

第 2 回 STAMP ワークショップ発表概要

タイトル

STAMP/STPA の鉄道信号システムへの応用と拡張

Application and extension of STAMP/STPA to Railway Signalling System

著者・発表者

東日本旅客鉄道 高野 友佑、佐々木 裕史、森田 雄一、杉浦 弘人、川野 卓

EAST JAPAN RAILWAY COMPANY Yusuke Takano, Hiroshi Sasaki, Yuichi Morita, Koji Sugiura, Takashi Kawano

概要

STAMP/STPA は、従来の信頼性工学の FTA や FMEA によるハザード分析と異なり、対象システムの機能を抽象化・階層化したトップダウンの安全解析法として注目されている。人間と機械の協調による安全制御、インターネット接続や高度なソフトウェアなど複雑化したシステムの安全制御といった近年の新しい複雑システムの安全確保には、コンポーネント故障を最小化するという従来の信頼性工学的手法では十分でなく、コンポーネント間のコミュニケーションエラーまで含めたハザード要因をどのように抑制・制御するかというトップダウンの抽象的機能レベルでの安全設計が大事になる。

STAMP/STPA の利点として、ドメインの専門家でない技術者でも解析が可能であることが挙げられる。一方で、鉄道信号システムはこれまでの事故や不具合を基にドメインの専門家により対策が検討され、現在の安全性が築き上げられている。また、鉄道信号システムにおいては、安全性のみならず信頼性も重要な要素となる。そこで、STAMP/STPA を信頼性についても拡張し、鉄道信号システムにおけるこれまでの事故や不具合などを評価する。

キーワード

- (1) STAMP/STPA
- (2) Railway signalling system
- (3) Safety
- (4) Reliability