第 2 回 STAMP ワークショップ発表概要

タイトル

STAMP/STPA による踏切制御システムの安全性要求分析

Safety requirement analysis of level crossing control system using STAMP/STPA method

著者・発表者

東日本旅客鉄道　国藤　隆

East Japan Railway Company　Takashi KUNIFUJI

概要

近年、鉄道の信号保安システムは、その基となる情報通信技術の発展に伴い、ハードウェア・ソフトウェア双方の高度化・複雑化が進んでいる。信号保安システムには、その専門性も相まって、安全要求が非常に高い・オーダーメイド要素の大きい・事業者とメーカの責任境界の曖昧いであるといった特殊事情が存在しており、これらが信号保安システムをより一層複雑なものとしている。このような中で、信号保安システムの開発費低減および安全性向上に繋がる技術開発の一つとして、ソフトウェアや制御論理そのものの安全解析を通して要求仕様の正当性・妥当性の検証に取り組んでいる。

本研究では、過去に試作した、駅構内の踏切制御システムを題材にして、開発の上流工程で行うリスク分析への STAMP/STPA 手法の適用を試行した。本試行において、踏切制御における一般的な安全に関する要求事項を効率的に抽出することができ、STAMP/STPA 手法がイベント駆動型システムである信号制御システムに有効性であることを確認した。一方で、リスク分析の網羅性確保については、解析者が保有する対象システムに対する経験に依存する部分が大きいという課題が残存していることも分かった。これらを踏まえて、STAMP 手法をより効果的に活用するための将来展望についても提示する。

キーワード

(1)　踏切

(2)　信号保安装置

(3)　安全性

(4)　STAMP/STPA

(5)　STAMP/CAST