第 2 回 STAMP ワークショップ発表概要

タイトル

IPA が提供する STAMP 支援ツール i-STAMP（開発コード）

IPA/SEC will provide a STAMP based hazard analysis tool i-STAMP(code name)

著者・発表者

独立行政法人情報処理推進機構　石井　正悟

Information-technology Promotion Agency, Japan.　Shogo Ishii

概要

STAMP(Systems-Theoretic Accident Model and Processes)は、システムの創発的特性（Emergent Properties）によってアクシデントが発生する、という新しい概念であり、STPA(System Theoretic Process. Analysis)はその STAMP をベースとし、コンポーネント間の相互作用に着目してハザード要因を特定するという新しいハザード分析手法である。

新しい概念、新しい手法であるため、はじめて STAMP/STPA の適用に取り組む技術者にとっては、何をどうすれば良いのかという具体的な手順を調べ、なぜその手順で行うべきなのかの本質を理解することに悩まされることになる。また、STAMP/STPA は分析において自由な発想を引き出す手法であるので、分析途中で新たな気付きを得て、前の Step に立ち戻り分析を続けることが多い。それは、網羅性を向上させるために好ましいことである。一方、前の Step に立ち戻って分析を行うには、それまでに作成した図表を更新する必要があり、図表更新の作業に手間がかかるため、分析作業の効率が低下し、更に大きな問題として、思考を中断されることになる。

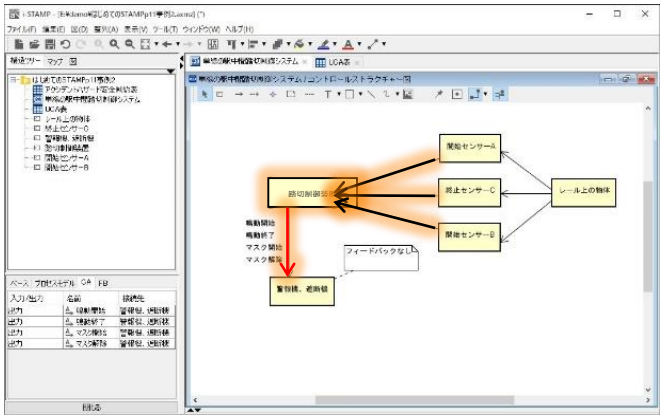
・具体的な分析作業内容と手順の習熟に時間がかかる。多くの経験を要する。

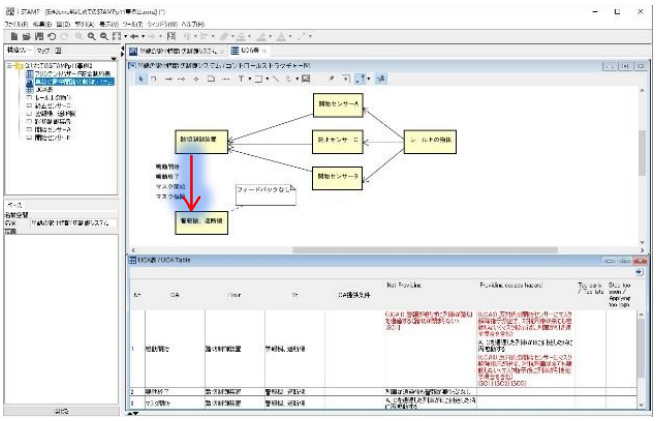
・図表作成・編集作業に手間がかかり、思考に専念できない

IPA は、これらを STAMP 普及の阻害要因であると捉え、その解決策として STAMP 支援ツール活用が有効と考えた。

これまでにも海外で STAMP 支援ツールがいくつか提案され、オープンソースとしてツールのソフトウェアが公開され、自由に使用できるようになっている。しかし、IPA がそれらのツールを試用したところ、分析を支援するツールとは言い難く、分析した結果を清書するためのツールであったり、STAMP による分析に関して上級レベルの技術者向けであったり、STAMP 研究者向けであろうと思われる。

そこで IPA は、これから STAMP を導入しようとする初級レベルの技術者もツール活用の効果を享受できて、分析を支援するツールを開発し、無償公開することとした。現在開発中の STAMP 支援ツールは、開発コードを i-STAMP と言い、2018 年 3 月にはバイナリーおよびソースコードを無償公開すべく開発を進めている。





キーワード

(1) STAMP/STPA

(2) STAMP 支援ツール

(3) IPA/SEC

(4) STPA 手順誘導

(5) STPA 作業効率改善