15

新しい列車制御システムを対象とした安全解析について

交通システム研究部　　※工藤　希　長谷川智紀　林田　守正

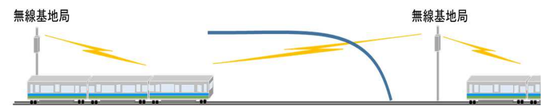
はじめに

- 鉄道システムに用いる装置の新設、改造等の際，技術的観点からおこなう安全性評価を実施する場合がある
  交通研では、主に鉄道信号システムの設計安全性評価に関し、国際規格との整合性を考慮した評価を実施
- 無線式列車制御システムなどの近年の複雑化した鉄道信号システムに対応するため、従来の安全性評価手法に加え、近年提案された新しい評価手法の検討が必要

無線式列車制御システムと安全性評価のポイント

- 列車位置等の伝送に無線を使う無線式列車制御システムは導入・検討が進んでいるところ
- 輸送密度等によって様々なシステムが想定される

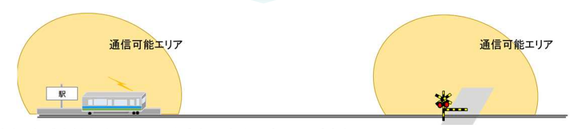
【安全性評価の主なポイント】
① 軌道回路式の安全性と同等の列車在線検知，閉そくの確保
② 無線通信の信頼性，安定性
③ 車上装置／地上装置の故障による影響と非安全事象の発生頻度
④ 無線通信途絶時の安全性担保
⑤ 制御データ伝送の確実性
⑥ 無線通信に関するセキュリティ
⑦ 国際規格との関連



都市鉄道向けの高頻度運行を可能とするシステム

- ✓ 地上装置に起因する輸送障害の減少
- ✓ 高頻度運行が可能
- ✓ 遅延回復効果が高い

路線ごとに様々な装置構成が想定される



地方鉄道向けの低頻度運行を前提としたシステム

- ✓ 地上設備の簡素化
- ✓ 保守の効率化・省力化に期待

安全解析手法の選定

これまでのFTA/FMEAは、多大な実績を有するが、機器の相互作用及び時間的遷移を伴うなどの複雑な事象の解析が難しい

	FMEA/FTA	STAMP/STPA
手順	FMEAにより、システムに起こりうる故障モードを予測し、考えられる原因や影響を事前に解析・評価し、その結果、発生が好ましくない事象に対して、FTAにより評価する	ハザードはシステムの中で安全のための制御をおこなう要素（コントローラ）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によって起きるというアクシデントモデル
メリット	部品レベルまで細分化して分析できるため、深い分析が可能	マクロな視点で機器の相互作用及び時間的遷移を含む解析を得意とする
デメリット	機器の相互作用及び時間的遷移を伴う等複雑な事象の解析に難	部品レベルに遡る解析には作業が膨大となることが想定される

STAMP…System Theoretic Accident Model and Processes
STPA…STAMP based Process Analysis
FMEA…Failure Mode and Effects Analysis　FTA…Fault Tree Analysis

➡今回はSTAMP/STPAを実施

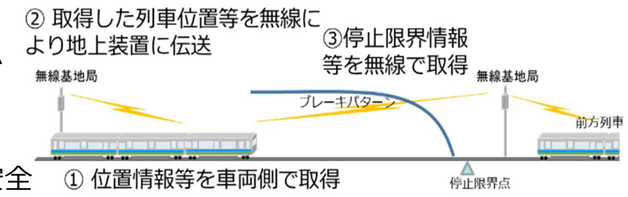
情報処理推進機構,"はじめてのSTAMP/STPA"
https://www.ipa.go.jp/sec/reports/20160428.html

無線式列車制御システムを対象としたSTAMP/STPAの試行

- 簡易的なモデルを対象として試行
- STAMP/STPAを行うことで、システム全体のどこに安全上の課題があるのか、俯瞰することができることがわかる

アクシデント・ハザード・安全制約の識別
↓
コントロールストラクチャを構築
↓
UCA(Unsafe Control Action)を抽出
↓
UCA毎にHCF (Hazard Causal Factor)を特定

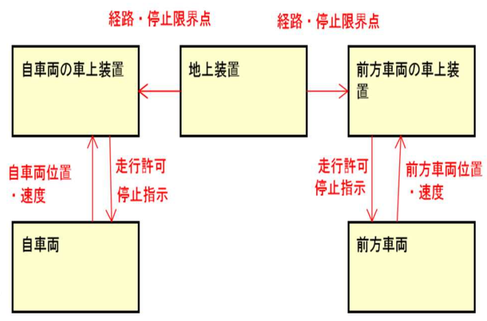
今回の対象としたシステム



アクシデント・ハザード・安全制約の一覧表（抜粋）

アクシデント	ハザード	安全制約
(A1) 前方列車との衝突	(H1) 停止すべきタイミングで停止指示がでない	(SC1)停止すべきタイミングで停止指示がでなければならない

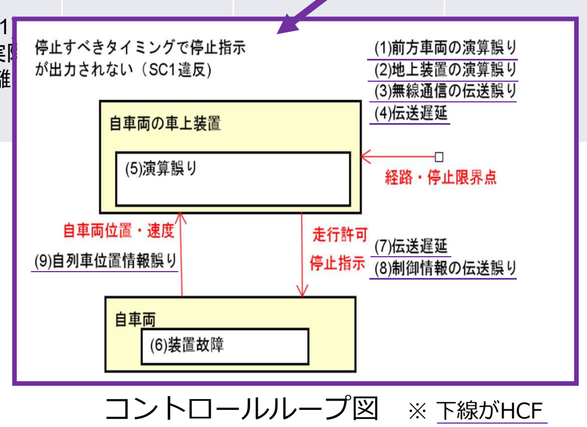
④停止限界情報等によりブレーキパターン演算・制御



コントロールストラクチャ

UCA抽出一覧表（抜粋）

No	CA	From	To	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	走行許可	自車両の車上装置	自車両	列車が停止	(UCA1-P-1) 停止すべきタイミングで走行許可が出る[SC1]	(UCA1-T-1) 停止すべきタイミングで走行許可が出る[SC1] 列車が停止し続ける	走行許可が出ない (UCA1-D-1) 停止すべきタイミングで走行許可がでる[SC1]
2	停止指示	自車両の車上装置	自車両	(UCA2-N-1) 停止すべきタイミングで列車が走行できる [SC1]	列車が停止	列車が停止し続ける (UCA2-T-1) 停止すべきタイミングまでに停止指示が出ない[SC1]	(UCA2-D-1) 停止すべきタイミングに停止指示が出ない[SC1] 列車が停止し続ける
3	自車両位置・速度	自車両	自車両の車上装置	(UCA3-N-1 上位置と実際位置が乖離 [SC1]			



コントロールループ図　※ 下線がHCF

新しい列車制御システムに対する安全性評価を実施する際の主な課題

- 評価基準は何か
  "従来の装置と同等かそれ以上"の判断が難しい
  定量的な安全性の算定方法と、基準値の設定をどうするか？
- 「境界」で抜け漏れを起こさない工夫
  評価対象装置と対象外装置とのインターフェース
  事業主体とメーカとの責任分担
  議論を重ねて抜け漏れを減らしていくことに意味があるため、評価には手間と時間がかかる

おわりに

- 近年導入・検討が進んでいる無線式列車制御システムに対して、設計安全性評価を行うための課題を整理し、STAMP/STPAを用いたリスク分析の一例を示した
- その結果、システム全体のどこに安全上の課題があるのか俯瞰できるため、新しいシステムには有用であることがわかった
- 今後は新しい列車制御システムに対する安全性評価手法を確立することを目標に検討を進めていきたい