第 2 回 STAMP ワークショップ発表概要

タイトル

システムモデルを用いた STAMP/STPA 試行の事例紹介

著者･発表者

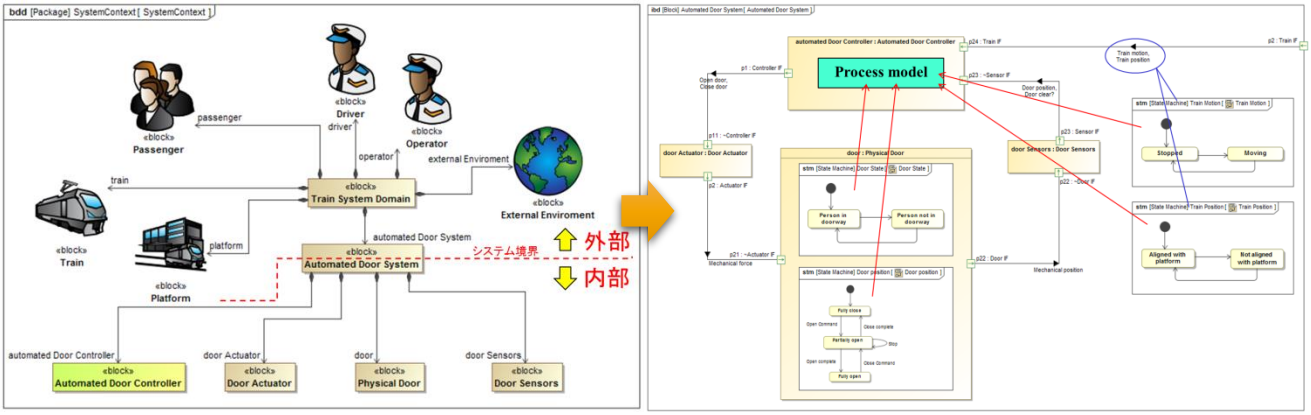
日立産業制御ソリューションズ　橋本　岳男

Hitachi Industry & Control Solutions, Ltd.　Takeo Hashimoto

概要

STAMP/STPAは、システムの故障だけでなく複数のシステムや人、環境といった様々なコンポーネント間の相互作用により引き起こされるアクシデントの要因を解析することが可能とされている。システムを構成する要素が決まる前の上流の構想段階においても安全解析を行えることが、従来の安全分析手法との違いの一つといえる。また、STAMP/STPA は、強制発想ツールという側面もあることから、分析担当者により様々な分析結果を得ることができる。しかし、分析プロセスの過程が残っていない場合、分析結果だけでは関係者や第三者がその分析結果の網羅性や妥当性を判断するのは困難である。そこで、分析プロセスの思考過程を可視化し残すことがその問題の解決に重要な役割を果たすと考え、システムズエンジニアリングアプローチにより構築したシステムモデルを活用したSTAMP/STPAの試行について具体的な事例を用いて紹介する。なお、コントロールストラクチャーや分析過程の可視化は、国際標準規格であるSysML(Systems Modeling Language, ISO/IEC 19514:2017)を使用した。

例えば、STAMP/STPAにおいて重要となるコントロールストラクチャー(右図)は、システムコンテキスト(左図)やシーケンス図等の分析結果により記述している。（ここでは途中省略）また、可視化により登場人物の過不足や考慮すべき点など新たな気づきを得やすい。



キーワード

(1) システムズエンジニアリング

(2) 非故障

(3) 分析過程の可視化

(4) SysML

(5) トレーサビリティ