安全性解析技法を用いた鉄道障害事故の分析

小笠原秀人（千葉工業大学）
hideto.ogasawara@p.chibakoudai.jp

瀬戸口大空（千葉工業大学）

要旨

鉄道事故の事例[2]を基に，Nancy G.Leveson 教授（MIT）が提案した STAMP/STPA (Systems Theoretic Accident Model and Process/ System-Theoretic Process Analysis)を活用した事例を報告する.

1. 分析対象と事故概要

今回の研究では，令和元年（2019 年）6 月 1 日に神奈川県横浜市の金沢シーサイドライン新杉田駅構内で発生した鉄道人身障害事故を対象とする.

本事故は，無人の自動運転で始発の新杉田駅を定刻（20 時 15 分）に出発したところ，列車の進行方向である下りとは反対方向の登りに発車して，線路終端部の車止めに衝突した.

本事故の原因は，列車の進行方向を伝える F 線が断線し，本来設定されるべき進行方向をモーター制御装置へ設定することができず，進行方向のメモリ機能により維持されていた上り方向にモーターを駆動させたためと推定される. さらに駅 ATO（Automatic Train Operation）車上装置がモーター制御装置への入力とは別の運転台選択用の指令線の加圧状態により進行方向状態を地上に送信していたため，駅 ATO 地上装置は列車の進行方向が正常に設定されたと認識し，また後退検知機能や他の手法により本事故のような逆走を検知する機能がなかったため，非常停止などの対応ができなかったものと考えられる[2].

2. 分析方法

文献[[1]に従い，図 1 に示す手順で分析した.

STMAP モデル作成:
・Step0 準備 1:アクシデント，ハザード，安全制約の識別
・Step0 準備 2:コントロールストラクチャの構築
STPA（分析）:
・Step1:非安全なコントロールストラクチャの抽出
・Step2:非安全なコントロール要因の特定

3. 分析結果と考察

Steo0 準備 1 で作成したアクシデント，ハザード、安全制約の識別結果の一部を表 1 に示す.

表 1 アクシデント，ハザード，安全の識別

アクシデント（Loss）	ハザード（Hazard）	安全制約（Safety Constraints）
(A1)列車が予期せぬ方向へ発車する	(H1)指令線が正しく加圧されていない	(SC1)指令線は正しく加圧されなければならない
(A1)列車が予期せぬ方向へ発車する	(H2)進行方向指令を正常に受信できていない	(SC2)進行方向指令は正常に送受信できていなければならない

表 1 を起点として分析を進めた結果，4 つのガイドワードをヒントにして，表 1 で示した 2 つの安全制約（SC1，SC2）に違反する UAC（Unsafe Control Action：非安全制御動作）が検出できた. 今回の分析は文献[2]を読んで実施しているため，ハザードの粒度などが細かくなり，結論ありきの分析になっている可能性は否めないが，この事故が事前に識別できる可能性は確認できた.

文献[2] 2.9 節に，設計・製造プロセスや実施した設計作業などが示されている. 従来の安全性解析技法も活用され，さまざまな関係者間で検討され審査されていることが分かる. 一方で，車両メーカーは，各装置の機能や装置間のやり取り全てについては把握することは難しいと述べている. 今回の事故における分析結果を，自動運転などのより相互作用が複雑なシステムにおける安全解析の教訓として引き継ぐことが重要と考える.

参考文献

[1] 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～，情報処理推進機構（IPA），2016.
[2] 運輸安全委員会，“鉄道事故調査報告書”，https://www.mlit.go.jp/jtsb/railway/rep-acci/RA2021-1-1.pdf, 2021.