講演３．新たな安全設計手法を用いた鉄道信号の設計安全性評価に関する取組

交通システム研究部　※工藤 希　林田 守正　渡邉 翔一郎　佐藤 安弘
東京大学　水間 毅

１．はじめに

交通安全環境研究所では、海外向け鉄道システムの設計安全性評価に関し、これまでの実績に基づき、国際規格との調和や規格適合性評価等との関連について検討してきた[1)]。一方、複雑化した鉄道信号システムに対応するためには、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活用が有効と考えられる。本稿では、新しい評価手法として STAMP（System Theoretic Accident Model and Processes）/ STPA （STAMP based Process Analysis）による評価を試行したので報告する。

２．第三者安全性評価の位置づけ

２．１．国際規格への対応

近年、メーカ等が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、表１に示したような機能安全関連の国際規格への適合性について第三者評価及び認証（以下、「規格適合性評価」という。）を受けることが一般化している。一方、海外向け鉄道システムの設計段階を主な対象とする第三者による技術的な安全性評価（以下、「設計安全性評価」という。）は、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。

規格適合性評価とは異なり、設計安全性評価は、システムの技術内容及び設計仕様等について、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ものである。鉄道システム導入先の必要に応じて、規格適合性評価等を補強する目的で実施され、規格適合性評価報告書の補足文書として添付される位置づけが考えられる。一方、導入先によっては、規格適合性に関する第三者評価を必要とせず、設計安全性評価だけを求められる場合もある。こうした設計安全性評価の目的に対応するため、当研究所としては、表１の中でも特に、IEC 62425 及び IEC 62278 を重点的に参照し、これらの規格との整合を図った安全性評価報告書の構成案を提案してきた[2)]。

表１　参照する国際規格の一例

規格番号	規格名・通称
IEC 62425	鉄道信号用安全関連電子装置の安全性証明
IEC 62278	鉄道における RAMS
IEC 62279	鉄道信号システムのソフトウェアの安全性
IEC 62280	鉄道信号システムの通信の安全性
IEC 62236	鉄道システムの EMC（電磁両立性）

２．２．安全性の水準

IEC 62425 においては、安全性の水準として、非安全事象の発生頻度に基づいて 4 段階の SIL（Safety Integrity Level）が定義されており。その最高水準は SIL4（発生頻度 1×10^{-9}～10^{-8}/h）とされている[3)]。一般的に鉄道の列車制御システム及び信号システムに対しては SIL4 を達成することが要求されるため、各要素又はシステム全体における非安全事象の発生頻度が SIL4 を達成するか否かを主要な判断基準とする。

２．３．これまでの安全性解析

これまで、設計安全性評価では、FMEA（Failure Mode and Effects Analysis）及び FTA（Fault Tree Analysis）を中心とする評価手法により実施してきた。これらの手法は、システムのハザードとその要因を事前に分析するための安全解析手法である。部品レベルまで細分化して分析できるため、深い分析が可能であるという特徴がある。

これまでの設計安全性評価においては、FMEA の結果から選定した非安全事象をトップ事象とする FTA を行い、そのトップ事象が発生する確率又は頻度が十分に小さいことを確認してきた。図 1 に FTA の例を示す。FTA では部品の故障率を積み上げることでトップ事象に至る確率、すなわち非安全事象の発生頻度を求めることができるが、FTA の制約ゲート（制約条件事象が発生する場合に限って入力事象が有効となるゲート。AND ゲートと同等に計算できるもの）には、定期検査等の人の動作によるものが含まれるが、それらにより防護しなければ、安全性の水準（例えば、SIL4）を達成できないケースもある。このようなヒューマンエラーの発生確率は、安全性の水準の達成目標から逆算して求めることもでき、これまでの評価では、逆算した結果、ヒューマンエラーの発生確率を 0.01～0.001 以下に抑えることを条件として SIL4 が達成されるケースも存在した。

一方、一般的には定例作業時のエラー発生率は 0.01～0.00001 とされている [4]ため、この前述の逆算によって求めた結果は妥当と考えられる。但し、このエラー発生率は教育・訓練がきちんと行われていることが前提であり、特に海外向けの評価においては、この前提を明示しておくことが必要である。

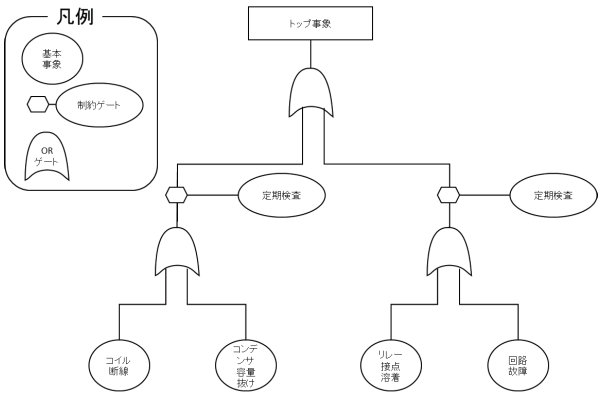

図 1　FTA の例

3．STAMP/STPA の概要

3．1．概要

技術の進展に伴い評価対象装置も複雑化してきており、これまでの FMEA 及び FTA のみで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が難しくなってきた。そのため、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 STAMP/STPA を用いた安全性解析を検討した。

STAMP は 2012 年にマサチューセッツ工科大学の Leveson 教授が提唱した安全解析手法である [5]。現代のシステムのアクシデントの多くは、システムの構成要素の故障によって起きるのではなく、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）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であり、この STAMP を前提として、システムのハザード要因を分析する安全解析手法が STPA である。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一方、部品レベルの解析には解析が膨大となることが想定され、そのような解析にはこれまで通り、FMEA 及び FTA を用いる方が良いと思われる。

3．2．鉄道への活用事例

鉄道における STAMP/STPA の活用事例としては、踏切制御を扱った例 [5]、ATC に対する安全性・信頼性解析を行った例 [6]及び ATS 装置を対象とした例 [7]等がある。

特に ATS 装置を対象とした例では、FMEA 及び FTA と共に STAMP を実施し、FTA で抽出できなかった項目を STAMP/STPA により抽出した項目が示されており、今後の安全性評価について、FMEA 及び FTA だけでなく必要に応じて STAMP/STPA を行うことに一定の効果があることが示されている。

STAMP/STPA 自体が最近提唱された手法であるため、活用例は多くはないが、今後の安全性評価に有用な手法であると考えられる。

4．STAMP/STPA の試行

前報 [1]に続き、図 2 に示すような簡単な連動装置をモデルとして STAMP/STPA の適用を試行した。

4．1．試行手順

STAMP/STPA ではまず、アクシデント・ハザード・安全制約の識別及びコントロールストラクチャを構築する。次に、UCA（Unsafe Control Action：非安全制御動作）を抽出し、UCA 毎に HCF（Hazard Causal Factor：ハザード誘発要因）を特定する。

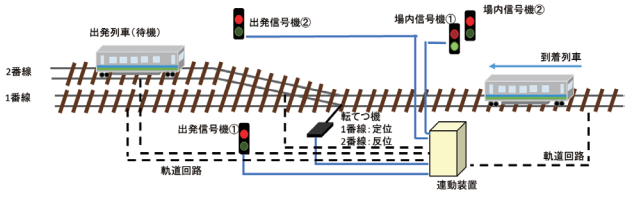

図 2　モデル

4．2．STAMP/STPA の適用

本検討では、制御を行う要素を連動装置、制御され

る要素を転てつ機と仮定し、制御構造図（コントロールストラクチャ）を図３に示すように構築した。連動装置から転てつ機への制御指示は、定位への転換、反位への転換、鎖錠及び解錠とし、各々の制御指示について連動装置へのフィードバック機能を有することとした。また、それ以外の関係要素として、進路構成、軌道回路（4 区間）及び信号機（出発／場内）を挙げた。

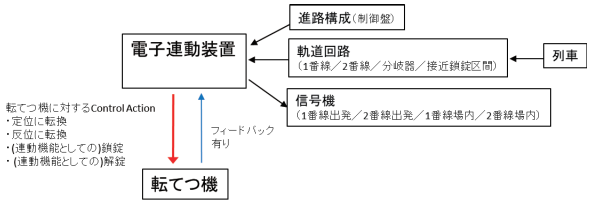

図３　コントロールストラクチャ

この検討で出てくるアクシデント・ハザード・安全制約の一覧を表２に示す。アクシデントに分岐器上の脱線又は衝突を挙げ、そのハザードと安全制約を挙げた。次に、コントロールアクションに対して安全制約違反となる UCA を表３に整理した。表中赤字の項目が UCA となる。コントロールアクションが与えられない場合、与えられた場合、早すぎ／遅すぎ及び早すぎる停止／長すぎる適用のそれぞれの場合にどういった事象が起こりえるかを整理しており、装置間の時間的な遷移も考慮に入れた抽出が可能である。

これらの抽出された UCA に対し、図４に示すガイドワードを参考に、図５に示すようなコントロールループ図を作成し、HCF を抽出した。ガイドワードとは、解析する際のヒントとなる言葉であり、これがあ

表２　アクシデント・ハザード・安全制約一覧表

アクシデント	ハザード	安全制約
(A1) 列車が分岐器上で脱線する	(H1) 列車が分岐器上に在線中に不正転換する	(SC1) 列車が分岐器上に在線中は転換してはならない
(A1) 列車が分岐器上で脱線する	(H2) 列車が分岐器上を走行中に鎖錠されない	(SC2) 列車が分岐器上に在線中は鎖錠しなければならない
(A1) 列車が分岐器上で脱線する	(H3) 列車が非開通の分岐器を背向で通過する	(SC3) 列車が背向で分岐器を通過する際に非開通であってはならない
(A2) 列車同士が衝突する	(H4) 到着列車の進路が駅在線列車と競合する方向に分岐器が開通している	(SC4) 進路が競合するように分岐器を開通させてはならない
所定の列車が駅から出発できない	・分岐器非開通の場合、解錠ができない ・分岐器非開通の場合、定位または反位への転換ができない ・分岐器開通後の鎖錠ができない	出発ができるよう解錠、転換、鎖錠を行う
所定の列車が駅に到着できない	・分岐器非開通の場合、解錠ができない ・分岐器非開通の場合、定位または反位への転換ができない ・分岐器開通後の鎖錠ができない	所定の到着ができるよう解錠、転換、鎖錠を行う

表３　UCA 識別表

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／長すぎる適用でハザード
反位から定位に転換指示	・1番線の発着が不可 ・(UCA1)1番線から誤発車すると脱線SC3違反	・(UCA2)列車が分岐器上に在線すると脱線SC1違反 ・(UCA3) 2番線から誤発車すると脱線SC3違反	早すぎると ・1番線からの列車より先行する2番線からの列車の出発が不可 ・1番線からの列車出発前の2番線への列車到着が不可 ・1番線への列車に先行する2番線への列車の到着が不可 ・2番線への到着列車が分岐器直前だと1番線に誤進入（(UCA4) 1番線に他列車在線だと衝突）) SC4違反 ・(UCA5)2番線への到着列車が分岐器上だと脱線 SC1違反 ・(UCA6)2番線からの出発列車が分岐器上だと脱線 SC1違反 遅すぎると ・1番線からの出発が遅延 ・1番線への到着が遅延	早すぎる停止だと ・転換が途中で停止し列車の発着が不可 長すぎる適用だと ・次の反位への転換が不可
定位から反位に転換指示	・2番線の発着が不可 ・(UCA7) 2番線から誤発車すると脱線SC3違反	・(UCA8) 列車が分岐器上に在線すると脱線SC1違反 ・(UCA9) 1番線から誤発車すると脱線 SC3違反	早すぎると ・2番線からの列車より先行する1番線からの列車の出発が不可 ・2番線からの列車出発前の1番線への列車到着が不可 ・2番線への列車に先行する1番線への列車の到着が不可 ・1番線への到着列車が分岐器直前だと2番線に誤進入（(UCA10) 2番線に他列車在線だと衝突）SC4違反 ・(UCA11) 1番線への到着列車が分岐器上だと脱線 SC1違反 ・(UCA12) 1番線からの出発列車が分岐器上だと脱線 SC1違反 遅すぎると ・2番線からの出発が遅延 ・2番線への到着が遅延	早すぎる停止だと ・転換が途中で停止列車の発着が不可 長すぎる適用だと ・次の定位への転換が不可
鎖錠指示	(UCA13) 車両が分岐器上を走行中だと脱線 SC2違反	転換が不可	遅すぎると ・(UCA14) 分岐器に進入した車両が脱線 SC2違反	早すぎる停止だと ・(UCA15) 分岐器に進入した車両が脱線 SC2違反 長すぎる適用だと ・次の解錠、転換が不可
解錠指示	転換が不可	(UCA16) 車両が分岐器上を走行中だと脱線 SC2違反	早すぎると ・(UCA17) 分岐器から進出前の車両が脱線 SC2違反	早すぎる停止だと ・解錠が不完全で次の転換が不可 長すぎる適用だと ・次の鎖錠が不可

ることで、対象とする装置に詳しい人間でなくても容易に解析を行うことができるものである。

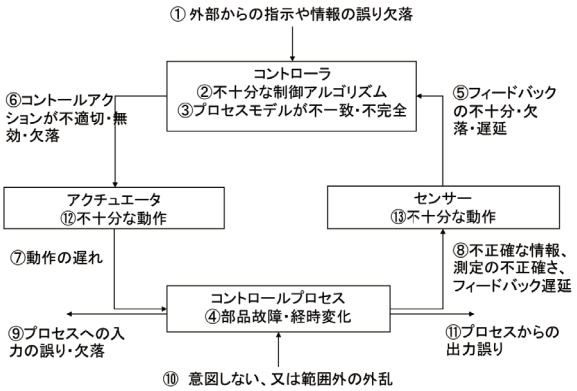

図４　STAMP におけるガイドワード[8)]

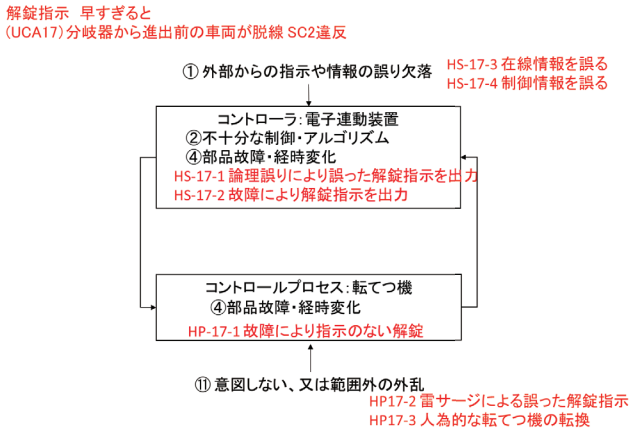

図５　コントロールループ図の例（UCA17）

図５はUCA17に対してコントロールストラクチャを作成しそのハザード要因を解析したコントロールループ図の例である。同様に他の UCA に対しても解析を行った。抽出されたすべての UCA に対して解析を行った結果、表４のように、HCF とその対策を整理した。

以上より、STAMP/STPA を実施することにより、相互作用及び時間的遷移も考慮に入れた安全性解析を行うことが可能であることを確認した。

表４　HCF とその対策の例（UCA17）（一部）

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

５．おわりに

海外向け鉄道システムの設計安全性評価に関し、複雑化した鉄道信号システムに対応するための評価手法について検討した。

これまでの FMEA 及び FTA のような部品故障を対象とする考え方だけではなく、装置間の相互作用を解析する STAMP／STPA の活用が有効なケースもあると考えられ、その一例として連動装置を例に検討を実施した結果、時間的遷移も考慮に入れた解析が可能なことから、その有効性を確認した。

今後は、FMEA 及び FTA による従来の安全性解析に加え、複雑化した鉄道信号システムに対応した STAMP/STPA の適用実績を積み重ねていき、引き続き設計安全性評価に貢献していきたい。

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) 林田他，“軌道系交通システムの国際展開に対応した技術評価手法の検討”，交通安全環境研究所フォーラム 2015 講演概要集，pp.53-56（2015）
3) IEC 62425 “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling”, Ed.1.0 (2007)
4) 中條武志，“人間信頼性工学：エラー防止への工学的アプローチ”，http://www.indsys.chuo-u.ac.jp/~nakajo/open-data/Healthcare_Errorproofing2.pdf
5) 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”，独立行政法人情報処理推進機構 p.1（2016）
6) 川野卓，“列車制御システムにおけるアシュアランス技術の適用に関する研究”，pp.70-85（2018）
7) 杉本他，“STAMP 解析による時系列表現を取り入れた FTA 解析の提案”，日本信頼性学会，第 27 回春季信頼性シンポジウム発表報文集，pp.109-112
8) システム安全性・信頼性解析手法 WG，“はじめての STAMP/STPA（実践編）”，独立行政法人情報処理推進機構 p.8（2017）