鉄道システムの安全性検証にSTAMPを使ってみて

東日本旅客鉄道株式会社
JR東日本研究開発センター
北村　知

Agenda

１．これまでのJR東日本の取り組み
「初めてのSTAMP/STPA」での事例検討

２．ケーススタディ
「無線タイマー式踏切制御装置を導入するとしたら」
- 無線タイマー式踏切制御装置とは
- STAMP/STPAによる検証

３．考察
- FTAとの比較

４．まとめ

1．これまでのJR東日本の取り組み

2016年3月　はじめてのSTAMP/STPA

単線の3点制御踏切における安全性検証にSTAMP/STPAを活用

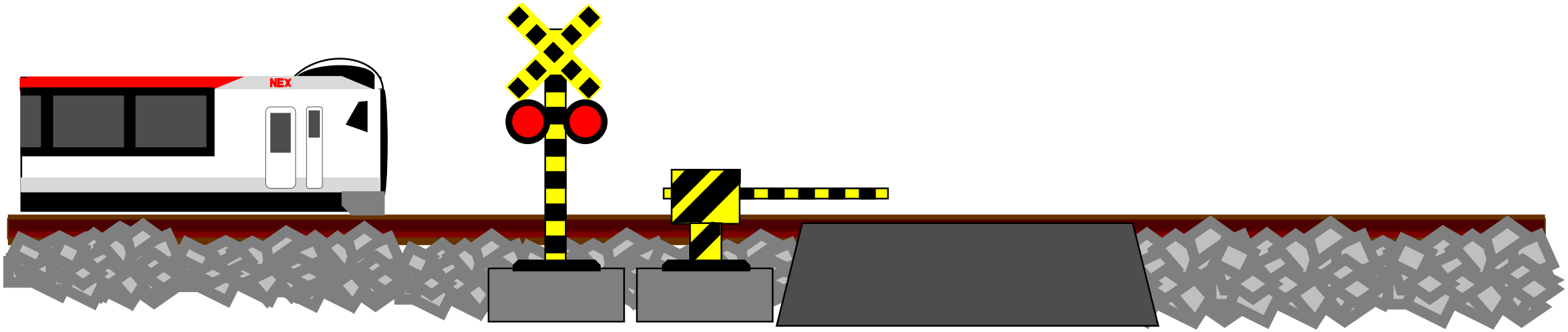
6つのUCAに対して、17のハザードシナリオを抽出

STAMP/STPA手法の可能性を認識

1．これまでのJR東日本の取り組み

2016年3月　はじめてのSTAMP/STPA

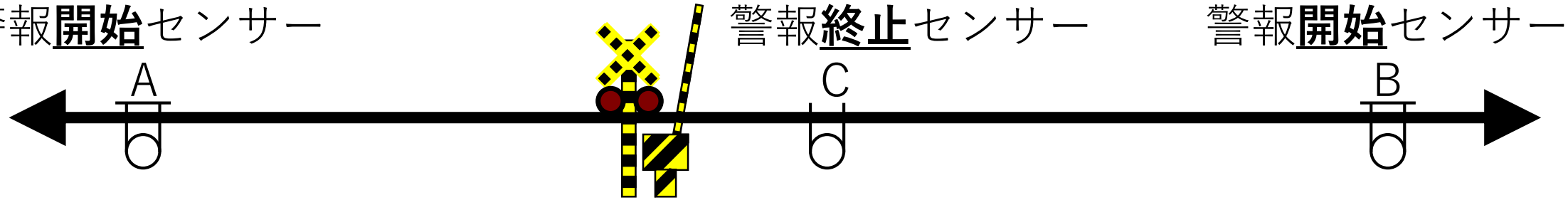
単線の3点制御踏切における安全性検証にSTAMP/STPAを活用



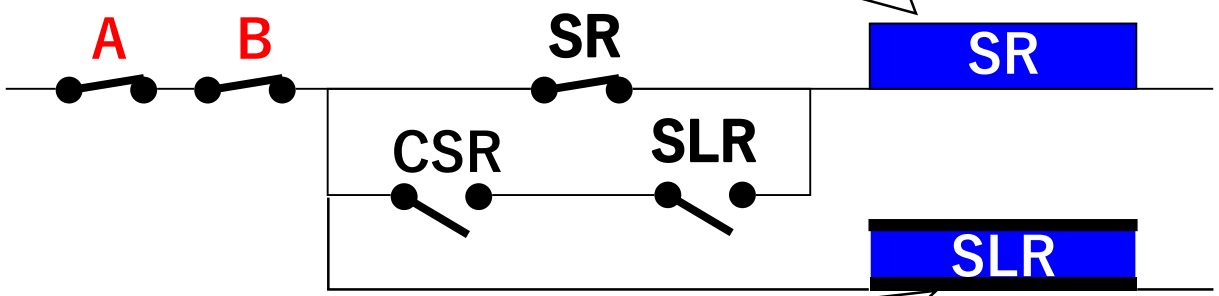
1．これまでのJR東日本の取り組み

単線踏切制御の動き
（国鉄時代のもっとも簡易なもの）

A, B, Cの3センサと
SR, SLR, CSRの3条件で制御

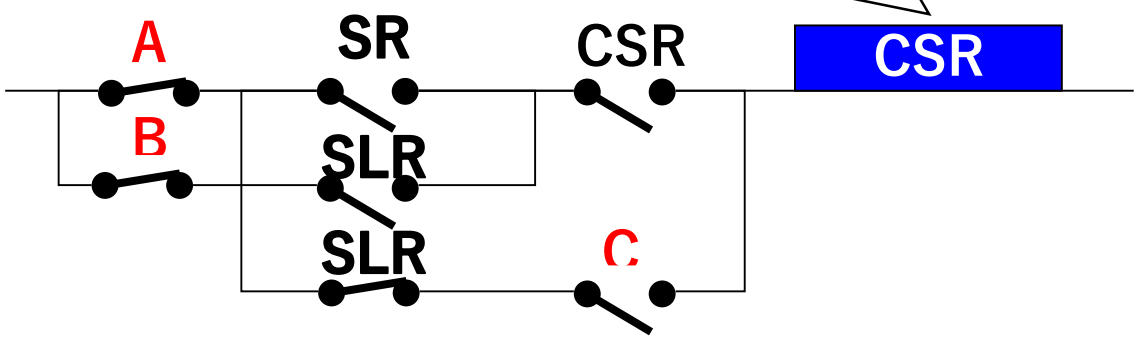


A↔B間に列車がいる状態
警報条件

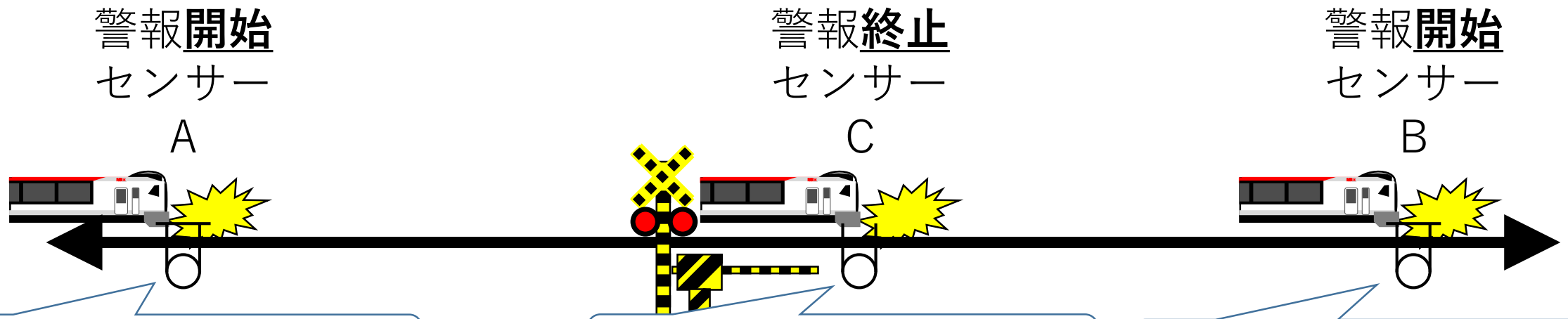


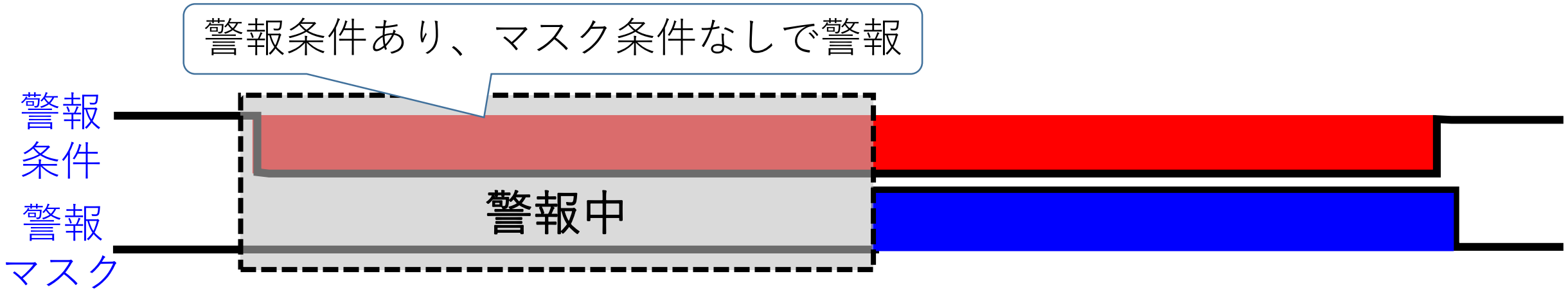
A又はBの**列車検知条件**
（遅れ時間あり）

C→AまたはB間に列車がいる状態
マスク条件

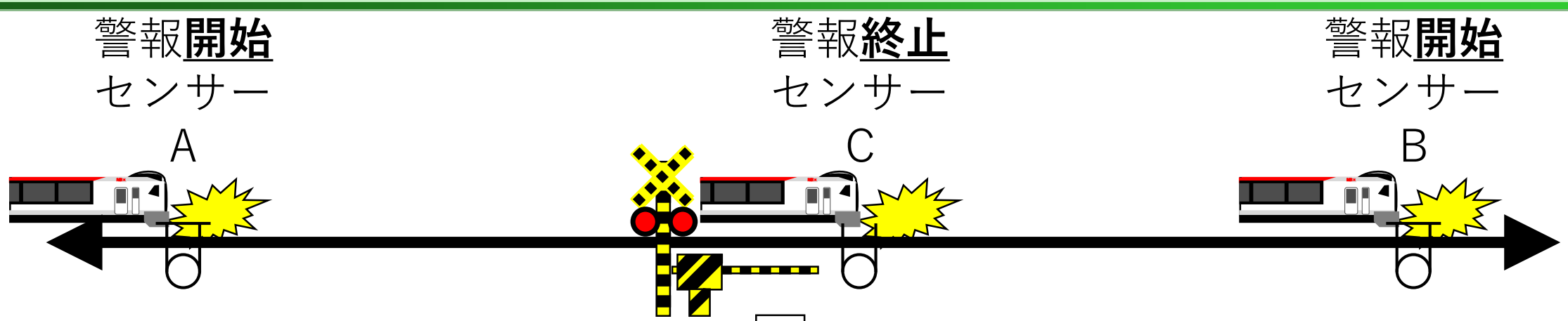


1．これまでのJR東日本の取り組み

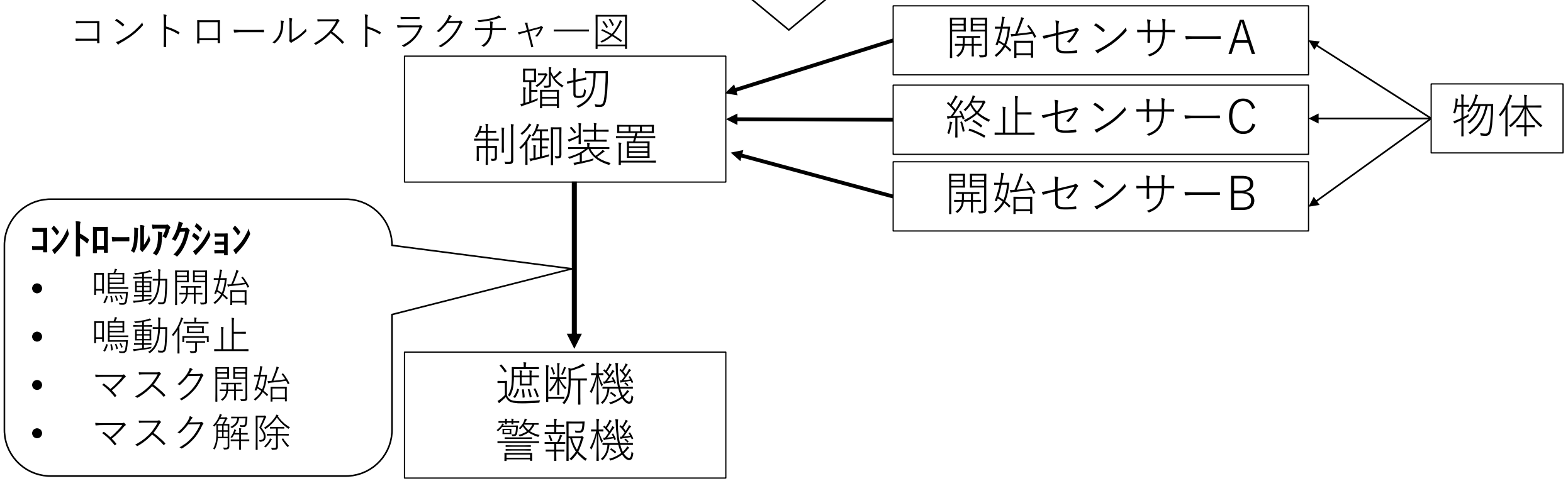




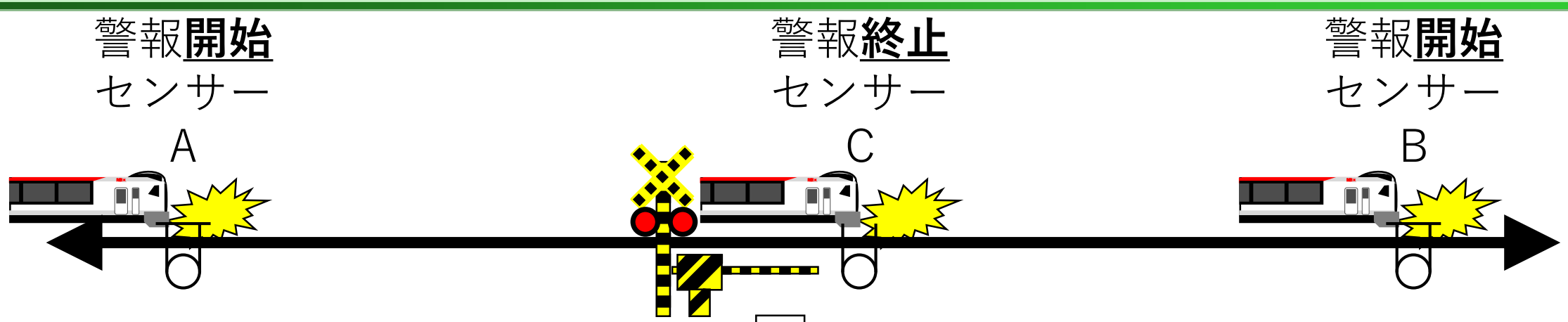
1．これまでのJR東日本の取り組み



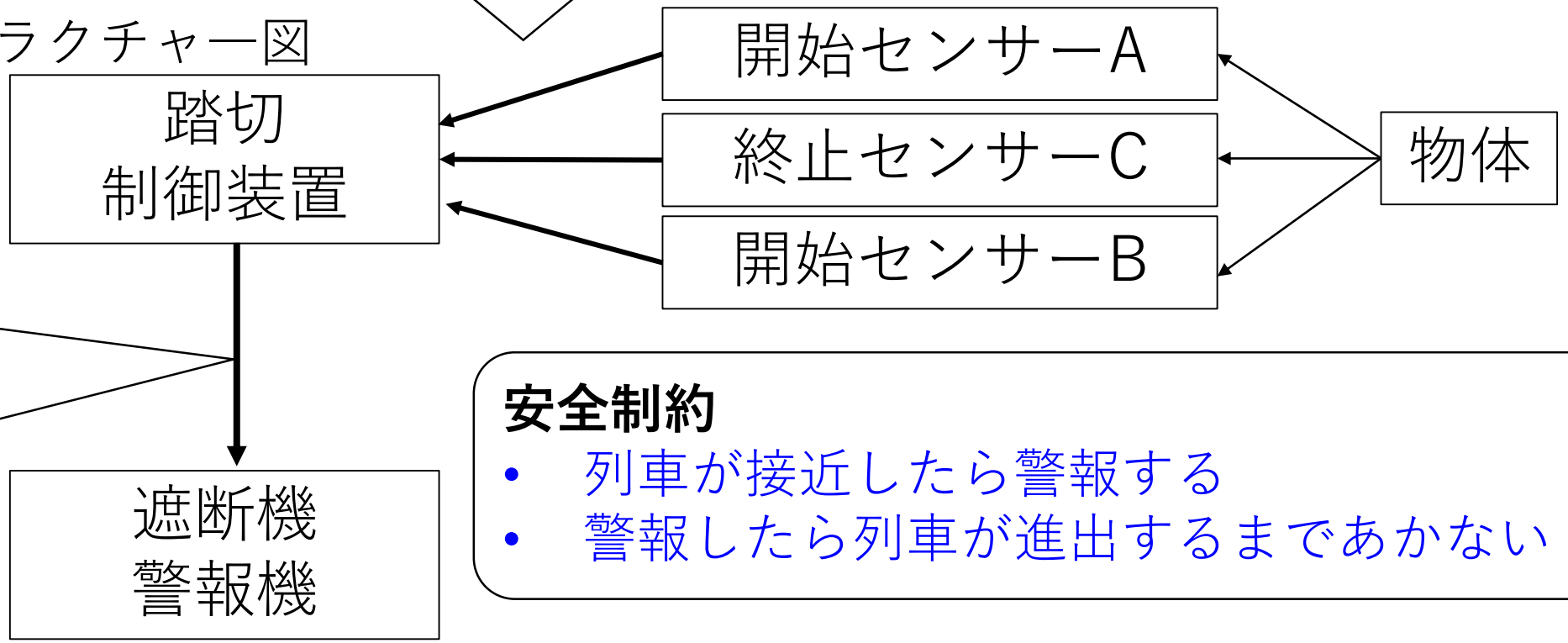
コントロールストラクチャー図



1．これまでのJR東日本の取り組み



コントロールストラクチャー図



ｺﾝﾄﾛｰﾙｱｸｼｮﾝ

- 鳴動開始
- 鳴動停止
- マスク開始
- マスク解除

安全制約

- 列車が接近したら警報する
- 警報したら列車が進出するまであかない

1．これまでのJR東日本の取り組み

4つのｺﾝﾄﾛｰﾙｱｸｼｮﾝ
- 警報開始
- 警報停止
- マスク開始
- マスク解除

２つの安全制約
- 列車が接近したら警報する
- 警報したら列車が進出するまで開かない

6つの危険誘発要因
- 列車接近しても警報開始しない
- 警報開始前に列車が踏切に到着
- 警報開始したのち途中で警報停止
- 不正なマスク開始指示
- マスク解除遅れ
- マスク解除もれ

17個のハザードシナリオ

1．これまでのJR東日本の取り組み

導出されたハザードシナリオの例

例①　センサーAが故障して、Aから踏切制御装置への通知が届かない
→　JRで実施されていた対策：開始センサー故障時は警報する**システム構成**。

例②　Bを通過したのにマスク解除指示が来ないと、次列車で警報しない
→　JRで実施されていた対策：
一定時間以上マスク継続した場合は、**故障とみなして警報する論理。**

例③　Aからきた列車がCを折り返してA方向に引き返す。
→　JRで実施されていた対策：退行する場合は、**特別な取扱いマニュアル**に従う。

例④　Aから来た列車がCに到達する前に、外乱（金属物等）がCで検知。
→　JRで実施されていた対策：
Cを踏切道から**20メートル以上離して施工し**、外乱を減らす。

1．これまでのJR東日本の取り組み

考察と新たな取り組み

システム構成、警報論理、取り扱いマニュアル、施工方法等、対策が多岐にわたるハザードシナリオの導出ができた。

1．平易なコントロールストラクチャ図により

①自由な発想による検討の効果の可能性
②運用まで含めた全体俯瞰した検討ができる可能性

↓

従来の安全性検証との併用により、検討の抜け漏れを防止する効果の期待

↓

システム適用可否検討のケーススタディに活用して検証。

○無線タイマー式踏切制御装置とは

「踏切制御装置の種類」

①　地上式踏切制御装置

→　地上に設置されたセンサにて、警報を制御

②　無線式踏切制御装置

②-1　ATACS型　無線式踏切制御装置

→　列車内の位置情報と線路DBより警報位置を検出して無線で踏切警報を制御

－世界唯一の無線制御踏切制御装置

－列車位置ベース

②-2　無線タイマー式踏切制御装置

－列車位置と警報想定時刻による警報制御

（現在、信号メーカで検証中）

今後の活用可否を検討するため、ケーススタディを実施

○無線タイマー式踏切制御装置とは

「**各方式のメリット・デメリット**」

①　地上式踏切制御装置

○　実績のある制御論理、検知装置・ケーブルを用いた確実な制御

×　重厚な設備となるため、設備の維持・管理費用が大きい
雷や落ち葉など環境変化により、警報持続となることが多数
（復帰作業も手間がかかる）

②　無線式踏切制御装置

○　地上設備を最小限にできる可能性

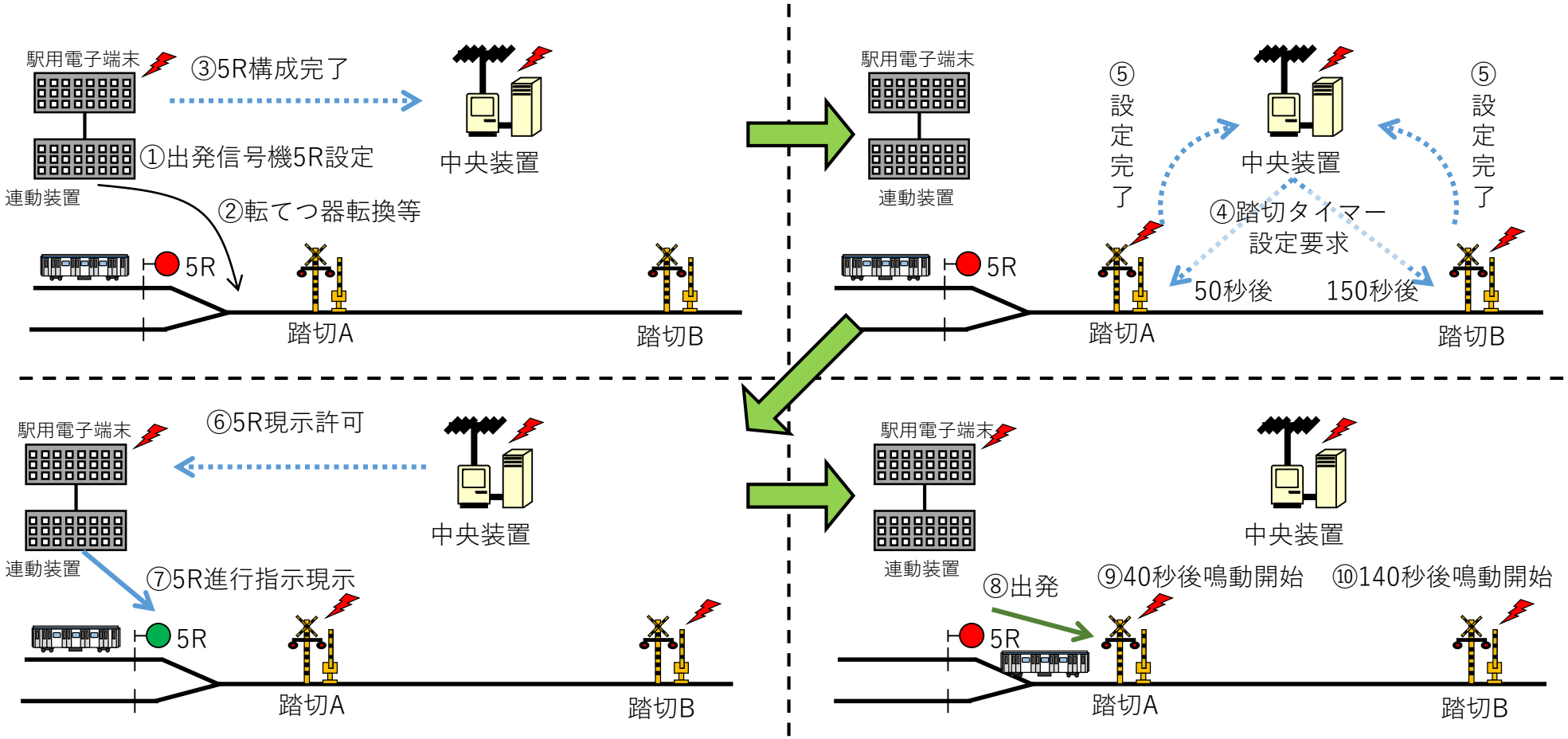
×　汎用無線通信の利用による伝送遅延や途絶による無遮断の恐れ
→結局バックアップ設備が必要

タイマー式による、アルゴリズムだけでの実現の可否を検討

2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○無線タイマー式踏切制御装置とは

【基本機能（タイマー方式）】

①列車が駅を進出する前に、次駅までの全踏切の鳴動時間をセット。（最高速度で設定）
②セットされたのちに信号機に進行指示。
③列車位置を無線で送信し、タイマー時刻を補正。（警報遅延制御）



2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○無線タイマー式踏切制御装置とは

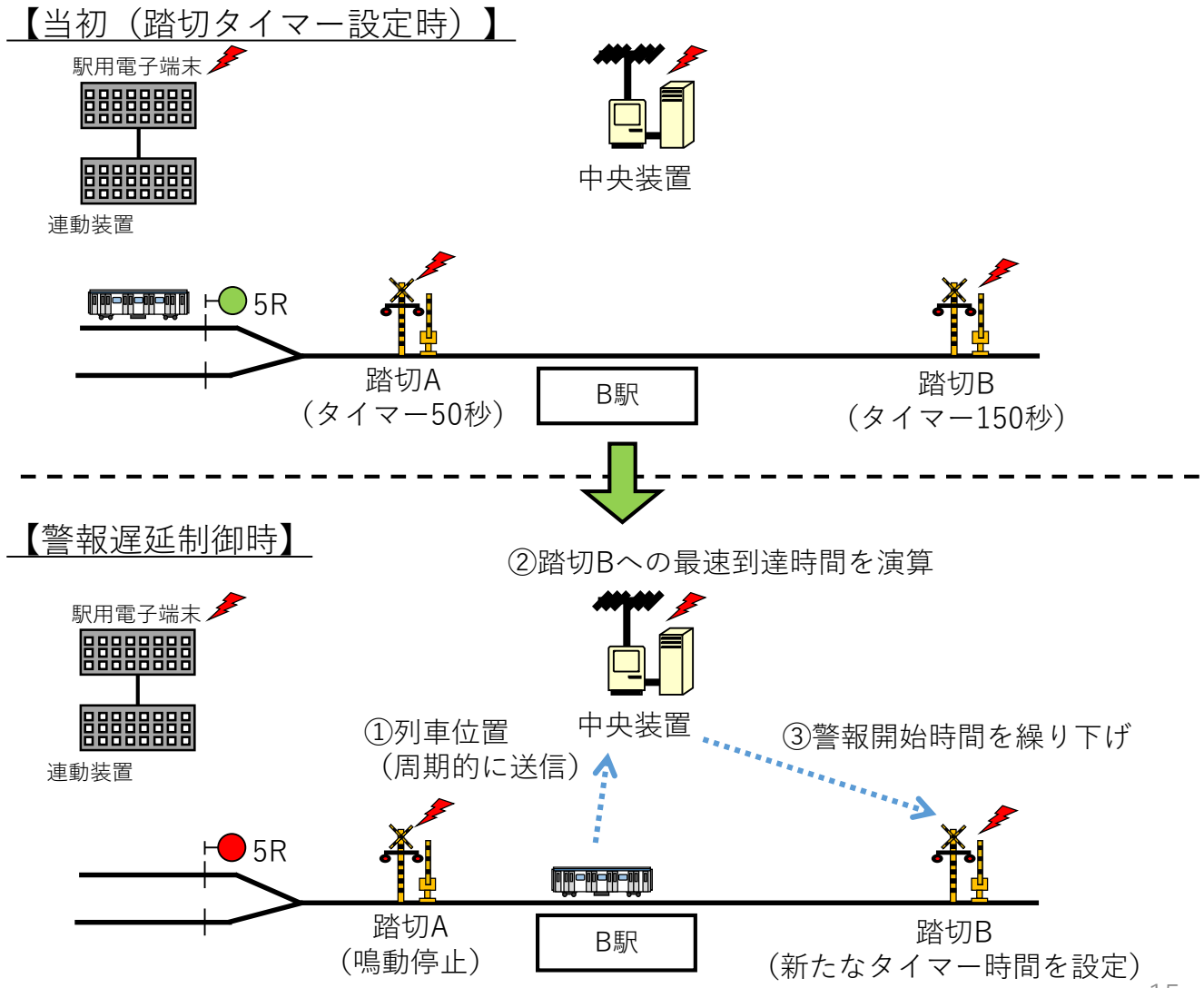
【警報遅延制御】

踏切タイマーは、列車が最速で当該踏切に到達する時間をセット

⇒列車が踏切までに駅停車や徐行等を行うと、警報時間が長くなる可能性あり

⇒列車の現在位置に基づき、警報開始時間を繰り下げ（新たなタイマー時間を設定）

※途中列車との通信が断絶しても、当初の踏切タイマー設定時の時間に応じて、実際に列車が踏切に到達するよりも「早めに踏切が鳴動する」だけで、不安全側事象にはならない



２．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

今回は、検討段階におけるハザード解析に

① STAMP/STPAによる検証

② FTA (Fault Tree Analysis)による検証

を同時並行して実施して、結果を比較。**完璧を求めず、淡々と実施して比較。**

STAMP/STPAで悩むところ

コントロールストラクチャ作成が難しい。

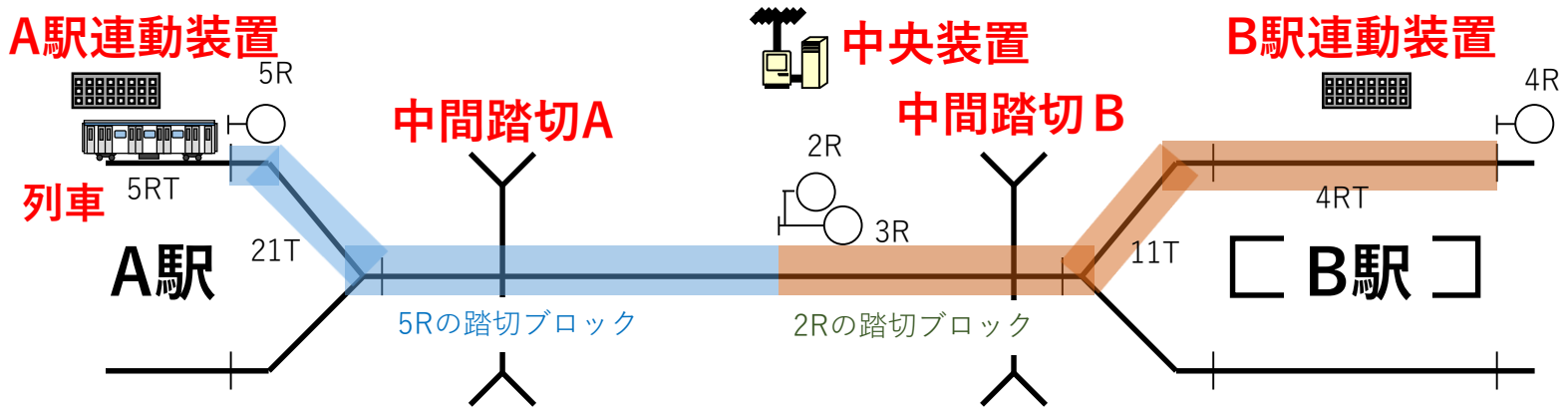
・シンプルな構成にしようとしても難しい。
・いろいろな意見があり、どれも正解に思える。
・このストラクチャで正しい答えが出るのか不安。

→一意に決めようとすると非常に時間がかかる。

システムが正常動作するシナリオを作って、シーンごとにコントロールストラクチャを作成して実施。

2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「踏切機能のシナリオ策定」
各装置間（列車、連動装置、踏切）でのやりとりについて
正しく動作する場合のシナリオを作成
※列車はA駅発、B駅停車



No.1　中央装置からA駅連動装置に5R進路設定要求、
A駅連動装置で5R進路構成を行い、中央装置に進路構成設定完了を通知

No.2　中央装置から中間踏切に踏切タイマー設定要求、
中間踏切で踏切タイマー設定を行い、中央装置に踏切タイマー設定完了を通知

No.3　中央装置からA駅連動装置に5Rの進行現示許可を通知、
A駅連動装置で5Rに進行を現示

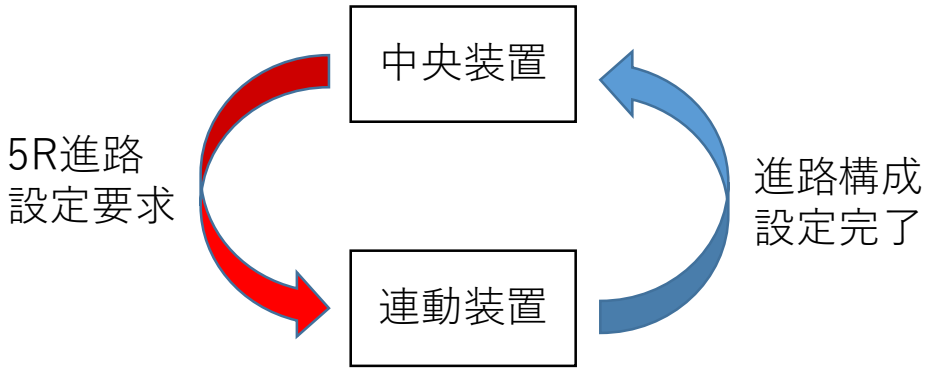
No.4　列車がA駅から発車、5R内方に進入（駅中間に進出）

No.5　中央装置から中間踏切に警報遅延設定要求、
中間踏切で警報遅延設定を行い、中央装置に警報遅延設定完了を通知

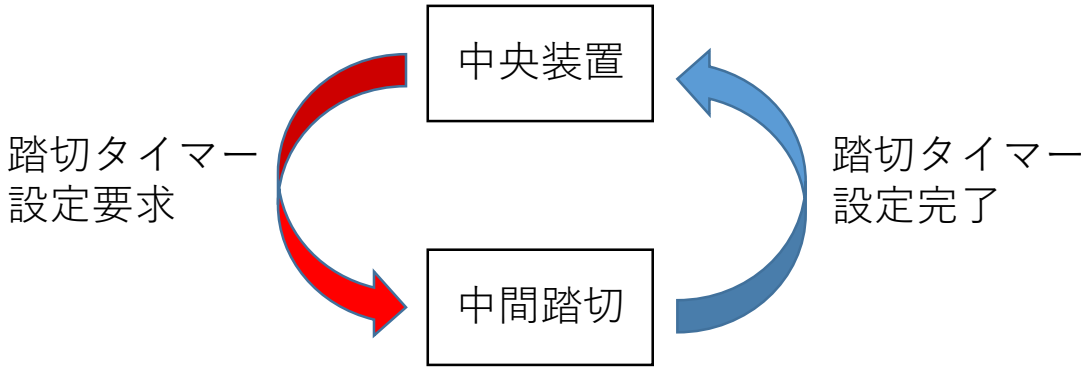
2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「**コントロールストラクチャー図をシナリオごとに作成**」
各装置間（列車、連動装置、踏切）でのやりとりについて
シナリオごとにコントロールストラクチャー図を作成、検討を実施

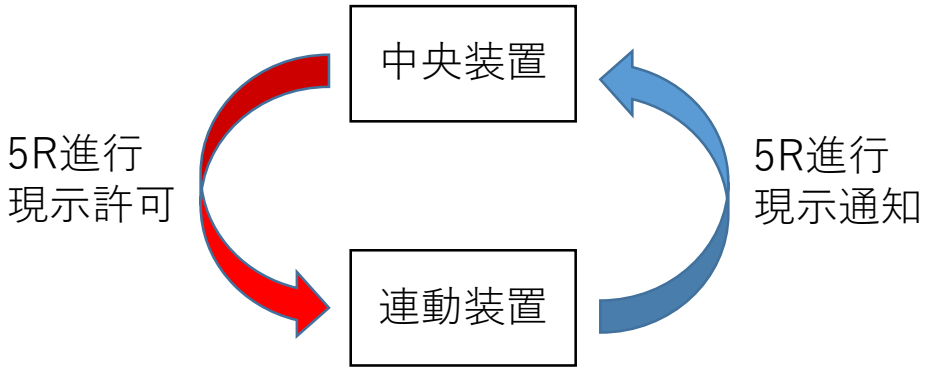
No.1



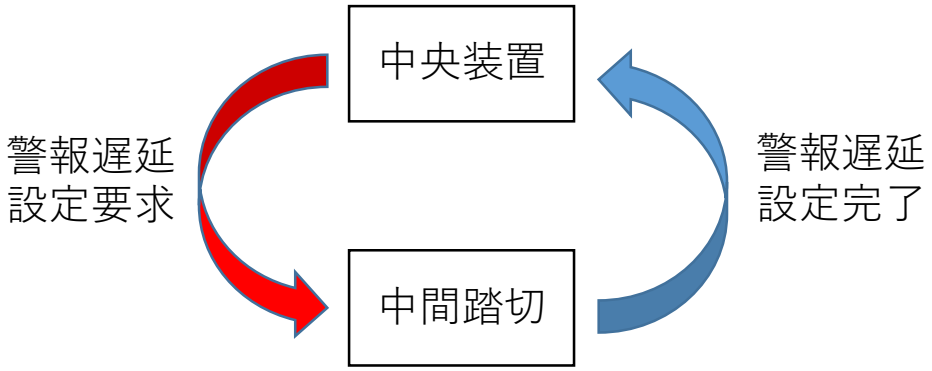
No.2



No.3



No.4



2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「非安全なコントロールアクション（UCA）の抽出」

シナリオで示した情報のやりとりをコントロールアクションと定義し、
４種類のガイドワードを適用し、５種類のUCAを抽出

コントロールアクション（与えられる情報）	イベント元→イベント先	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、長すぎる適用でハザード
①現在距離程・車両ID送信（距離程、車両ID）	列車・車上装置→中央装置	情報が与えられない→列車位置が把握できない	A)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）	情報が遅めに与えられる→警報遅延設定が遅れる（タイマー時間を情報	
②定周期ポーリング（位置要求）送信（車両ID）	中央装置→列車・車上装置	情報が与えられない→列車位置が把握できない	誤った情報が与えられる→位置要求した列車と照合結果が不一致となる	情報が遅めに与えられる→警報遅延設定が遅れる（タイマー時間を情報	
③5R進路設定要求（進路名）	中央装置→A駅連動装置	情報が与えられない→5R進路構成がされない	誤った情報が与えられる→5R進路構成がされない	情報が早め、遅めに与えられる→5R進路構成が早まる、遅れる	
④5R進路構成完了通知（進路名）	A駅連動装置→中央装置	情報が与えられない→踏切タイマー設定要求がされない	誤った情報が与えられる→設定要求した進路と照合結果が不一致となる	情報が遅めに与えられる→踏切タイマー設定要求が遅れる	
⑤踏切タイマー設定要求（踏切番号、車両ID、タイマー時間）	中央装置→中間踏切A	情報が与えられない→踏切タイマーが設定されない	B)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）	情報が遅めに与えられる→踏切タイマー設定完了が遅れる	
⑥踏切タイマー設定完了通知（踏切番号、タイマー時間）	中間踏切A→中央装置	情報が与えられない→5R現示が許可されない	C)タイマー設定がされていないにも関わらず、タイマー設定完了が通知される→無しゃ断	情報が遅めに与えられる→5R現示許可が遅れる	
⑦5R現示許可通知（進路名）	中央装置→A駅連動装置	情報が与えられない→5Rの現示がされない	誤った情報が与えられる→現示許可した信号機と照合結果が不一致となる	情報が遅めに与えられる→列車進出が遅れる	
⑧列車進出・5R内方進入通知（車両ID、軌道回路条件）	列車→中央装置	情報が与えられない→車両IDが駅中間に遷移しない	誤った情報が与えられる→列車在線位置が正しく把握できなくなる	情報が遅めに与えられる→車両IDの駅中間への遷移が遅れる	
⑨警報遅延設定要求（踏切番号、車両ID、タイマー時間 or 遅延時間）	中央装置→中間踏切A	情報が与えられない→警報遅延が設定されない（警報開始時間が早いままとなる）	D)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）	情報が遅めに与えられる→警報遅延設定が遅れる（タイマー時間を情報	
⑩警報遅延設定完了通知（踏切番号、車両ID、タイマー時間）	中間踏切A→中央装置	情報が与えられない→⑦は一定時分ごとに繰り返される（再試行回数の限度による異常検知を設け	誤った情報が与えられる→警報遅延設定要求した情報と照合結果が不一致となる		
⑪踏切A警報開始情報通知（踏切番号）	中間踏切A→中央装置	情報が与えられない→踏切Aパターンが消去されず、列車にパターンに応じたブレーキがかかる	誤った情報が与えられる→踏切Aパターンが消去されず、列車にパターンに応じたブレーキがかかる		
⑫踏切A警報開始情報通知（踏切番号）	中央装置→列車	情報が与えられない→踏切Aパターンが消去されず、列車にパターンに応じたブレーキがかかる	誤った情報が与えられる→踏切Aパターンが消去されず、列車にパターンに応じたブレーキがかかる		
⑬踏切A警報停止要求（踏切番号）	中央装置→中間踏切A	情報が与えられない→鳴動持続になる	E)誤った情報が与えられる→不適切なタイミングで踏切警報停止（無しゃ断を含む）	情報が遅めに与えられる→踏切警報停止が遅れる	
⑭警報停止完了通知（踏切番号）	中間踏切A→中央装置				

2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「非安全なコントロールアクション（UCA）の要因の検討」

抽出したUCAの要因として、各装置の故障やその他の要因を検討

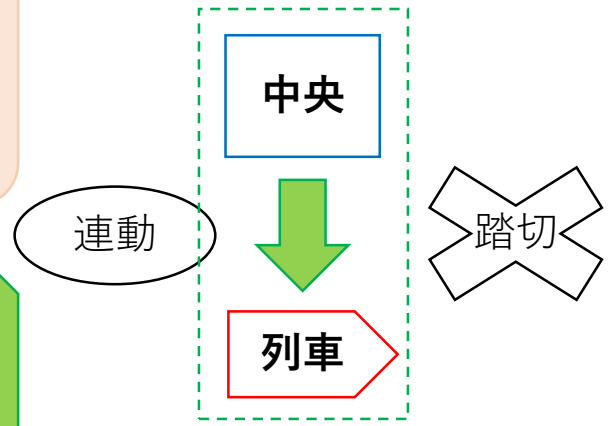
コントロールアクション（与えられる情報）	イベント元→イベント先	UCA	UCAの要因
①現在距離程・車両ID送信（距離程、車両ID）	列車・車上装置→中央装置	A)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）	「α．列車位置算出の誤り」 「β．データの誤り」 ・列車・車上装置の故障 ・中央装置の故障 ・携帯端末（列車・車上装置側 or 中央装置側）の故障 「γ．データの改ざん（セキュリティリスク）」
⑤踏切タイマー設定要求（踏切番号、車両ID、タイマー時間）	中央装置→中間踏切A	B)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）	「α．データの誤り」 ・中央装置の故障 ・中間踏切の故障 ・携帯端末（中央装置側 or 中間踏切側）の故障 「β．データの改ざん（セキュリティリスク）」
⑥踏切タイマー設定完了通知（踏切番号、タイマー時間）	中間踏切A→中央装置	C)タイマー設定がされていないにも関わらず、タイマー設定完了が通知される→無しゃ断	・中間踏切の故障
⑨警報遅延設定要求（踏切番号、車両ID、タイマー時間 or 遅延時間）	中央装置→中間踏切A	D)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）	・UCAのA)と同様
⑬踏切A警報停止要求（踏切番号）	中央装置→中間踏切A	E)誤った情報が与えられる→不適切なタイミングで踏切警報停止（無しゃ断を含む）	「α．データの誤り」 ・中央装置の故障 ・中間踏切の故障 ・携帯端末（中央装置側 or 中間踏切側）の故障 「β．データの改ざん（セキュリティリスク）」

2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「非安全なコントロールアクション（UCA）および要因の例（その１）」

コントロールアクション（与えられる情報）	イベント元→イベント先	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	早過ぎる停止、長すぎる適用でハザード
①現在キロ程・車両ID送信（キロ程、車両ID）	列車・車上装置→中央装置	情報が与えられない→列車位置が把握できない	**A)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）**	情報が遅めに与えられる→警報遅延設定が遅れる(タイマー時間を情報提供していれば問題はない)	

【UCA】 列車のキロ程（現在位置）もしくは車両ID（識別番号）が誤って伝わると、当該踏切に接近する列車を中央装置が正しく認識できず、踏切に対して正しい踏切タイマーを設定できない
⇒正しいタイミングで踏切が警報開始されない（最悪無しゃ断！）



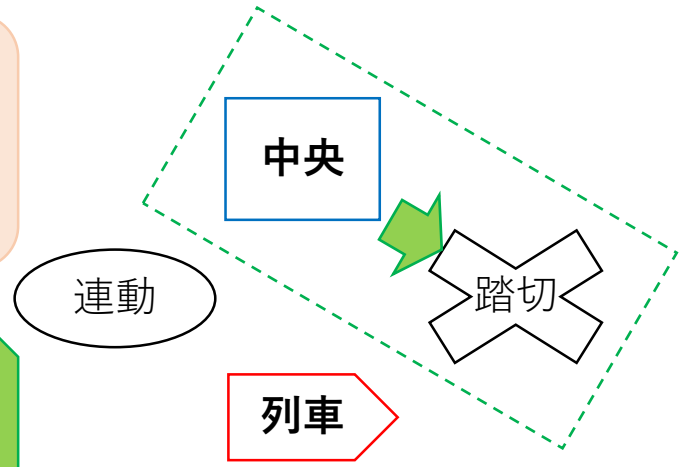
【HCF： UCAの要因】
「α．列車位置算出の誤り」
「β.データの誤り」 ・列車・車上装置の故障
・中央装置の故障
・携帯端末（列車・車上装置側 or 中央装置側）の故障
「γ.データの改ざん（セキュリティリスク）」

2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「非安全なコントロールアクション（UCA）および要因の例（その２）」

コントロールアクション（与えられる情報）	イベント元→イベント先	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	早過ぎる停止、長すぎる適用でハザード
⑤踏切タイマー設定要求（踏切番号、車両ID、タイマー時間）	中央装置→中間踏切	情報が与えられない→踏切タイマーが設定されない（出発信号機に進行現示を出さないので問題はない）	**B)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）**	情報が遅めに与えられる→踏切タイマー設定完了が遅れる	

【UCA】 タイマー時間が誤って伝わると、踏切で誤ったタイマー時間が設定される
⇒正しいタイミングで踏切が警報開始されない（最悪無しゃ断！）



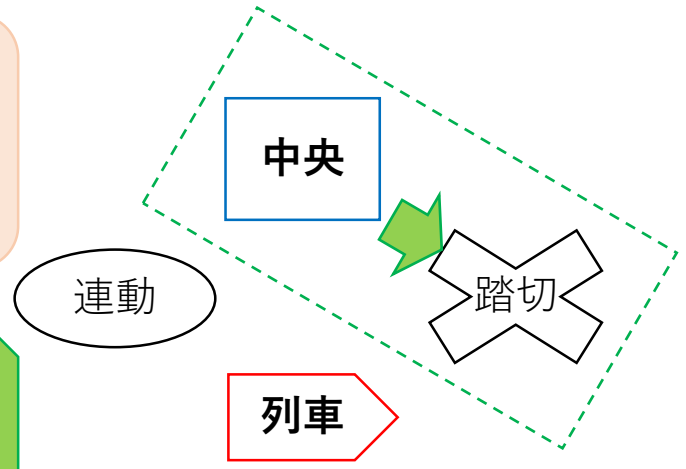
【HCF：UCAの要因】
「α.データの誤り」
・中央装置の故障
・中間踏切の故障
・携帯端末（中央装置側 or 中間踏切側）の故障
「β.データの改ざん（セキュリティリスク）」

2．ケーススタディ「無線タイマー式踏切制御装置を導入するとしたら」
○STAMP/STPAによる検証

「非安全なコントロールアクション（UCA）および要因の例（その３）」

コントロールアクション（与えられる情報）	イベント元→イベント先	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	早過ぎる停止、長すぎる適用でハザード
⑨警報遅延設定要求（踏切番号、車両ID、タイマー時間）	中央装置→中間踏切	情報が与えられない→警報遅延が設定されない（警報開始時間が早いままとなるだけで問題はない）	**D)誤った情報が与えられる→不適切なタイミングで踏切警報開始（無しゃ断を含む）**	情報が遅めに与えられる→警報遅延設定が遅れる（タイマー時間を提供しており問題はない）	

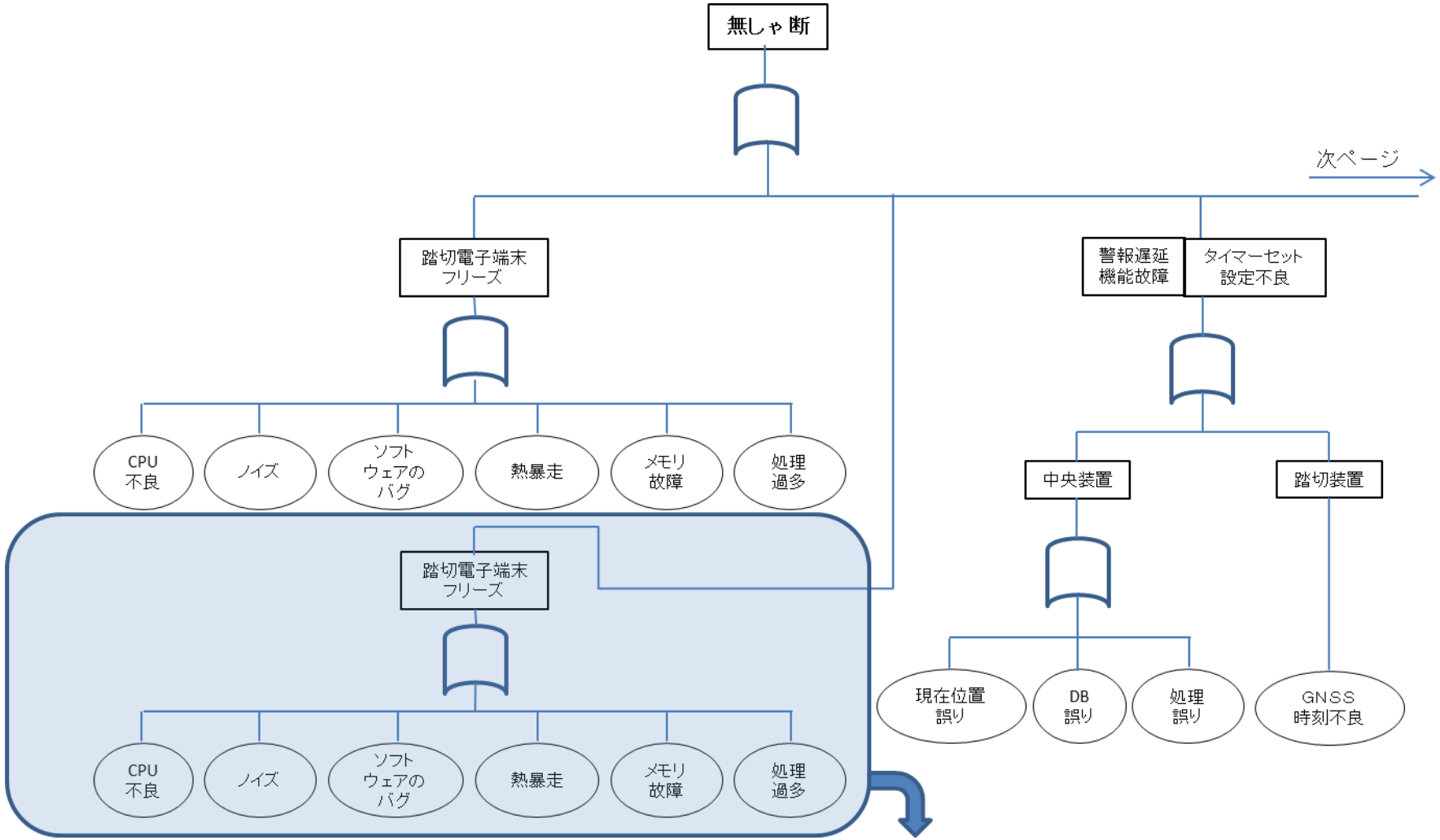
【UCA】 警報遅延設定としてタイマー時間が誤って伝わると、踏切で誤ったタイマー時間が設定される
⇒正しいタイミングで踏切が警報開始されない（最悪無しゃ断！）



【UCAの要因】
「α.データの誤り」
・中央装置の故障
・中間踏切の故障
・携帯端末（中央装置側 or 中間踏切側）の故障
「β.データの改ざん（セキュリティリスク）」

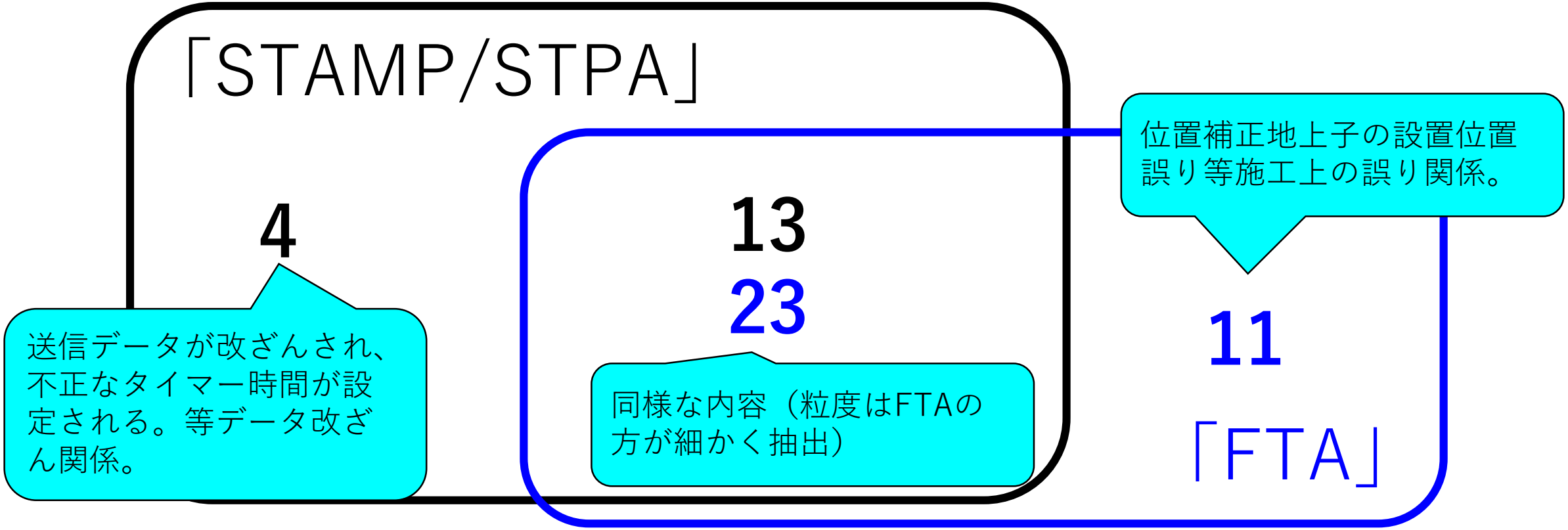
3．考察
○FTAとの比較

「**FTAによる検証結果**」
“無しゃ断”をトップ事象として、無しゃ断に至る不具合事象を抽出



3．考察
○FTAとの比較

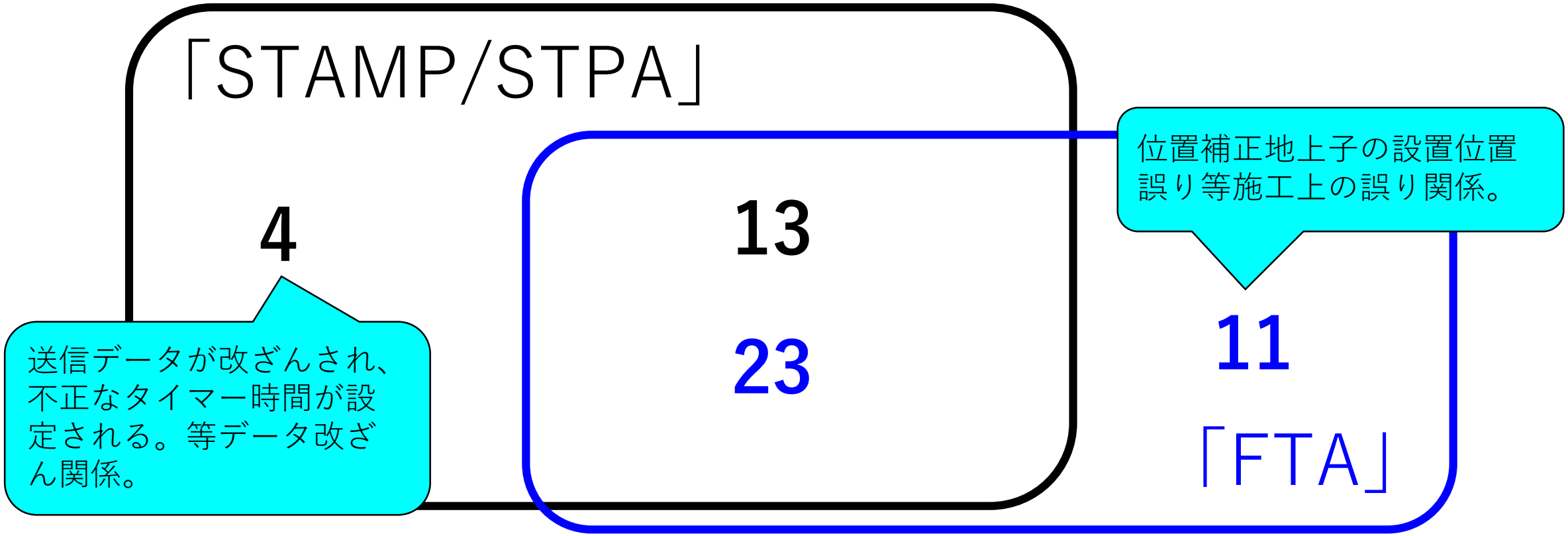
- FTAは全34事象抽出。FTAは装置構成毎をにらみながら事象を検討。踏切のプロからすると、具体的な想定事象項目を多く抽出。今回は施工不良などがFTAのみで抽出された。
- STAMP/STPAは全17事象抽出。コントロールストラクチャがシンプルなため、集約された。今回はデータ改ざん関連の事象がFTAとは外れて抽出された。



3．考察
○FTAとの比較

今回は、何も前提なしにハザード解析を実施したが、ガイドワードの活用により、どちらの方法でも抽出された可能性大。

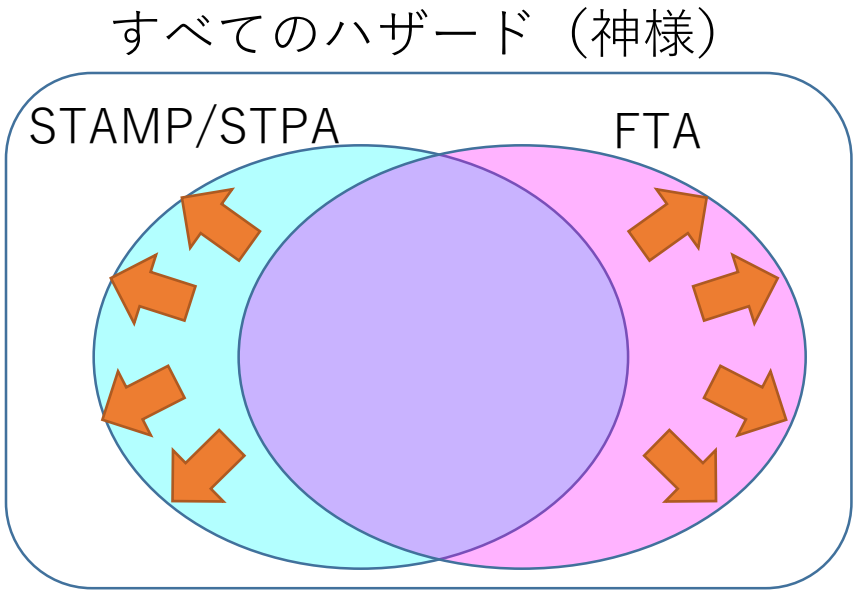
・人的オペレーションのあまり入らない踏切の制御シナリオで実施したため、差が少なかった
・オペレーションが多く入るシナリオのシステムではSTAMP/STPAの効果が出るのではないか
・シナリオシーン毎のSTAMP/STPAは、構造検討の時間がかからず、気軽にできてよかった。



４．まとめ

鉄道の安全性検証にSTAMP/STPA解析をつかってみて

- シナリオ毎のコントロールストラクチャによる検討を採用。簡易で、気軽にハザード要因が抽出できた。
- 従来の安全性解析手法FTAとの組み合わせにより、より効果を発揮する可能性を感じた。



ソフトウエアによる安全システムの拡大は、ハザード要因の複雑化、想定外事象増大につながっている。
ハザード要因抽出の拡大のため、有用な安全解析手法の活用および、ブラッシュアップが重要だと感じた。

ご清聴ありがとうございました。