第 3 回 STAMP ワークショップ発表概要

タイトル

STAMP／STPA を用いたハザードログツールの提案

A Proposal to Use a Hazard Log Tool in Conjunction with STAMP/STPA

著者・発表者

（株）京三製作所　髙田　哲也・堺　将人

Kyosan Electric Manufacturing Co.,Ltd.　TETSUYA　TAKATA / MASATO　SAKAI

概要

STAMP/STPA は、従来の FTA や FMEA などの事故評価モデルでは見つけることが難しかったシステム全体の設計や、構成要素間のインタフェースの齟齬に起因する事故原因をソフトウェアモジュールの故障時のインタフェースの挙動から解析できるため，より説得力のある解析ができる。

STAMP/STPA の解析手順は、作業手順が示されており、作業を容易に進めることができる。また、モデリングツールを活用することで、初心者でもツールが提供するガイドに従って作業をしていけば、STAMP 理論に基づいた安全解析を始めることができる状況にある。

しかしながら、STAMP/STPA はハザードを引き起こす安全ではない制御指示としては抽出されたが、実際にはあり得ないものと、現実に考え得る注視すべきものとが区別なく評価されるという利用上の課題もある。このことから、リスクベースの設計手法と STAMP/STPA による解析結果の網羅性を融合することにより、解析対象が安全なシステムを構築していることを示す証拠として有効となると考えられる。

ここでは、定義したアクシデントから鉄道の国際規格 RAMS（IEC62278）の第 3 段階リスク分析項に基づき体系的かつ、STAMP/STPA 利用により網羅的にシステムに含まれるハザードリスクを抽出して、それらへの対策を施し、許容されるレベルにまでリスクが軽減されることを示す手順について示す。

更に、モデリングツールにはない抽出したハザードをキーとし、この結果をまとめたハザードログツールを提案する。ハザードログは、各ハザードのリスクの軽減過程を設計の進行と同期して更新可能で、その課程での追跡性、透明性を確保し、技術の妥当性・正当性を説明する上での中心的な論拠となる。

このようにこのハザードログは、実際に行われる安全性審査のためのリスク分析に使うことを想定し、ハザード管理手法の概念に基づいて整理した。

キーワード

(1) STAMP／STPA

(2) 電子連動装置

(3) RAMS（IEC62278）

(4) モデリングツール

(5) ハザードログツール