いにどのようにインタラクションするのかを明らかにし、その関係性の中に安全に係わるシステムの長所や短所を見出す



成功からも悪い結果が生まれると定義する安全工学

Safety-I と Safety-II

Safety-I

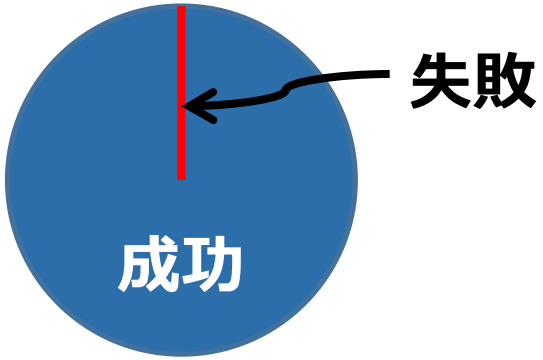
・悪い原因から悪い結果が生まれると定義する安全工学

・なぜ失敗するのかを分析してリスクを識別

Safety-II

・良い原因（成功）からも悪い結果が生まれると定義する安全工学

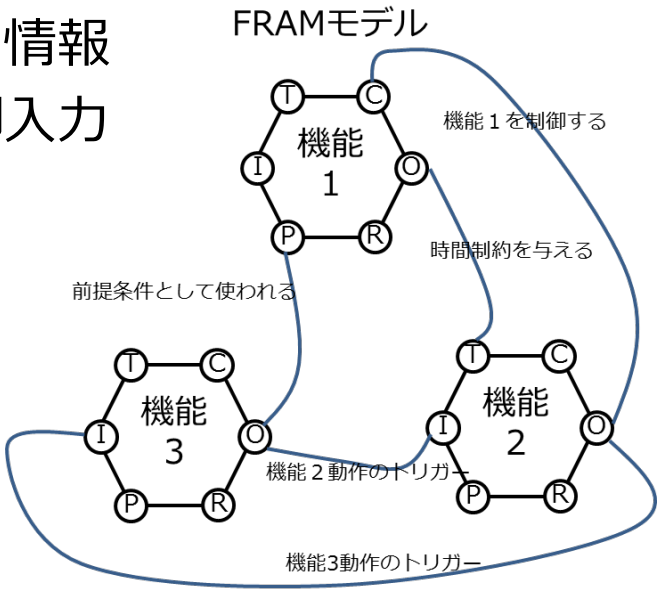
・なぜ成功するのかを分析してリスクを識別



FRAMモデルの作成

各機能を、以下の６つの要素（5入力＋1出力）で定義し、
FRAMモデルを作成する。

- I　Input　　機能の開始条件となる入力
- P　Precondition　機能の開始の前提条件となる入力
- R　Resource　　機能の実施に必要な資源となる入力
- T　Time　　機能の実施の制約となる時間情報
- C　Control　　機能の実施方法を変える制御入力
- O　Output　　機能の出力



2. FRAMの考え方
- 宇宙機（人工衛星） -

X線天文衛星ASTRO-H「ひとみ」

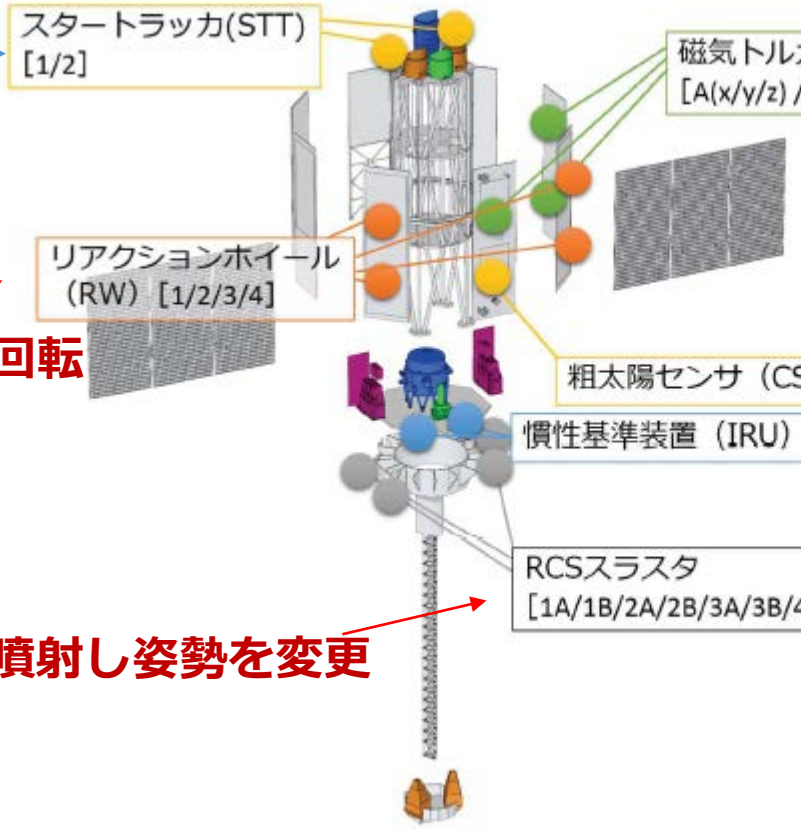
『X線天文衛星ASTRO-H「ひとみ」』にFRAMの考え方を適用

X線天文衛星ASTRO-H軌道上外観図

[出典]
国立研究開発法人 宇宙航空研究開発機構（JAXA),
『X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書 p.6』, 2016.6.14,
http://www.jaxa.jp/press/2016/06/20160614_hitomi_j.html

ASTRO-H 姿勢制御系機器

青字：センサー
赤字：アクチュエータ



姿勢角を取得

衛星内のコイルに電流を流し、磁気を発生させ、角加速度を与える

衛星内のホイールを回転させ、姿勢を変更

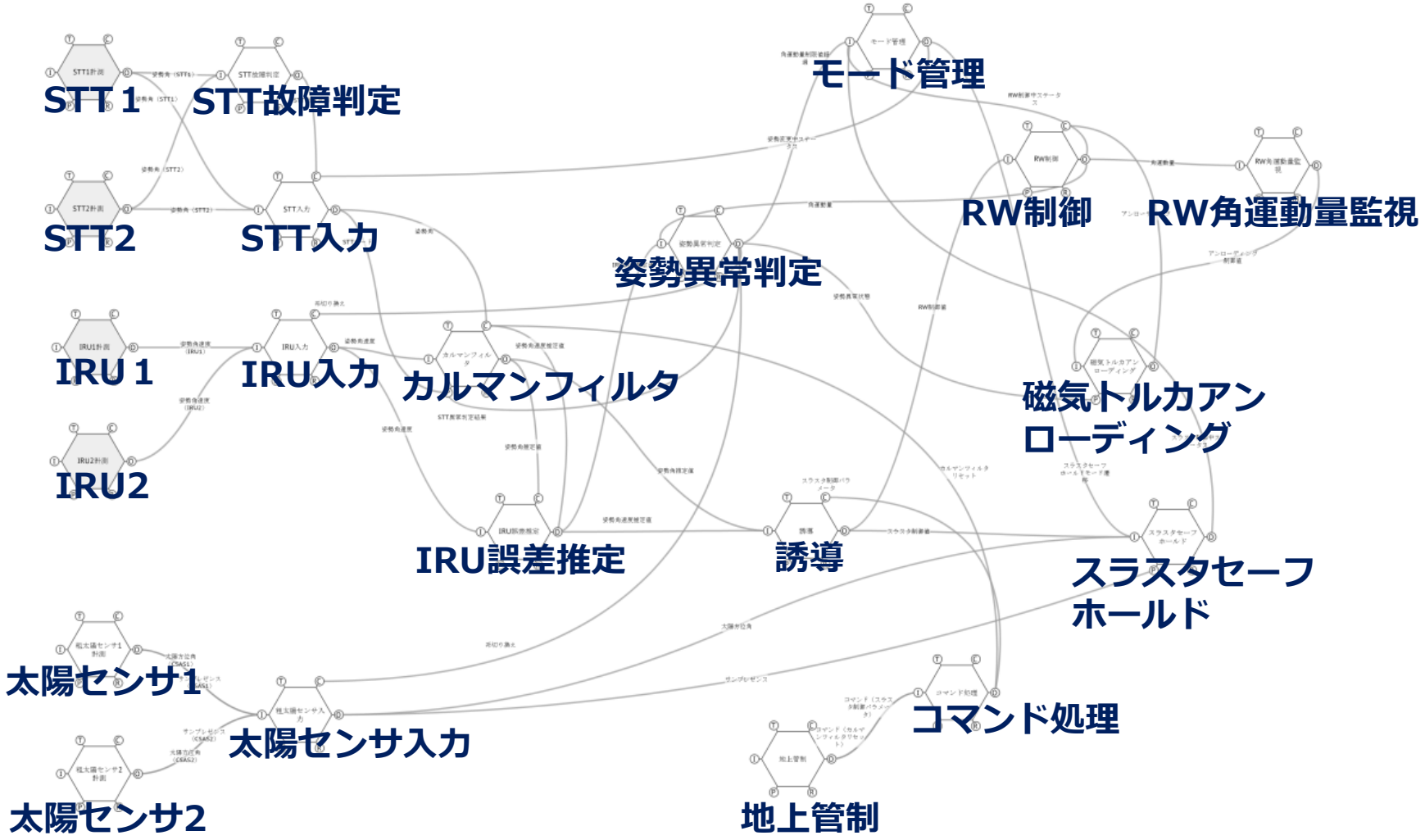
太陽の位置を取得し、現在姿勢を推定

推薬を噴射し姿勢を変更

姿勢角速度を取得

[出典]
国立研究開発法人 宇宙航空研究開発機構（JAXA),
『X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書 p.11』, 2016.6.14,
http://www.jaxa.jp/press/2016/06/20160614_hitomi_j.html

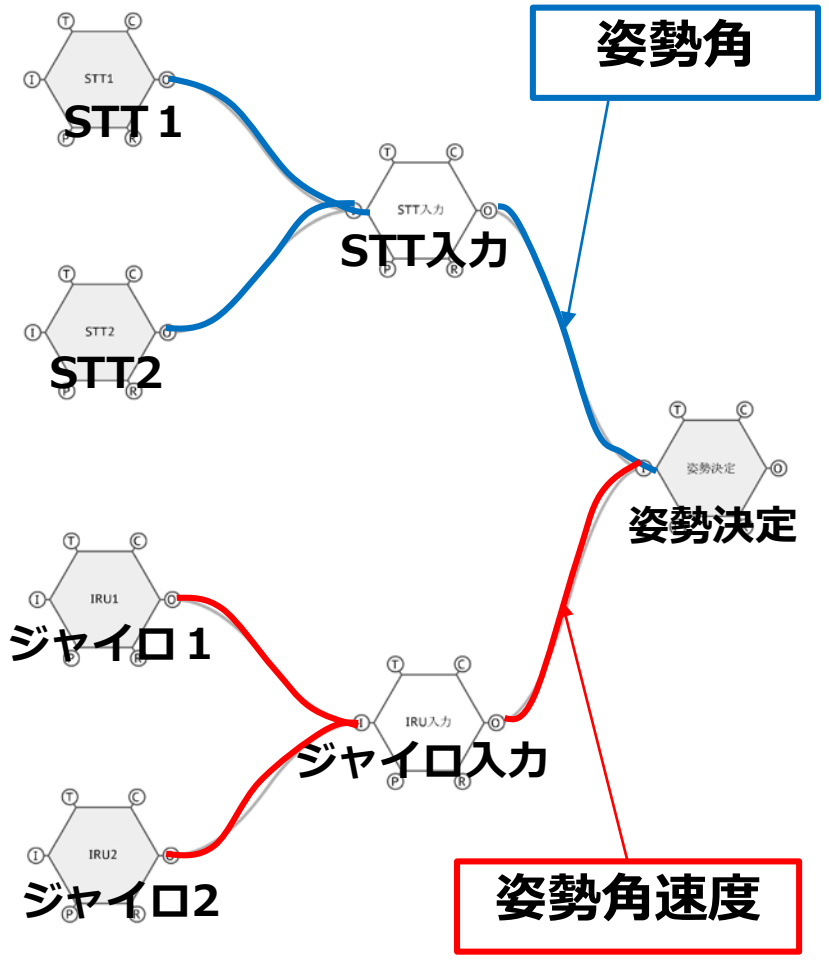
FRAMモデル



特徴

特徴：

- 衛星の姿勢を取得するセンサにスタートラッカー(STT)を使用
- STTは、星の位置を元に衛星の姿勢を高精度に把握
- STTを使用できない時は、IRU（ジャイロ）から得た角速度を時間積分

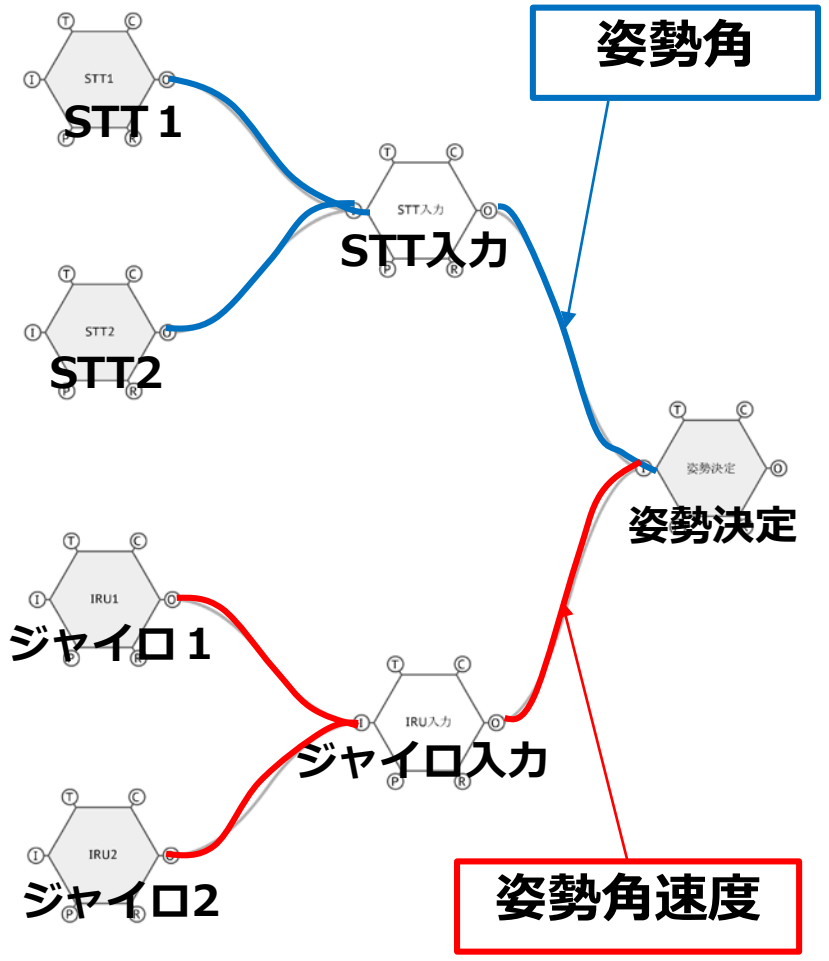


成功要因

成功要因：

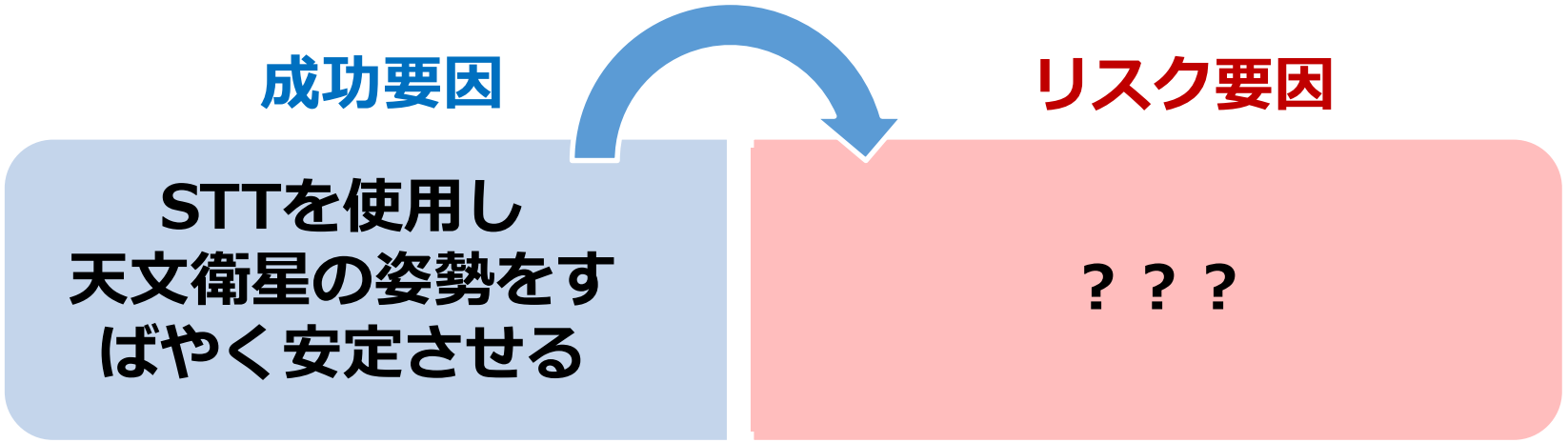
- STTの値は常に高精度、ジャイロの値は誤差を含む
- STTの方が性能が高いため、なるべくSTTの値を使用して、高度な姿勢制御を実現

天文衛星では、高度な姿勢制御が必要となるため、可能な限りSTTのデータを使用



成功からリスクを考える

成功からリスクを考える：



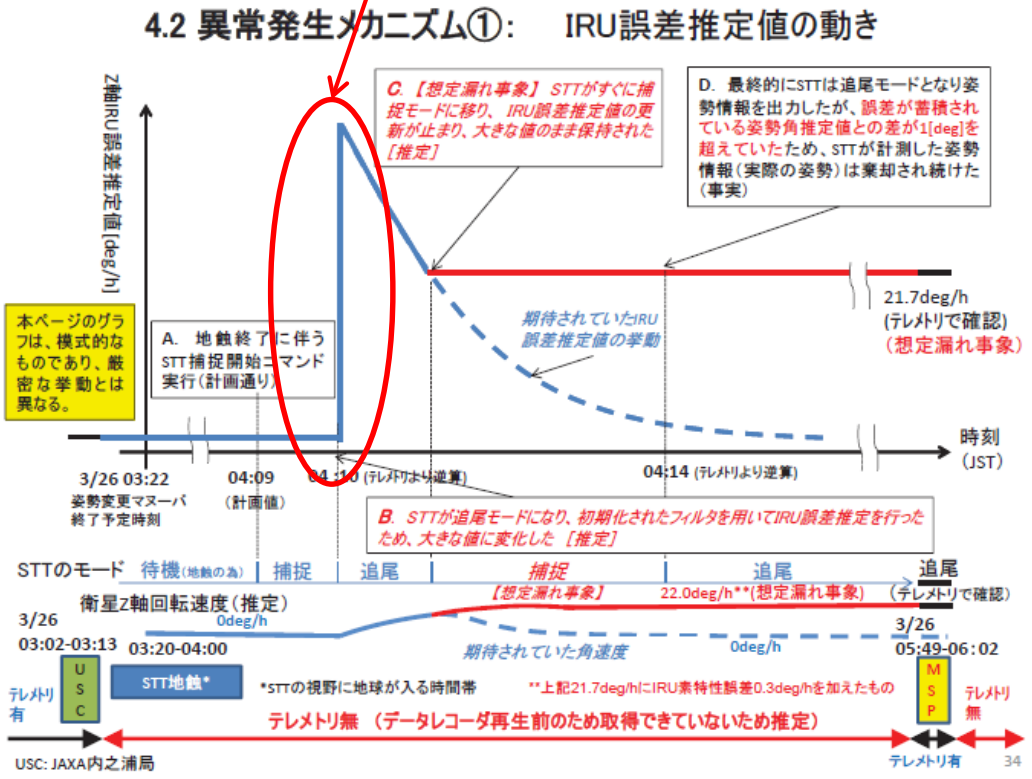
成功からどのようなリスクが考えられるか

リスク要因

リスク要因：

- STTを使用できない時はジャイロを使用する
- ジャイロから、STTにセンサーが切り替わったとき、精度の差があるため、衛星の姿勢が急激に変化する

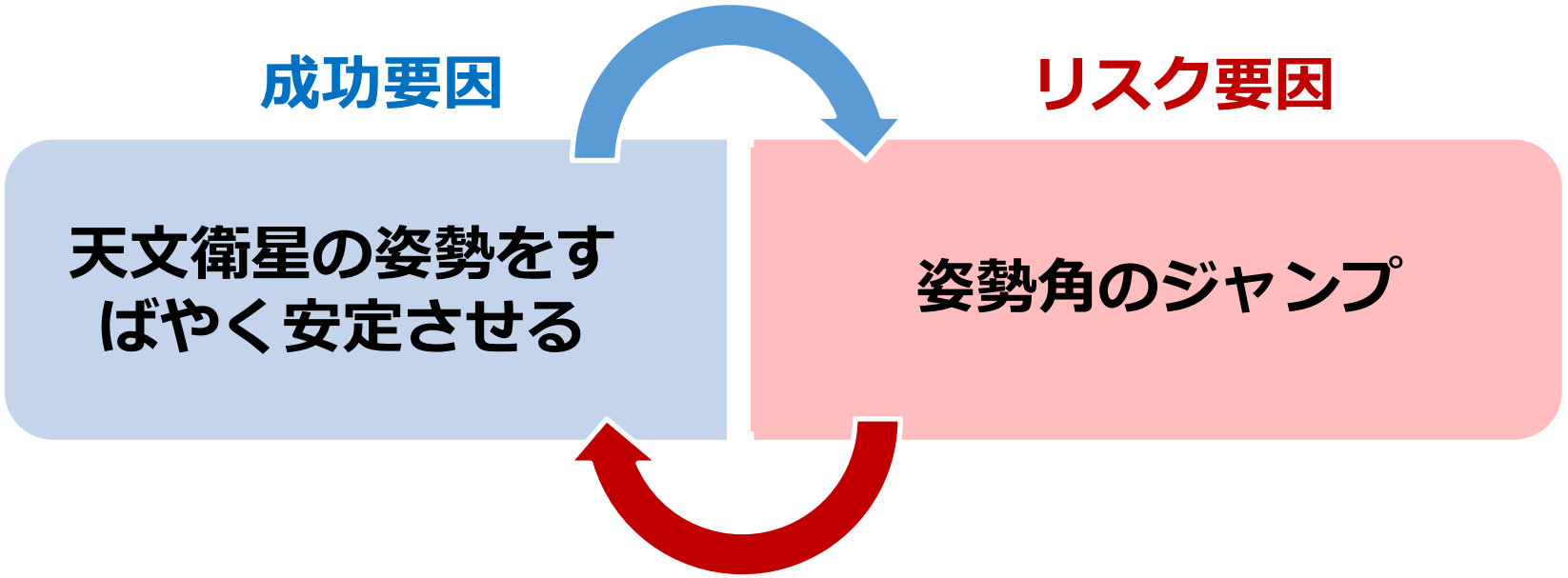
ジャイロからSTTに切り替わった時
衛星の姿勢が急激にジャンプする



[出典]X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書
P.34（4.2）異常発生メカニズム①：IRU誤差推定値の動き

成功からリスクを考える

成功からリスクを考える：

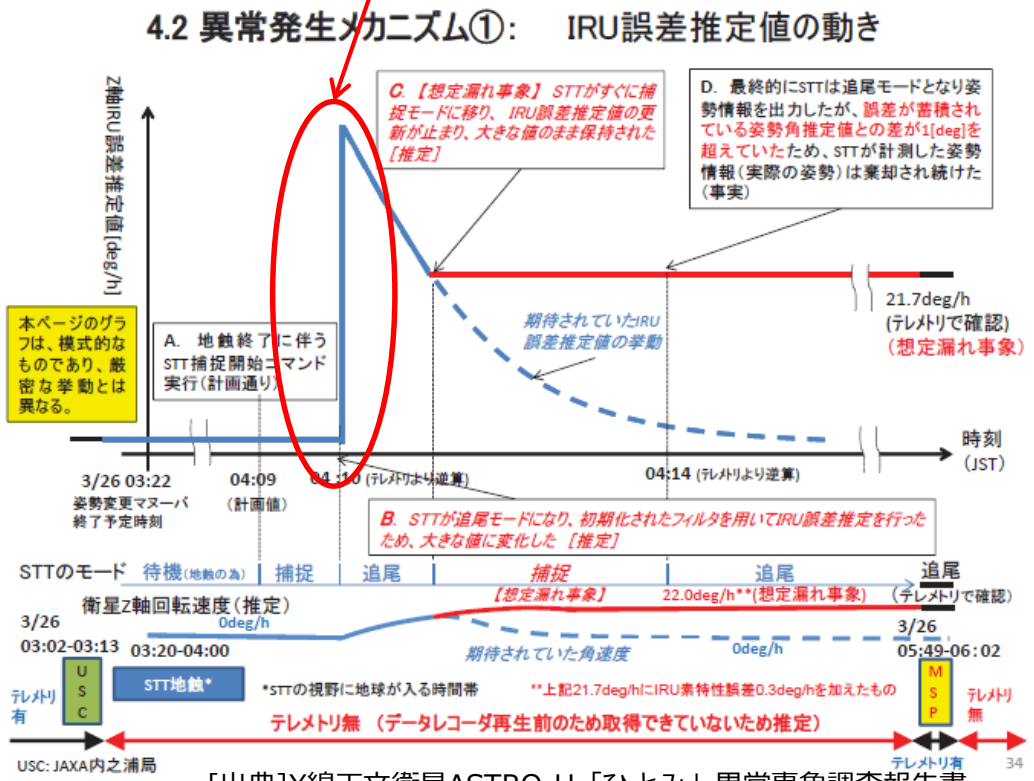


成功の裏返しにリスクが潜在

対策

姿勢角がジャンプしたことにより、衛星は正しい姿勢制御ができなくなった。

衛星の姿勢角が急激にジャンプした直後の値は使用しない



[出典]X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書
P.34（4.2）異常発生メカニズム①：IRU誤差推定値の動き

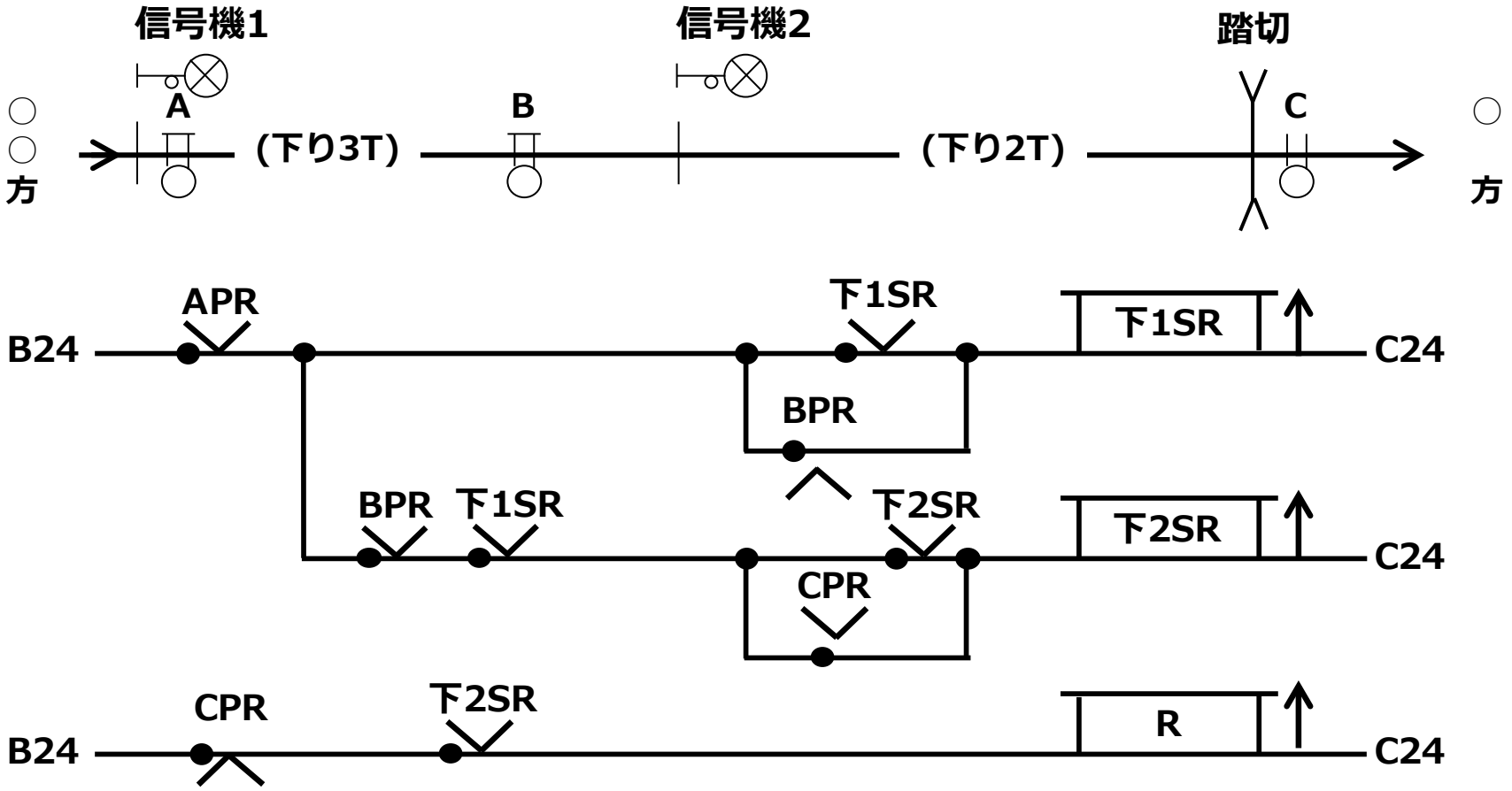
<u>対策：</u>

姿勢角がジャンプしないように、STTの値を緩やかに取り込む

2．FRAMの考え方
- 鉄道（踏切制御論理） -

踏切制御論理

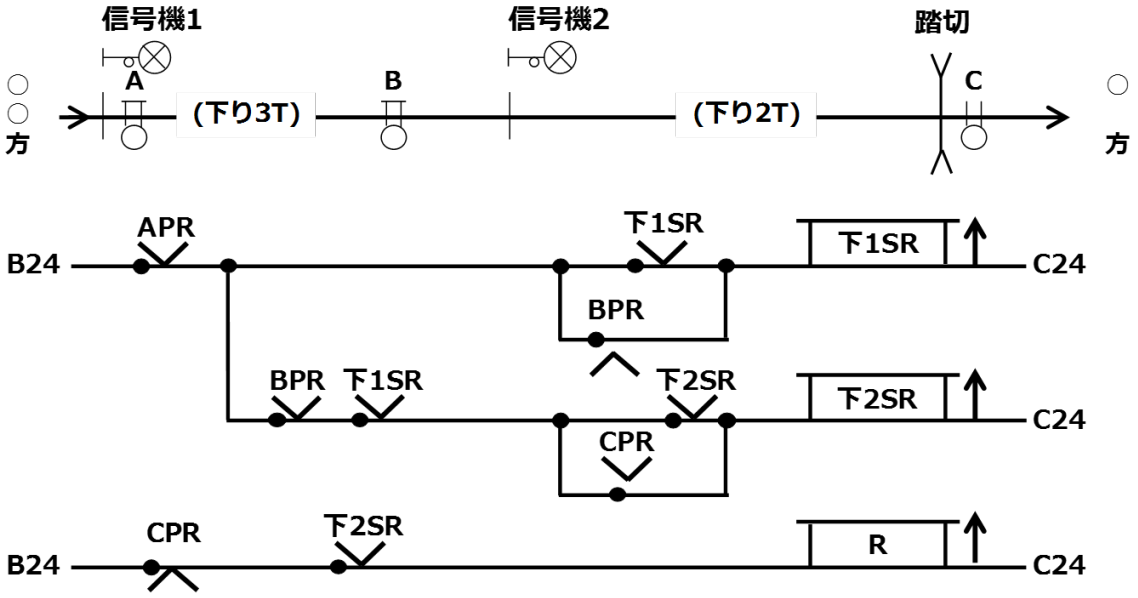
踏切制御論理にFRAMを適用して分析



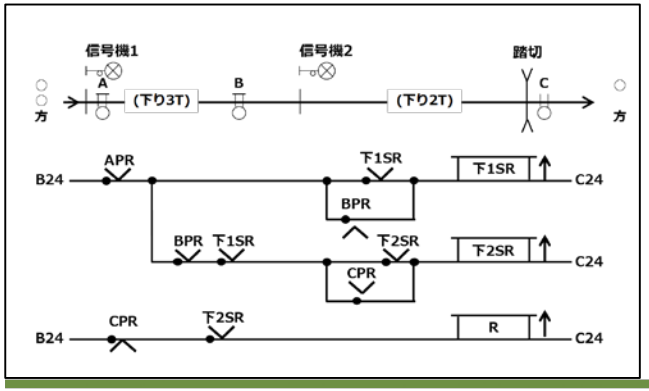
踏切制御論理の特徴

特徴：

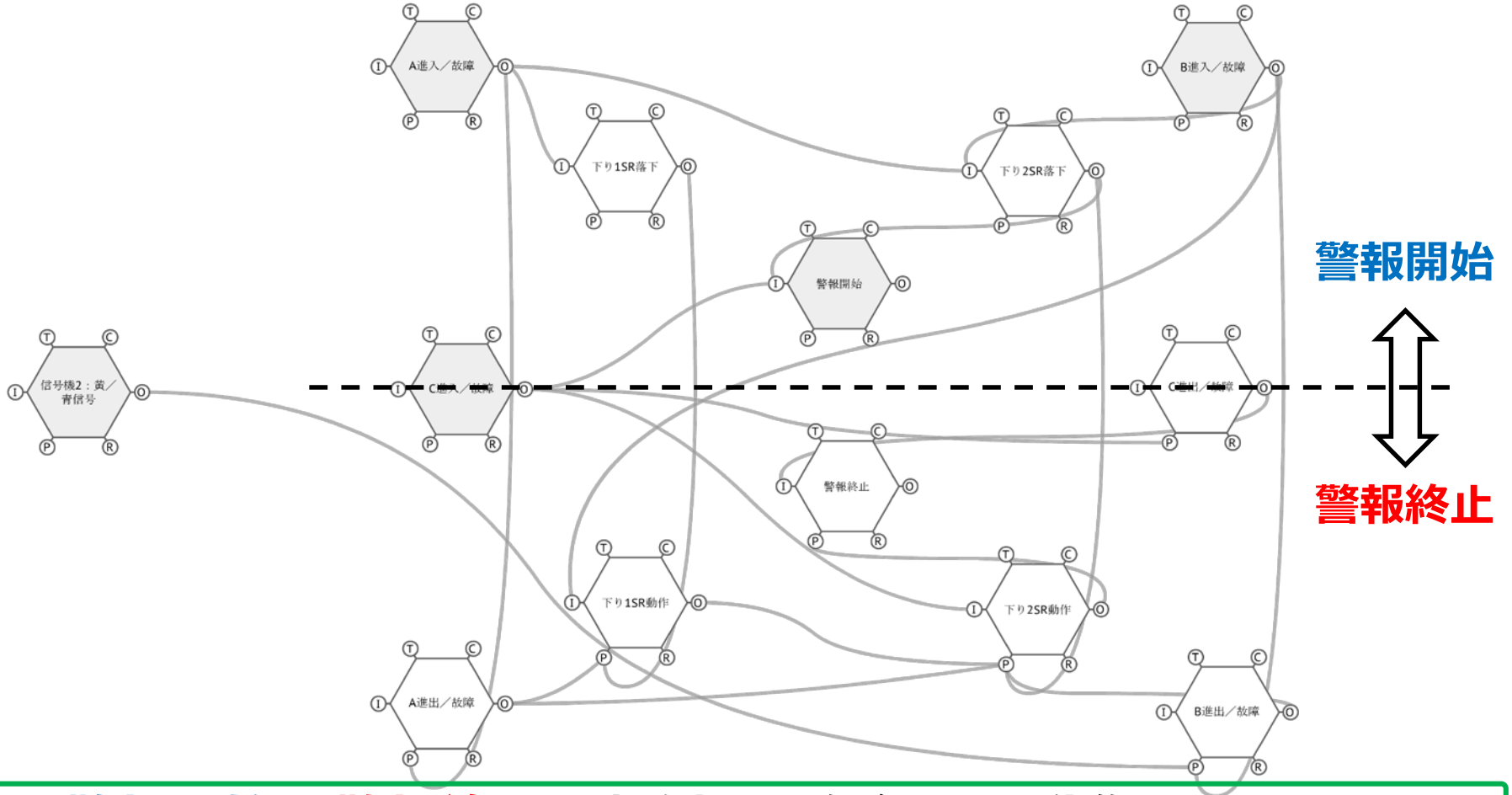
- 踏切警報を開始／終止させるための制御論理であり、開発の歴史は数十年に亘る。
- 線路に設置されたセンサの物理状態、列車の在線状態、警報状態から構成される。



FRAMモデル

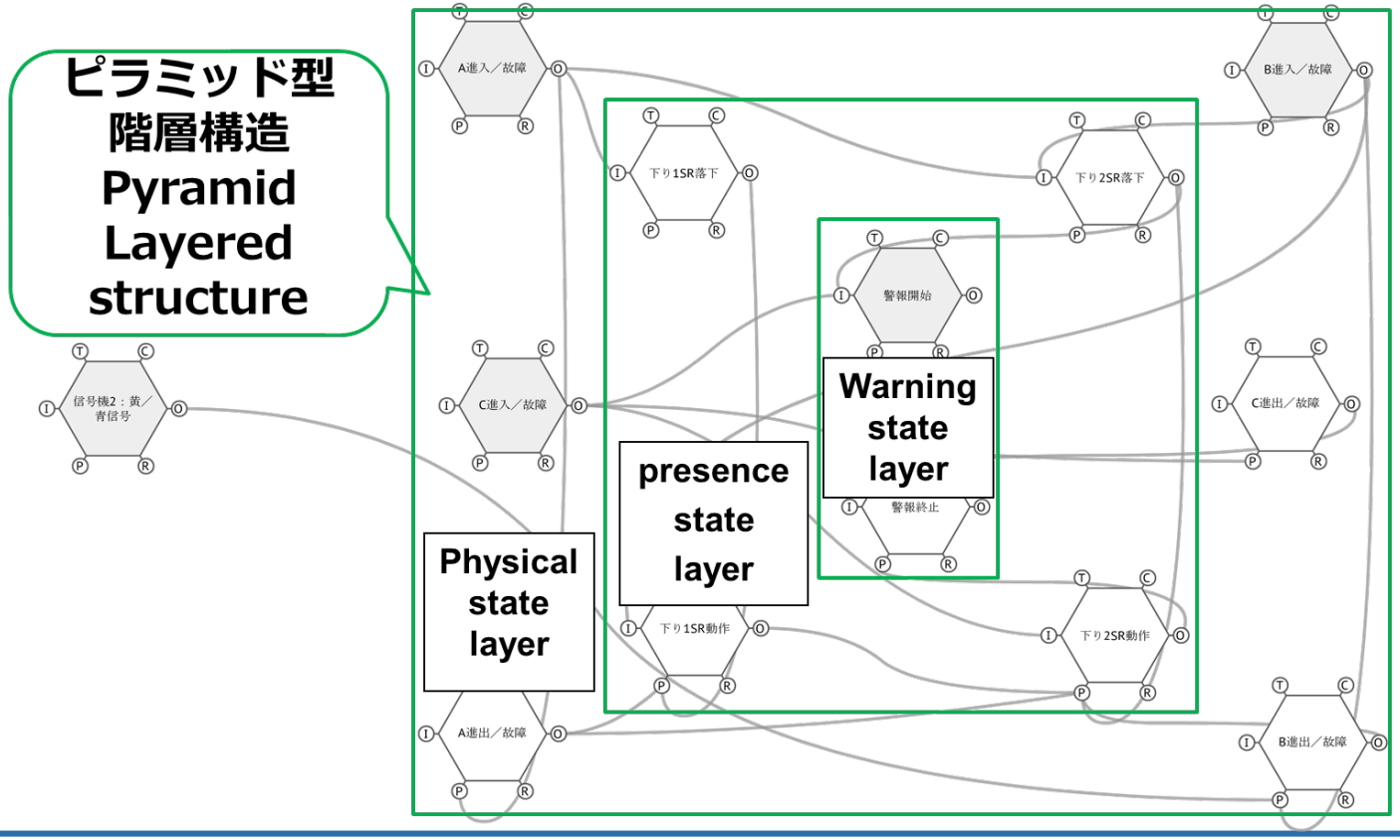


FRAMモデルの特徴



警報開始と警報終止は類似した仕組みで動作している
（対称性のある構造）

FRAMモデルの特徴



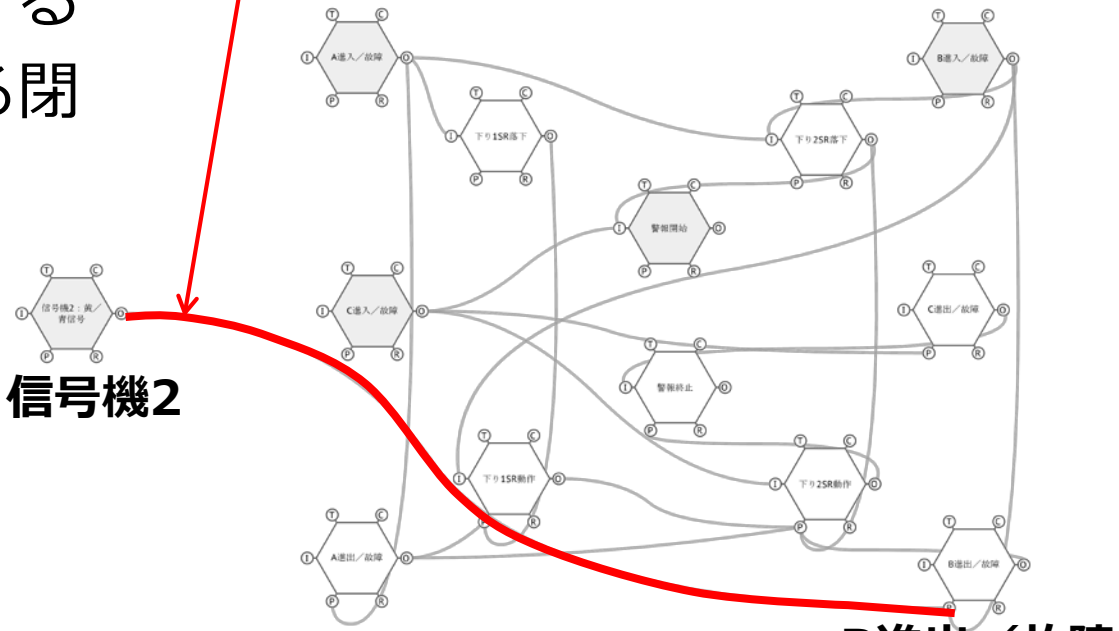
各レイヤーは、隣り合うレイヤーとのインタラクションだけを
ケアすれば良い（階層構造）ため、システム全体の
ネットワーク構成に影響を受けにくく、汎用性が高い。

リスク要因

リスク要因：

・正しく続行列車対策を実現するためには、閉塞信号機による閉塞区間の確保が前提

信号機の情報が、機能開始の前提条件となっている



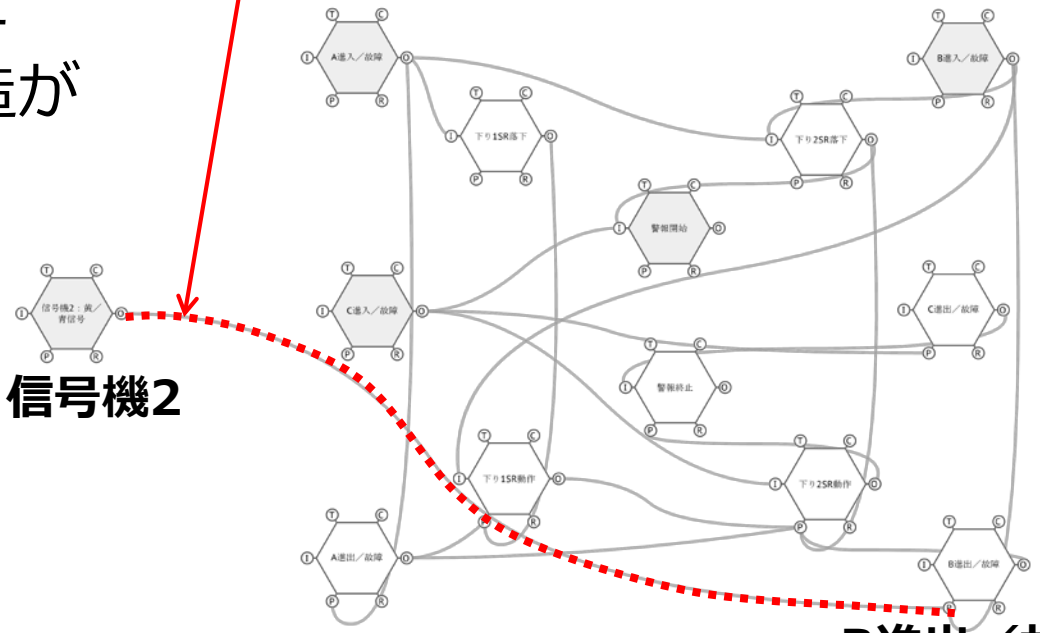
閉塞区間有り

リスク要因

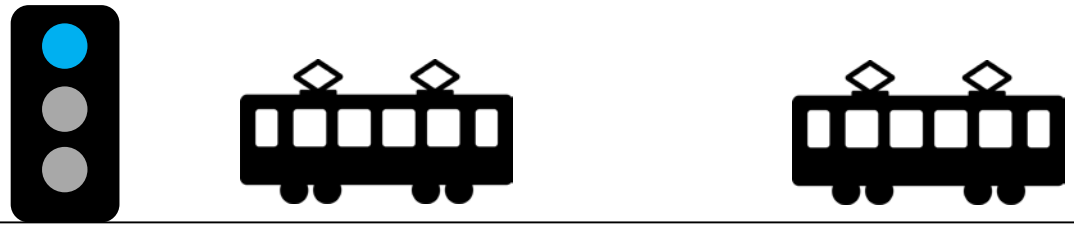
リスク要因：

・閉塞区間が無いと、これまで
安全を制御していた機能構造が
成立しなくなる

信号機の情報が無く、
機能開始の前提が成立しない



閉塞区間無し

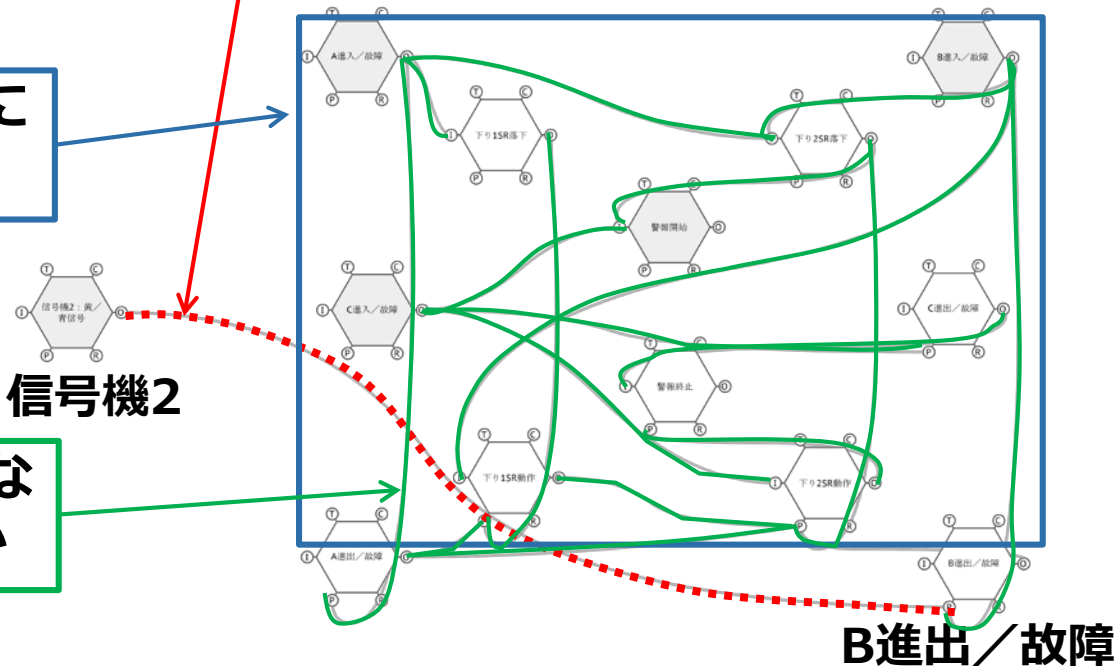


FRAMモデル

リレー制御を電子化する場合：

信号機の情報が無くなると

**これまで安全を確保していた構造に
どのような影響が生じるか？**



**機能間の繋がりに、今まで想定しな
かったような問題が発生しないか**

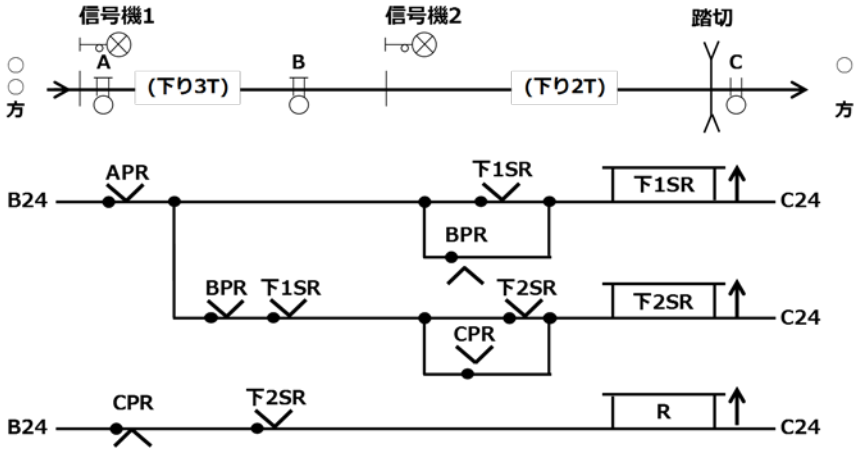
**もし、列車間の距離をフレキシブルに制御したい場合、
信号に依存しているアーキテクチャを変更しなければならない**

3. まとめ

まとめ

宇宙機／鉄道など、システムが大規模になり、自動制御化が進むと、システム全体のインタラクションが不明確になり、安全確保が困難となる

X線天文衛星ASTRO-H軌道上外観図



（出典）国立研究開発法人 宇宙航空研究開発機構（JAXA),
『X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書 p.6』, 2016.6.14,
http://www.jaxa.jp/press/2016/06/20160614_hitomi_j.html

まとめ

初めからリスクを探そうとしても、
前例の無いリスクを見つけることは困難

そこで、まずはシステム全体をモデル化し、
機能間のインタラクションを明確化する

そして、『何故このシステムは上手く制御できているのか』を考え、
『上手く制御できなくなった場合のリスクを見出す』

これが、FRAMによる安全解析

４．自動制御システムの課題

自動制御システムの課題

緊急時の対応：

・自動制御システムでも、緊急時は人が制御を実施

・問題の多くは、人が制御を代替する時に発生

(※)

自動制御 → **緊急時** → **手動制御**

緊急時に人に権限が移行した時に問題が発生

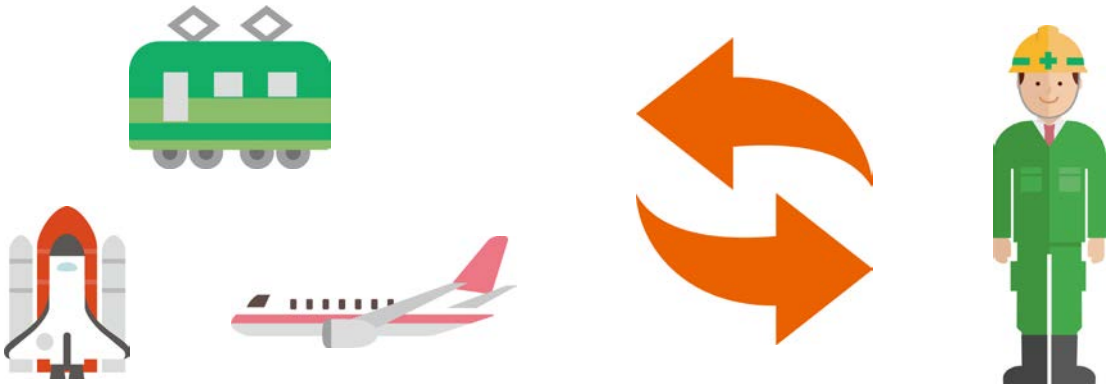
※（出典）Jasmina Stanojevic,
http://free-illustrations.gatag.net/2014/04/20/040000.html

自動制御システムの課題

Japan Manned Space Systems Corporation
JAMSS
ひとと宇宙を結ぶインテグレータ

人間に関与させることの重要性

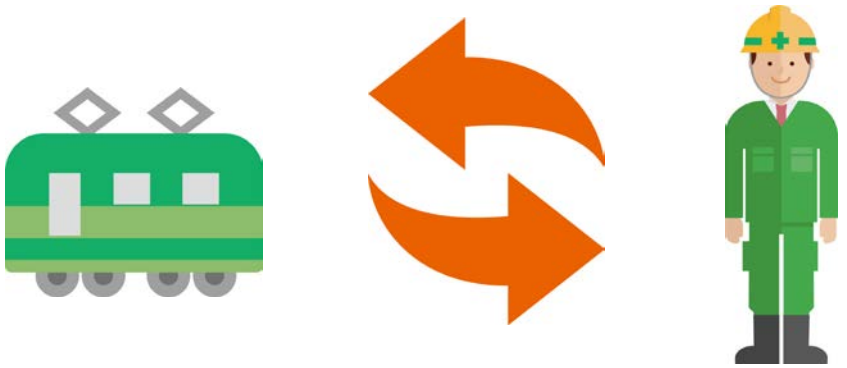
・トラブルに対して柔軟に対応するために、人に役割を持たせ続けた方が、切替えがスムーズになる
・ヒューマンエラーを防止するために、あえて人間に権限を残す
・システムトラブルから回復するために、あえて人間に権限を残す



自動制御時も人に役割を持たせ続ける

自動制御システムの課題

鉄道ではダイヤ乱れ等のトラブルが頻繁に発生
しかし、
自動制御システムと人が上手く連携し、トラブルに柔軟に対応



鉄道にこそ、
自動制御システムの安全を学ぶべき点が多数存在