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

1．はじめに

交通安全環境研究所では、第三者機関として国内外の列車制御システムに対する安全性評価をこれまでに実施してきた。近年では、新しい列車制御システムの導入・検討が進んでいることから、これに対応する安全性評価手法を検討したので、報告する。

2．安全性評価とは

鉄道信号分野における安全性評価とは、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評価を行うものである。近年、鉄道システムを輸出する際、安全性を相手先に証明する方法として、メーカはその製品の第三者評価を受けることが一般化している。この第三者評価には、安全性評価と、機能安全関連の国際規格への適合性評価／認証とに大別される。本稿では、前者を対象としている[1]。安全性評価のうち、評価の依頼者である事業者・メーカ等が作成した、設計仕様に対して評価を行うものを設計安全性評価という。基本的な手順は、まず、評価範囲を定め、その後、依頼者から提出された技術内容及び設計仕様、定量的なリスク分析、及びシステムの安全管理方法等に対し妥当性の評価を行う。

3．無線を使った新しい列車制御システム

3．1．無線を使った列車制御システムの概要

近年では、列車位置及び進行方向等の伝送に無線を使うなど、新しい列車制御システムの導入・検討が進んでいる。この無線を用いた列車制御システムは、統一的な仕様はないものの、国内においては、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[2]等により、導入・検討が円滑に進むような検討がなされている。無線を使った列車制御システムのイメージを図１に示す。従来の列車制御では、軌道回路及び地上子等の地上装置で列車検知し、制御も地上装置主体であることが多いが、無線式では、列車の位置演算を車上にて行い、地上装置から無線伝送により進路情報及び停止限界点等の情報を得て、停止限界点までのパターン制御を可能とする。

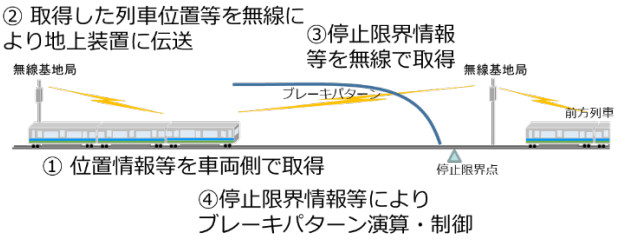

図１　無線式列車制御システムのイメージ

一般に、軌道回路を用いた従来の信号保安装置では、装置が故障した場合でも列車の在線状態となるため安全側であった。軌道回路を使わない場合、一部の装置が故障して列車位置が不明になってしまった際の、安全をどう担保するかが課題となる。また、無線式列車制御は列車密度や運転の考え方によって、情報更新間隔（地上制御装置及び車上制御装置の処理周期（制御周期）、制御装置間の伝送周期、並びに伝送品質によって定まる間隔）が異なるため、設計安全性評価を行う際に画一的な手法を取りにくいことが課題である。

3．2．無線式列車制御システムを対象とする安全性評価の課題

無線式列車制御システムを対象とする場合、設計安全性評価の主なポイントは、以下が挙げられる。

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

このうち、②、④及び⑥については、無線を用いることによる新たな項目と言える。⑤及び⑦は従来通りであるが、無線を使うことに注意をして評価を行う必要がある。さらに、①、③及び④については、従来の列車制御と比べ、車上装置／地上装置への機能の割付が異なることから、設計安全性評価の範囲を決定する上で特に注意が必要であると考える。また、通信を伴うため、タイミングなど、今までの安全性解析では評価の対象にならなかったものが対象になり得るようになり、新たな解析手法の追加の必要性が高まってきた。

4．STAMP/STPA を使った安全性評価の検討

4．1．STAMP/STPA とは

STAMP/STPA (System Theoretic Accident Model and Processes /STAMP based Process Analysis)は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を得意とする安全解析手法である[3]。従来の設計安全性評価には FTA (Fault Tree Analysis)及び FMEA (Failure Mode and Effects Analysis)等の安全解析手法を用いてきたが通信タイミングの考慮が難しい。また FMEA は、部品レベルでの詳細な解析を得意とするため、詳細な仕様が決まっていないと解析しにくい。一方、STAMP/STPA は概要レベルの情報でも解析できることが特徴である。そのため今回は STAMP/STPA を用いた検討を行った。

4．2．無線式列車制御システムを対象とした検討

図１にあるような簡単な無線式列車制御のイメージに対し、STAMP/STPA による解析を行った。表１にアクシデント・ハザード・安全制約の表を、図２にコントロールストラクチャを示す。ここでは簡易的に、車両の中を車上装置と車両（モータ、位置検知装置を含む）に分けて記載した。

ここで、図２において自車両への停止指示の誤りについて考えると、停止すべきタイミングで停止指示が出力されないことは、表１の SC1 違反となる。その原因を検討するため、自車両の車上装置に関するコントロールループ図を図３に示す。図３には、考えられる原因を記載しているが、このうち(3),(4)が無線伝送に関わる項目であることが分かる。このように、新しい列車制御システムの安全性評価の場合、最初に 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。

表１　アクシデント・ハザード・安全制約

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

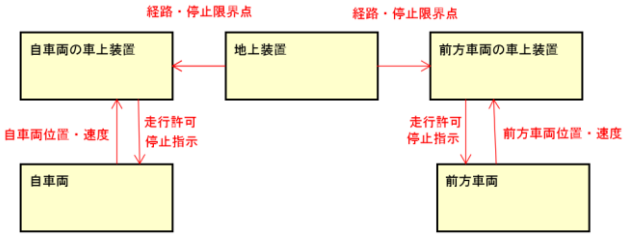

図２　コントロールストラクチャ

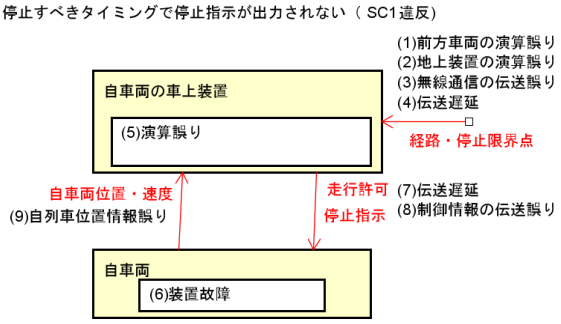

図３　コントロールループ図の例

5．おわりに

本稿では、近年導入・検討が進んでいる無線式列車制御システムをはじめとする新しい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。今後は、さらに検討を進め、新しい列車制御システムに対する安全性評価を進めていきたい。

参考文献

1) 林田他，“鉄道信号システムの設計安全性評価に関する新たな取組”，交通安全環境研究所フォーラム 2018 講演概要集，pp.55-58（2018）
2) 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，“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”，(2021)
3) 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”，(独)情報処理推進機構，(2016)