新しい列車制御システムに対応した安全性評価手法に関する取組

交通システム研究部　主任研究員　工藤 希

講演内容

1. はじめに
2. 背景
3. 安全性評価
4. 新しい列車制御システムに対応する安全性評価手法の検討
5. まとめ

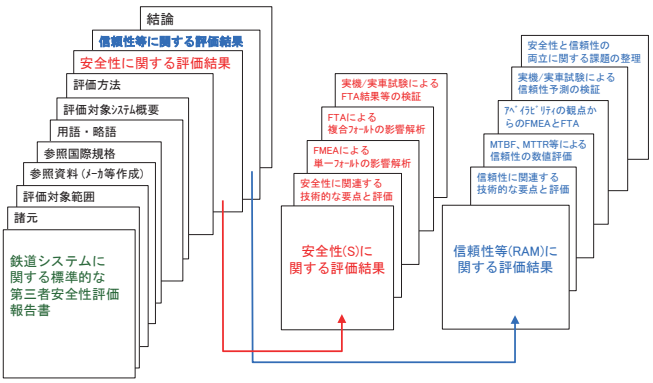
1．はじめに

- 交通安全環境研究所は鉄道技術に関する第三者機関としての安全性評価に数多く取り組んできた
- その中で、国内外の列車制御システムに対する安全性評価にも対応
- 近年では、新しい列車制御システムの導入検討が進んでいる

⇨ 新しい列車制御システムに対応する安全性評価手法と、今後の方向性について検討を行った

2．背景

- 鉄道信号分野における安全性評価は、新しいシステムや改修したシステムに対して、技術的な観点から、安全上の問題がないかについて評価をおこなうもの
- 鉄道システムの輸出に際し、その安全性を相手先に証明する方法として、第三者評価（安全性評価又は機能安全関連の国際規格への適合性評価／認証）を受けることが一般化
- 第三者評価には、規格適合性評価、認証と、技術的な安全性評価に大別
- 第三者による技術的な安全性評価も、機能安全性関連の国際規格を参照して行われることが多い

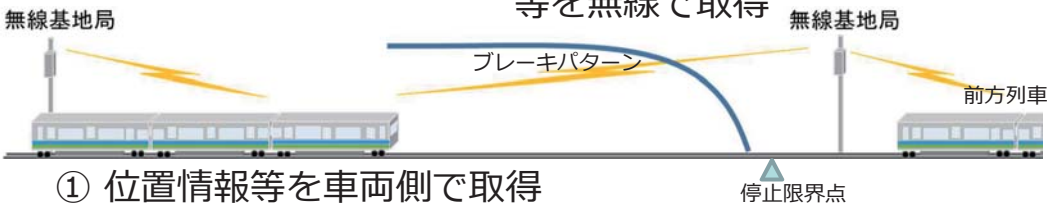


2．背景

近年では、無線を使った新しい列車制御システム（CBTC、ATACS等）の導入・検討が進んでいる

② 取得した列車位置等を無線により地上装置に伝送

③停止限界情報等を無線で取得



① 位置情報等を車両側で取得

④停止限界情報等により
ブレーキパターン演算・制御

新しい列車制御システムに対応した安全性評価手法の確立が必要

3．安全性評価

鉄道信号分野における安全性評価※は、新しいシステムや改修したシステムに対して、技術的な観点から、安全上の問題がないかについて評価をおこなうもの

※機能安全関連の国際規格への適合性評価／認証も広義の安全性評価に含まれるが、本報告ではこの定義に基づく。

新しいシステムや
改修したシステム等

事業者・メーカ等が作成した、
システムの技術内容及び
設計仕様等に対し、
リスク分析に基づいた
定量的評価や、システムの
安全管理にかかわる
定性的な評価などを行なう

設計安全性評価

3．安全性評価

設計安全性評価の基本的な手順

① 対象とする段階、範囲等を決定

Ex) 走行試験等の有無、評価済み装置等との差異の確認

② 評価対象資料の確認

- 設計図書
- リスク解析結果

…ハザード分析、FMEA/FTA等

3．安全性評価

FMEA（Failure Mode and Effects Analysis）：
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・評価する手法

FMEAの例

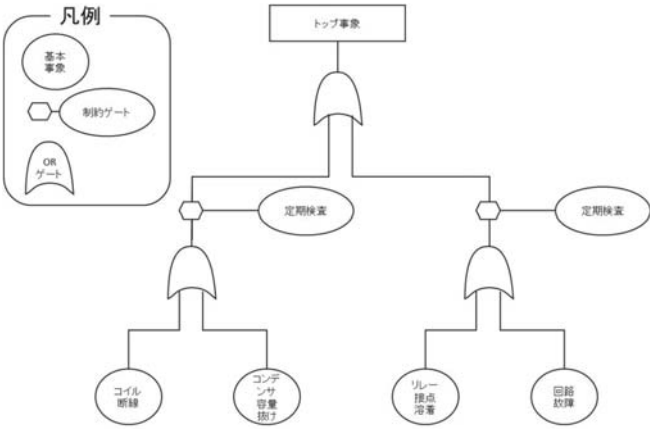
アイテム	機能	故障モード	故障影響	故障原因	対策前			低減策	対策後		
					頻度	深刻度	リスクレベル		頻度	深刻度	リスクレベル
例) 機器A	速度照査機能	速度認識誤り	列車どうしの衝突	ハードウェア故障	低い	重大	望ましくない	多重系構成を採用、故障診断機能を付加	起こり得ない	重大	許容できる
…											

故障の影響の発生頻度と深刻度のレベルとのマトリクスの例

頻度	深刻度のレベル			
	I：重要でない	II:軽微	III: 重大	IV:壊滅的
5：頻繁に起こる	望ましくない	許容できない	許容できない	許容できない
4：起こり得る	許容できる	望ましくない	許容できない	許容できない
3：時々起こる	許容できる	望ましくない	望ましくない	許容できない
2：低い	無視できる	許容できる	望ましくない	望ましくない
1：起こり得ない	無視できる	無視できる	許容できる	許容できる

3．安全性評価

FTA（Fault Tree Analysis）：
発生が好ましくない事象に対して、その事象を引き起こす要因を連鎖的に展開し、因果関係を樹形図に図示し、対策を打つべき発生経路および発生要因、発生確率を解析する手法



FTAの例

4．新しい列車制御システムに対応する安全性評価手法の検討

- 列車位置等の伝送に無線を使う等、新しい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

都市鉄道向け無線式列車制御システム（CBTC）
仕様共通化検討会とりまとめ
https://www.mlit.go.jp/common/001394016.pdf

都市鉄道向けの高頻度運行を可能とするシステム

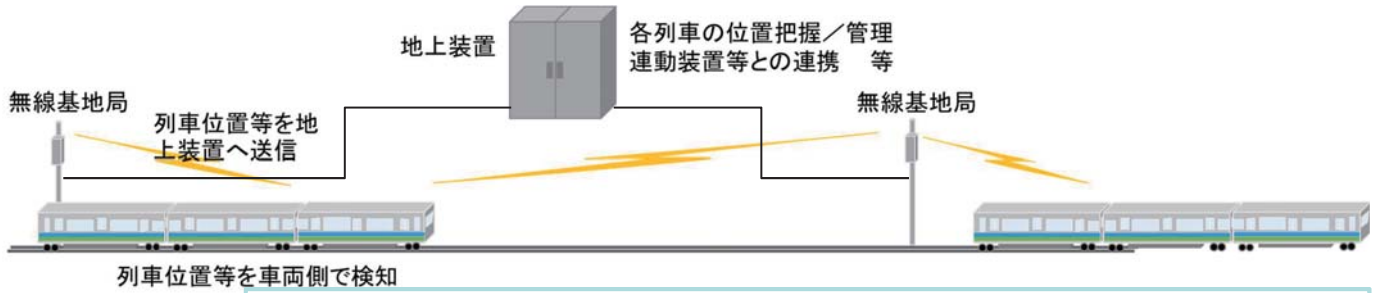
地上装置に起因する輸送障害の減少
高頻度運行が可能
遅延回復効果が高い

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

4. 新しい列車制御システムに対応する安全性評価手法の検討



【安全性評価の主なポイント】
- 軌道回路式と同等の列車在線検知、閉そくの確保
- 無線通信の信頼性、安定性（ノイズ対策、耐久性等）
- 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
- 無線通信途絶時の安全性担保（衝突／追突防止等）
- 制御データ伝送の確実性（データ変化等のチェック）
- 無線通信に関するセキュリティ（改ざん、なりすまし対策）
- 国際規格との関連
- FMEA/FTA等によるリスク解析

4. 新しい列車制御システムに対応する安全性評価手法の検討

- 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

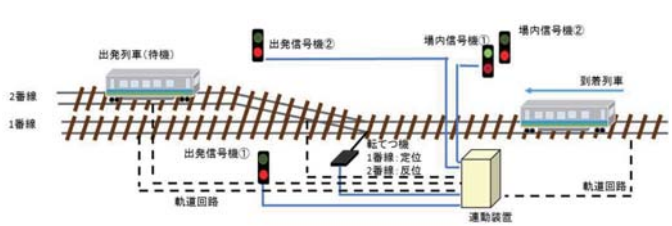
STAMP…System Theoretic Accident Model and Processes
STPA…STAMP based Process Analysis

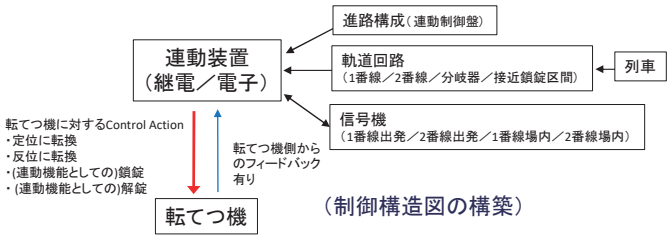
4. 新しい列車制御システムに対応する安全性評価手法の検討

- STAMP/STPAは2012年にマサチューセッツ工科大学のLeveson教授が提唱した要素間の相互作用と動的な遷移を考慮した安全解析手法
- 情報処理推進機構（IPA）の解説書では、踏切を例に解析されている
- 自動車等の他の交通モードにおいても、STPAを実施している事例が増えてきている

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

4. 新しい列車制御システムに対応する安全性評価手法の検討





（制御構造図の構築）

解錠指示　早すぎると　分岐器から進出前の車両が脱線　安全制約「列車が分岐器上に在線中は鎖錠しなければならない」に違反

① 外部からの指示や情報の誤り欠落　HS-17-3 在線情報を誤る　HS-17-4 制御情報を誤る

コントローラ：電子連動装置
②不十分な制御・アルゴリズム　HS-17-1 論理誤りにより誤った解錠指示を出力
④部品故障・経時変化　HS-17-2 故障により解錠指示を出力

コントロールプロセス：転てつ機
④部品故障・経時変化　HP-17-1 故障により指示のない解錠

⑪ 意図しない、又は範囲外の外乱　HP17-2 雷サージによる誤った解錠指示　HP17-3 人為的な転てつ機の転換

ハザード誘発要因	対策
HS-17-1 論理誤りにより誤った解錠指示を出力	設計段階・製造段階での検査
HS-17-2 故障により解錠指示を出力	定期検査
HP-17-1 故障により指示のない解錠	定期検査

簡単な連動装置を対象に解析した例

4. 新しい列車制御システムに対応する安全性評価手法の検討

現時点でRAMS関連規格に明記されている評価手法にはSTAMPは含まれていないものの、手法としてはRAMS関連規格であるIEC 62425において、安全性水準（SIL）の高レベル製品での利用がHR(Highly Recommend)である<u>HAZOPの誘導語をより具体的にしたもの</u>と考えられる

⇨ 今後も活用事例を増やし、検討を進める

HAZOP（Hazard and Operability Studies）
…1960年代、英国ICI社が、自社開発の新規化学プロセスを対象として、誘導語（Guide Word）を使って潜在危険性をもれなく洗い出し、それらの影響・結果を評価し、必要な安全対策を講ずることを目的として開発されたプロセス危険性の特定手法。

IEC　62425（鉄道信号システム）

Table E.6-　Failure and hazard analysis method (referred to in 5.4)

Techniques / Measures	SIL 1	SIL 2	SIL 3	SIL4
Preliminary hazard analysis	HR	HR	HR	HR
Fault tree analysis	R	R	HR	HR
Markov diagrams	R	R	HR	HR
FMECA	R	R	HR	HR
HAZOP	R	R	HR	HR
Cause-consequence diagrams	R	R	HR	HR
Event tree	R	R	R	R
Reliability block diagram	R	R	R	R
Zonal analysis	R	R	R	R
Interface hazard analysis	R	R	HR	HR
Common case failure analysis	R	R	HR	HR
Historical event analysis	R	R	R	R

PHA should only be considered at the early stages of the development. When precise technical information is available, during the design, the other methods should be preferred.

4. 新しい列車制御システムに対応する安全性評価手法の検討

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ように
  - 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
- 規格適合性評価／認証との併存
  - 規格適合性評価だけではカバーできない部分は何か？

5. まとめ

- 鉄道信号分野における安全性評価は
  - 新しいシステムや改修したシステムに対して、技術的な観点から、安全上の問題がないかについて評価をおこなうもの
  - これまで交通安全環境研究所では、国内外のシステムに対して安全性評価を実施してきた
  - 一方、国外向けシステムの安全性証明手段としては国際規格への適合性評価／認証を受けるケースが増加
- 近年では、CBTC等の無線を使った新しい列車制御システムの導入・検討が進んでいる
- 新しい列車制御システムに対応するため
  - 従来のFMEAやFTAに加え、相互作用及び時間的遷移を伴うなどの複雑な事象を対象とするSTAMP/STPAの活用を検討
  - 評価基準の設定や、特に評価対象外装置を含むシステムにおいて安全上の方策に抜け漏れがないかを確認する方法等について引き続き検討
- 今後も安全性評価を通じて、鉄道分野の発展に寄与していきたい