



# 安全性解析技法を用いた 鉄道障害事故の分析

千葉工業大学

社会システム科学部 プロジェクトマネジメント学科

小笠原秀人、瀬戸口大空

# 目次

1. 目的
2. 事故の原因
3. STAMP/STPA
4. 分析結果
5. 考察

# 1. 目的

- STAMP/STPAはよく知られている
  - 何度か説明は聞いたが、よく分からないという印象
- 実際に使えるのか、使うのは難しいのか？
  - 試してみないことには始まらない
- よく話題に出てくる鉄道事故がある
  - 金沢シーサイドライン新杉田駅構内で発生した鉄道人身障害事故を対象にする

## 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～

独立行政法人情報処理推進機構  
Information Technology Promotion Agency, Japan (IPA)  
技術本部 ソフトウェア高信頼化センター  
Software Reliability Enhancement Center (SEC)  
ソフトウェア高信頼化推進委員会  
Software Reliability Enhancement Promotion Committee  
システム安全性解析手法 WG  
System Safety Analysis WG

Ver.1.0  
2016年3月

# 金沢シーサイドライン鉄道人身障害事故

- 2019年6月1日20時頃発生
- 当該列車は新杉田発並木中央行2009B列車
- 新杉田駅を20:15に出発予定
- 出発後、進行方向と逆方向に発車  
→ 車止めに衝突
- 乗客25名中、17名が負傷



<https://news.ntv.co.jp/category/society/825366>

## 事故事例分析の目的

- STAMP/STPAでこの事故を事前に識別できる可能性はあったのか？
- この事故以外に事故につながるシナリオは検出できるのか？

## 2. 事故の原因（参考文献[2]P38～43）

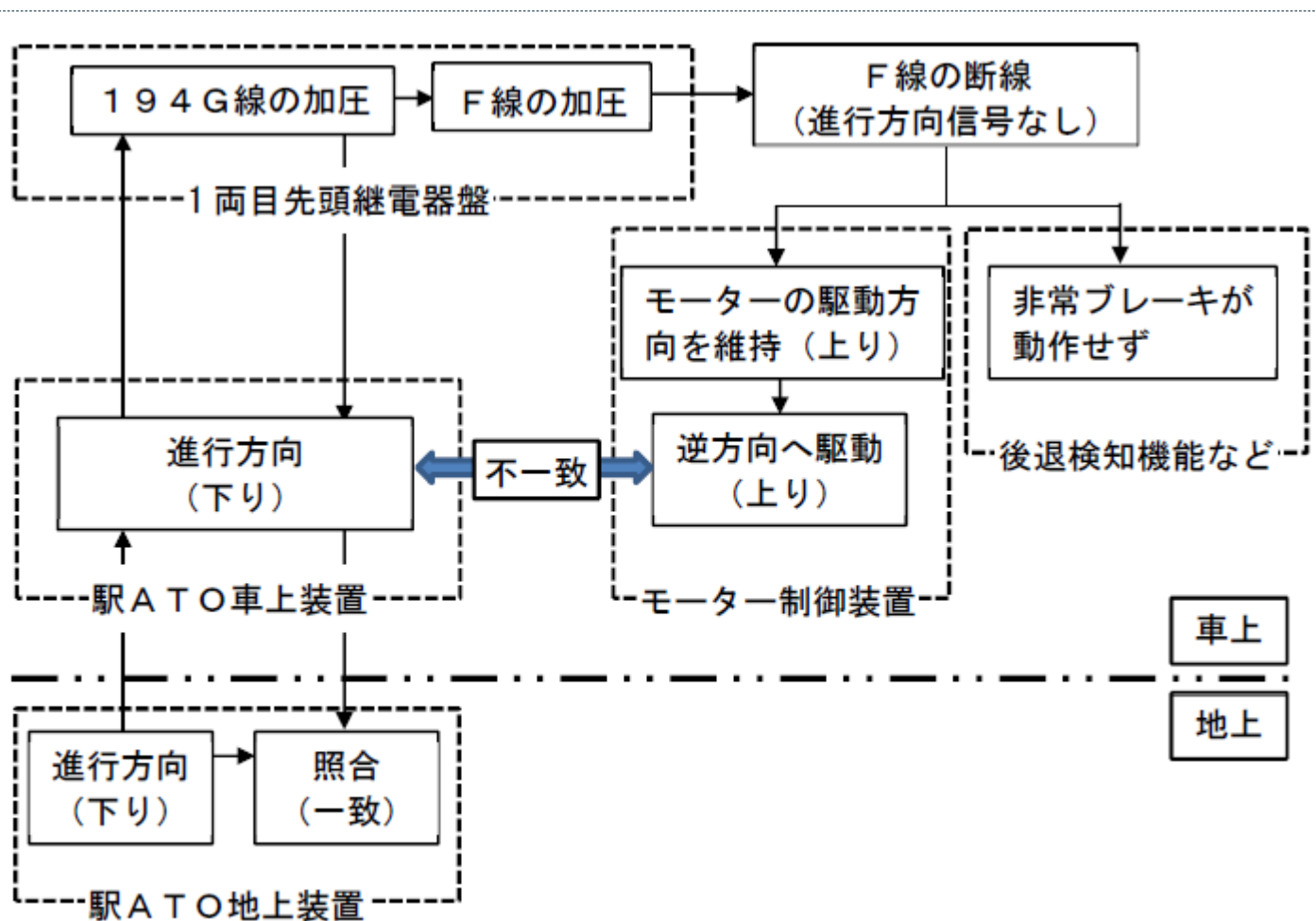


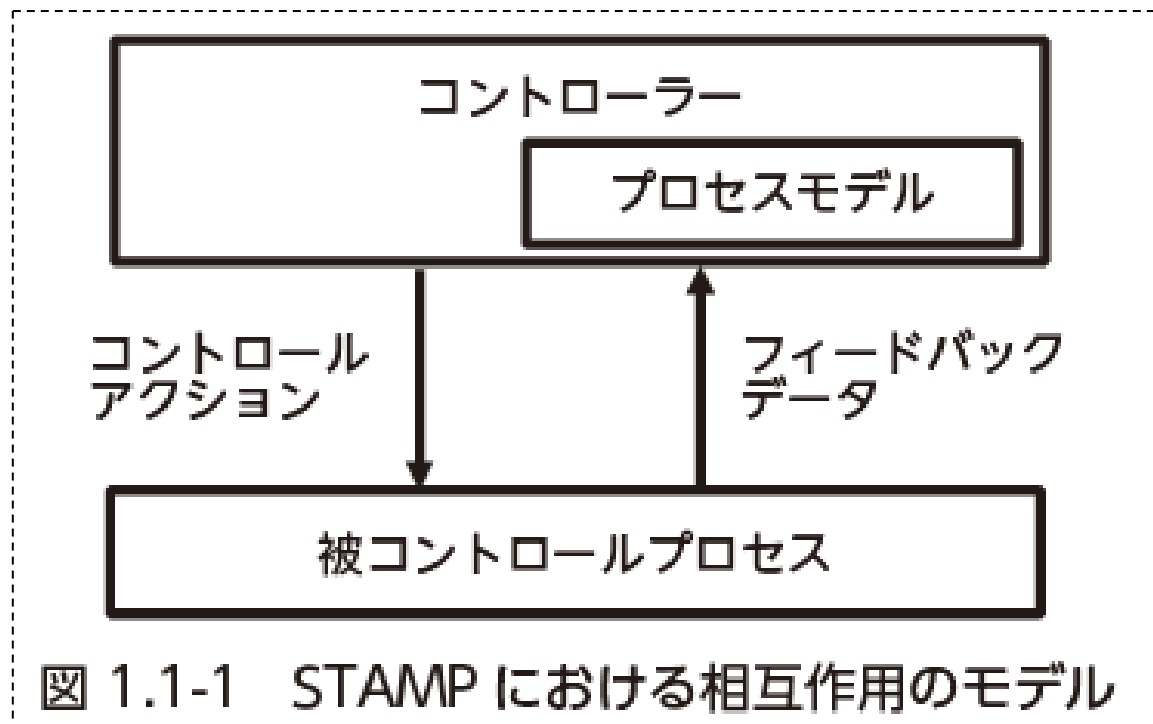
図19 本事故時の信号の伝送及び各装置における認識

- 駅ATO（Automatic Train Operation：自動列車運転装置）地上装置は車両への進行方向指令と車両からの進行方向状態が下りで一致したと判断した。
- モーター制御装置は、進行方向をメモリ機能が維持していた上り方向にモーターを駆動するようになっていたことから、本件列車の進行方向と逆である上り方向にモーターを起動した。
- ATC（Automatic Train Control：自動列車制御装置）車上装置にある後退検知機能や他の手法により異常走行を検知せず、列車が車止めに衝突するまでブレーキが動作しなかった。

# 3. STAMP/STPA

- マサチューセッツ工科大学（MIT）のNancy G.Leveson 教授が提唱
- アクシデントモデルSTAMP（Systems-Theoretic Accident Model and Process：システム理論に基づくアクシデントモデル）
  - 現代のシステムのアクシデントの多くは、システムの中で安全のための制御を行う要素（コントローラー）と制御される要素（被コントロールプロセス）の相互作用が働かないことが原因
  - これを作成することで、制御主体と制御対象の間で行われる制御を明確化し、STPA分析において理解しやすいイメージを共有することができる
- 安全解析手法STPA（STAMP based Process Analysis）
  - STAMPを前提として、システムのハザード要因を分析する新しい安全解析手法

# STAMPにおける相互作用モデル



参考文献[2]から引用

- アクシデントは、相互作用が適切に働かないことによって起こる
- 具体的にはコントローラーから被コントロールプロセスへの必要な制御指示（コントロールアクション）が適切に与えられないために起こる
- そして、不適切なコントロールアクションが与えられる要因として、コントローラー自身が想定する被コントロールプロセスの状態（これをプロセスモデルという）が、実際の被コントロールプロセスの状態を正しく反映できていないことが主要な要因である

# STAMP/STPAの手順





# 4. 分析結果



Step0  
(準備1)

アクシデント、ハザード、安全制約の識別

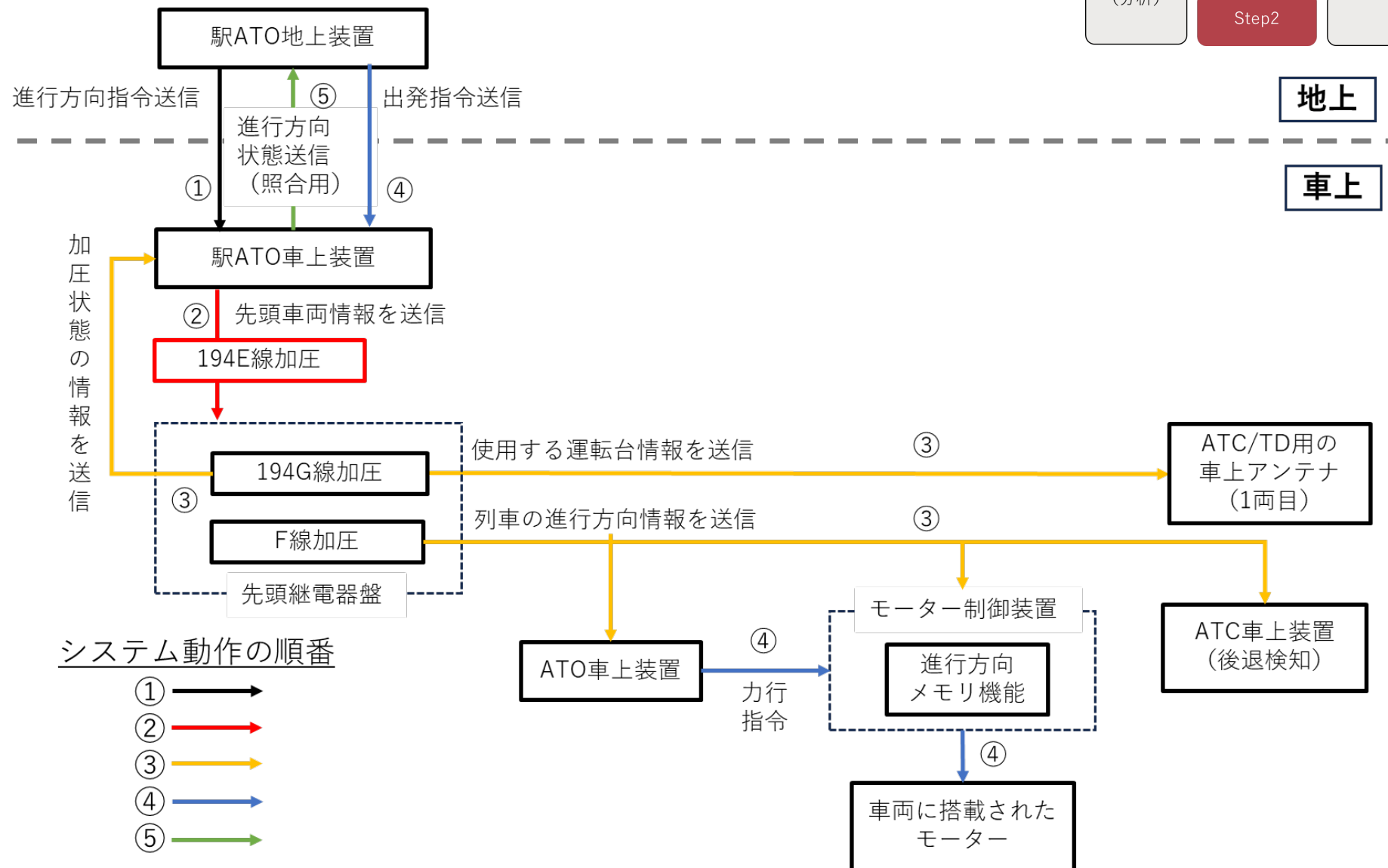
| アクシデント<br>(Loss)   | ハザード<br>(Hazard)        | 安全制約<br>(Safety Constraints)    |
|--------------------|-------------------------|---------------------------------|
| (A1)列車が予期せぬ方向へ発車する | (H1)指令線が正しく加圧されていない     | (SC1)指令線は正しく加圧されなければならない        |
| (A1)列車が予期せぬ方向へ発車する | (H2)進行方向指令を正常に受信できていない  | (SC2)進行方向指令は正常に送受信できていなければならない  |
| 列車が自走不能になる         | モーターやコンプレッサー等、走行機器が故障する | 仕業前に列車検査を行い、走行機器が正常に動作することを確認する |
| 列車が発車できない          | 乗客の乗降に時間がかかっている         | 乗客は、定められた停車時間内に乗降を行う            |
| 列車が発車できない          | 悪天候による線路状態の悪化           | 気象条件に基準を設け、基準を守れない場合は列車の運行を停止する |

列車折り返し時に使用されるシステムのエラーを対象としているため、保安装置以外の走行機器の故障に関するアクシデントや、気象条件が直接要因となるアクシデントは分析の対象外とし、対象をA1「列車が予期せぬ方向へ発車する」に関連するH1・SC1、SC1、H2・SC2とした。

## Step0 (準備2)

# 構築したコントロールストラクチャ

|                    |                |                     |
|--------------------|----------------|---------------------|
| STAMP<br>モデル<br>作成 | Step0<br>(準備1) | アクシデント、ハザード、安全制約の識別 |
|                    | Step0<br>(準備2) | コントロールストラクチャーの構築    |
| STPA<br>(分析)       | Step1          | 非安全なコントロールアクションの抽出  |
|                    | Step2          | ハザード要因の特定           |



Step1

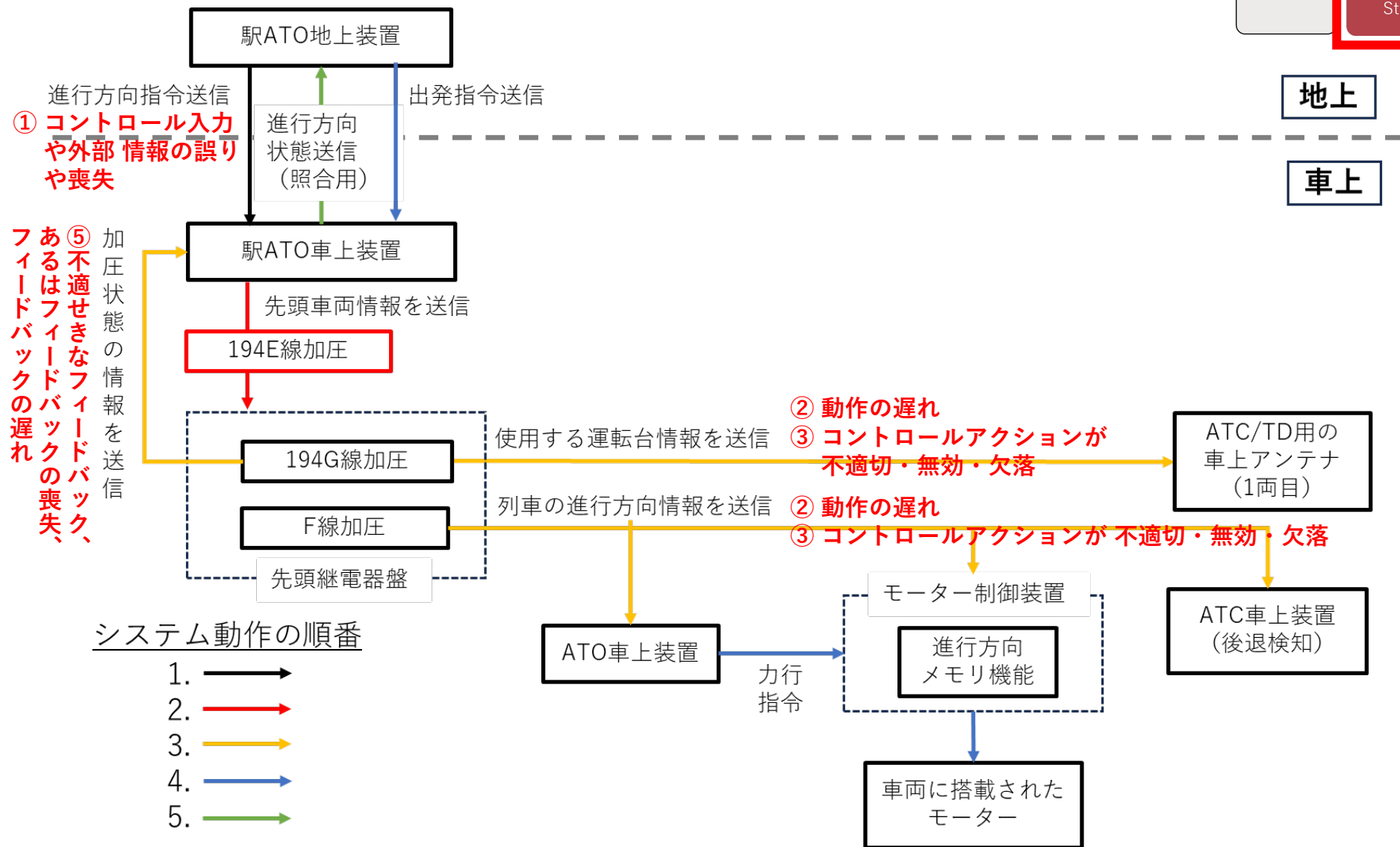
# 非安全なコントロールアクション (UCA: Unsafe Control Action) の抽出結果

|                    |                |                     |
|--------------------|----------------|---------------------|
| STAMP<br>モデル<br>作成 | Step0<br>(準備1) | アクシデント、ハザード、安全制約の識別 |
|                    | Step0<br>(準備2) | コントロールストラクチャーの構築    |
| STPA<br>(分析)       | Step1          | 非安全なコントロールアクションの抽出  |
|                    | Step2          | ハザード要因の特定           |

|   | コントロールアクション                | 与えられないとハザード                                                      | 与えられるとハザード                                                        | 早すぎ、遅すぎ、誤順序でハザード                                                                      | 早すぎる停止、<br>長すぎる運用でハザード      |
|---|----------------------------|------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------|
| 1 | 進行方向指令を送信する                | 列車の進行方向が変化せず、モーター制御装置の進行方向が切り替わらないが、列車は出発指令が出るまでは出発できないため、暴走しない  | (UCA2) 出発時刻でないのに指令を送信する (SC2に違反)                                  | 情報の受信が早すぎると、列車の進路が未開通のまま出発準備が進むが、列車の出発指令が出るまでは出発できないため、列車は暴走しない                       | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 2 | 先頭車両情報を送信する                | 先頭車両の設定ができない                                                     | (UCA3) 反対側の先頭車両を先頭車両に設定する (SC2に違反)                                | 情報の受信が遅すぎると、列車遅延に繋がる                                                                  | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 3 | 使用する運転台情報を送信する             | ATC/TD用の車上アンテナの信号が正常に切り替わらず、発車後の速度照査ができないため、発車できない               | ATC/TD用の車上アンテナの信号が反対側の先頭車両に切り替わる (=切り替わっていない)                     | 遅すぎる場合、ATC/TD用の車上アンテナの信号が切り替わらず、発車後の速度照査ができないため、発車できない                                | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 4 | 194G 線の加圧状態を、駅ATO車上装置へ送信する | 駅ATO地上装置へ進行方向状態を送信できない                                           | (UCA4) 194G線を加圧していない状態のまま、加圧したとみなして加圧状態を駅ATO車上装置に送信する (SC1に違反)    | 遅すぎる場合、駅ATO地上装置が出発指令を送信できないため、列車が出発できない                                               | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 5 | 列車の進行方向情報を送信する             | (UCA1) モーター制御装置の進行方向メモリ機能に記憶されている進行方向情報が変わらず、車止め方向へ発車する (SC1に違反) | 正常に進行方向が切り替えられる                                                   | (UCA1) 遅すぎる場合、モーター制御装置の進行方向メモリ機能に記憶されている進行方向情報が切り替わらないまま発車する、後退検知機能も正常に動作しない (SC1に違反) | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 6 | 進行方向状態を、駅ATO地上装置へ送信する      | 進行方向の照合が出来ず、駅ATO地上装置が出発指令を送信できないため、列車が出発できない                     | (UCA5) 194G線が加圧されていない状態のまま、加圧したとみなして進行方向状態を駅ATO地上装置へ送信する (SC2に違反) | 遅すぎる場合、駅ATO地上装置が出発指令を送信できないため、列車が出発できない                                               | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 7 | 出発指令                       | 列車が出発できない                                                        | 正常に指令が出される                                                        | 早すぎる場合、車両の側扉及び可動式ホーム柵が閉状態にならないまま走行する                                                  | 指令の長さは影響しないため、特に重大な問題は発生しない |
| 8 | 力行指令                       | 力行することが出来ず、発車することが出来ない                                           | 正常に指令が出される                                                        | 早すぎる場合、車両の側扉及び可動式ホーム柵が閉状態にならないまま走行する                                                  | 極端に長く指令が出ると、列車は減速せず、暴走する    |

# ハザード要因 (HCF : Hazard Causal Factor) の特定 (1/2)

## ④ コンポーネントの故障・経年変化 (全コンポーネントに共通)



|                    |                |                     |
|--------------------|----------------|---------------------|
| STAMP<br>モデル<br>作成 | Step0<br>(準備1) | アクシデント、ハザード、安全制約の識別 |
|                    | Step0<br>(準備2) | コントロールストラクチャーの構築    |
| STPA<br>(分析)       | Step1          | 非安全なコントロールアクションの抽出  |
|                    | Step2          | ハザード要因の特定           |

## 今回使用するHCFを特定するためのガイドワード

- ① コントロール入力や外部情報の誤りや喪失
- ② 動作の遅れ
- ③ コントロールアクションが不適切・無効・欠落
- ④ コンポーネントの故障・経年変化
- ⑤ 不適切なフィードバック、あるいはフィードバックの喪失、フィードバックの遅れ

|                                                                 | ①コントロール入力や外部情報の誤りや喪失                      | ②動作の遅れ       | ③コントロールアクションが不適切・無効・欠落                     | ④コンポーネントの故障・経年変化                           | ⑤不適切なフィードバック、あるいはフィードバックの喪失、フィードバックの遅れ |
|-----------------------------------------------------------------|-------------------------------------------|--------------|--------------------------------------------|--------------------------------------------|----------------------------------------|
| （UCA1）モーター制御装置における進行方向のメモリ機能の進行方向が切り替わらないまま発車する（SC1に違反）         | 駅ATO地上装置と駅ATO車上装置の間における進行方向指令の送受信が上手くいかない | F線の加圧が間に合わない |                                            | F線の断線による進行方向切り替えの失敗と、メモリ機能による進行方向の記憶で逆走が発生 |                                        |
| （UCA2）出発時刻でないのに指令を送信する（SC2に違反）                                  |                                           |              | 所定の時間前に出発指令を誤送信                            | 駅ATO地上装置の故障によるデータ誤送信                       |                                        |
| （UCA3）反対側の先頭車両を先頭車両に設定する（SC2に違反）                                |                                           |              | 加圧する指令線が不適切であるために、予定とは反対側の先頭車両を先頭車両として設定する |                                            |                                        |
| （UCA4）194G線を加圧していない状態のまま、加圧したとみなして加圧状態を駅ATO車上装置に送信する（SC1に違反）    |                                           |              |                                            |                                            | 194G線の加圧情報が正常に伝達できていない                 |
| （UCA5）194G線が加圧されていない状態のまま、加圧したとみなして進行方向状態を駅ATO地上装置へ送信する（SC2に違反） |                                           |              |                                            |                                            | 194G線の加圧情報が正常に伝達できていない                 |

# UCAに至るハザードシナリオと 解決策の例

## UCA1の内容と安全制約の違反内容

(UCA1) モーター制御装置の進行方向メモリ機能に記憶されている進行方向情報が変わらず、車止め方向へ発車する

(UCA1) 遅すぎる場合、モーター制御装置の進行方向メモリ機能に記憶されている進行方向情報が切り替わらないまま発車する、後退検知機能も正常に動作しない  
上記2つは、安全制約1「指令線は正しく加圧されていなければならない」に違反

### シナリオ

#### ④コンポーネントの故障・経年変化

F線の断線による列車の  
進行方向の切替に失敗する

### 対策 対象：モーター制御装置

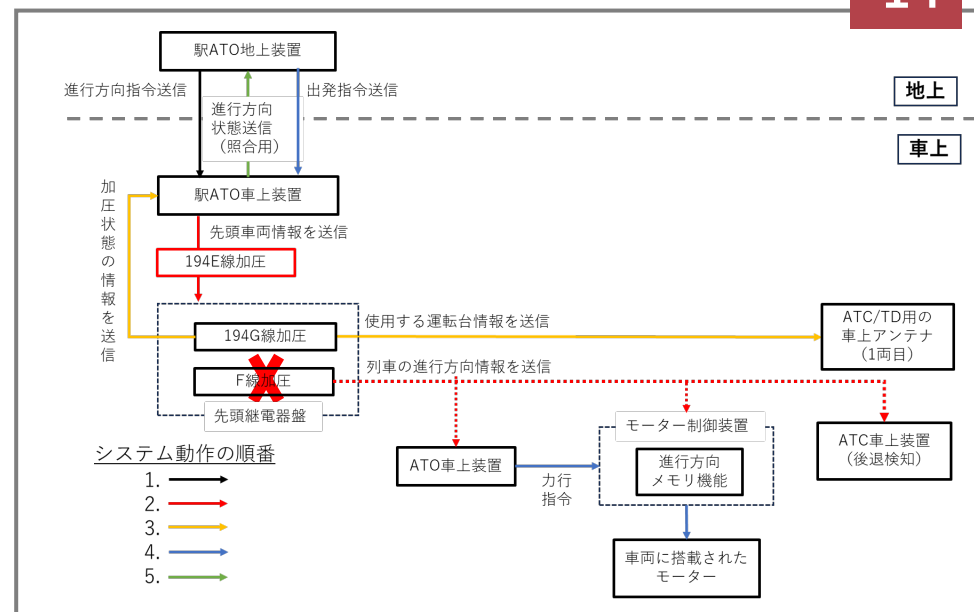
進行方向の切替確認のため、当装置と駅ATO車上装置の間で進行方向の照合を行う

#### 一致しない場合

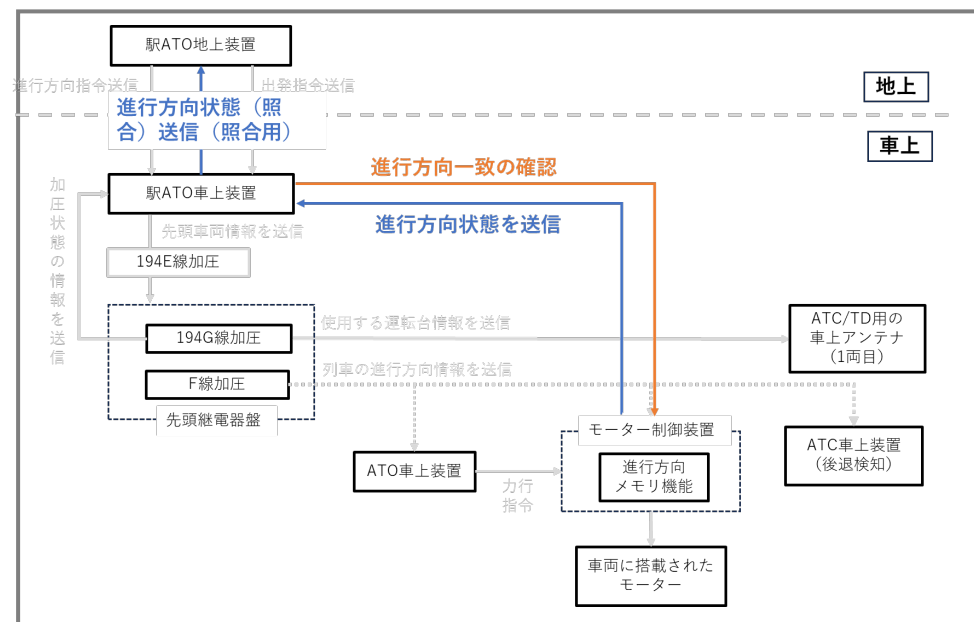
列車の運行を抑止  
(保護動作)

#### 一致する場合

駅ATO地上装置へ  
進行方向状態を送信



シナリオの発生個所



対策案のイメージ

# 分析結果のまとめ

| Step   | 実施内容                 | インプット                                     | アウトプット           | 抽出数／特定数          |
|--------|----------------------|-------------------------------------------|------------------|------------------|
|        | 前提条件の整理              | ・仕様書他                                     | システムの流れを把握できる資料  |                  |
| 0(準備1) | アクシデント、ハザード、安全制約の識別  | ・システムの流れを把握できる資料                          | アクシデント、ハザード、安全制約 | アクシデント数：2        |
| 0(準備2) | コントロールストラクチャーの構築     | ・システムの流れを把握できる資料<br>・安全制約                 | コントロールストラクチャー    |                  |
| 1      | UCAの抽出               | ・システムの流れを把握できる資料<br>・安全制約<br>・用意されたガイドワード | UCA              | UCA：6            |
| 2      | HCFの特定（シナリオ作成）と対策の検討 | ・UCA<br>・用意されたガイドワード                      | HCF              | シナリオ：9<br>対策案：10 |

## 事故事例分析の目的

- STAMP/STPAでこの事故を事前に識別できる可能性はあったのか？  
→ 安全制約（SC1、SC2）に違反するUCA（非安全制御動作）を特定できた
- この事故以外に事故につながるシナリオは検出できるのか？  
→ 「出発事項ではないのに指令を送信する」「反対側の先頭車両を先頭車両に設定する」に関するシナリオを検出できた



## 5. 考察

- 分析結果の確からしさ
  - 今回の分析は、文献[2]を読んだうえで実施
  - ハザードの粒度などが細くなり、結果ありきの分析になっている可能性は否めない
  - しかしながら、STAMP/STPAのステップで分析した結果から、今回の事故を事前に識別できる可能性は確認できた
- 手法適用に際して
  - 対象となるシステムの流れや動作環境などを理解する必要あり
    - 高度な専門性を有するシステムであるほど、UCAの適切な抽出やハザード対策案の練り込みが難しい
  - 凝り固まった考えを排除する仕組みや仕掛けが必要
    - アクシデントやハザード、安全制約の識別において、「発想」の作業が現場の経験や発想力に頼ってしまう傾向がある



- 設計に関する情報（文献[2] 2.9節）
  - 設計・製造プロセスや実施した設計作業などが示されている
  - 従来の安全性解析技法（ミニデザインレビューなど）も活用され、さまざまな関係者間で検討され審査されていることが分かる
  - 一方で、車両メーカーは、「各装置の機能や装置間のやり取り全てについては把握することは難しい」、「制御装置などの極めて専門性が高いものについては、装置メーカーの企業秘密として開示されないところもあり、近年のエレクトロニクス化の進展に伴い、その範囲は拡大傾向にある」と述べている
- どのように立ち向かえばよいのか？
  - 今回の開発では、事業者と車両メーカー、車両メーカーと装置メーカー（複数）間で認識の齟齬があった
    - 当たり前だが、関係者間での齟齬をなくすことが必要
  - 相互作用が複雑なシステムに対する既存の安全解析手法とSTAMP/STPAなどの新しい安全解析手法の融合を考える

# 参考文献

[1] システム安全性解析手法WG, 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～, 情報処理推進機構 (IPA), 2016.

[2] 運輸安全委員会, “鉄道事故調査報告書”,  
<https://www.mlit.go.jp/jtsb/railway/rep-acci/RA2021-1-1.pdf>,  
2021.