STAMP/STPAにおける振舞いモデル記述の 効用について

岡野 浩三^{1,a)} 楊 盼¹ 辛島 凜¹ 小形 真平¹

概要: STAMP/STPA は近年における複雑システムの解析手段の1つとして有望視されている。STAMPでは各コンポーネントが信頼できると仮定しても、その結びつきによって誘発される不具合がありうることを前提とし、その不具合の発見を支援する手法(STPA)を与えている。いったんSTAMP/STPAでハザードが特定された後は、ハザードに至る具体的シナリオの導出がされる。著者らは各コンポーネントの振舞いモデルを記述し、モデル検査を活用してシナリオ導出に有用である事例を研究してきた。本稿では、その手順をまとめ、モデル導出の有用性についてリスク分析の応用の観点から考察をする。

On Utility of Behavioural Model Description for STAMP/STPA

KOZO OKANO^{1,a)} PAN YANG¹ RIN KARASHIMA¹ SHINPEI OGATA¹

1. はじめに

システム理論に基づくアクシデントモデルとしてSTAMP (Systems Theoretic Accident Model and Processes) が提案されている [1]。またSTPA (STAMP based Process Analysis) はSTAMPに基づいた解析手順を与えており [2]、近年における複雑システムの解析手段の1つとして有望視されている。STAMPの特徴としてコンポーネントの詳細はブラックボックスとし、各コンポーネント (人間もコンポーネントとして扱う) 間の制御の結びつきをコントロールストラクチャとして抽象化し、そのコントローラストラクチャにおいてハザード分析を行うことを挙げることができる。STAMPでは各コンポーネントが信頼できると仮定しても、その結びつきによって誘発される不具合がありうることを前提とし、その不具合の発見を支援する手法を与えている。STAMPでは起こってはいけない事象をアクシデントと呼び、アクシデントに至る1つ手前の状態をハザードと呼んでいる。STPAではハザードを導く動作 Undsafe Control Action (UCA) をガイドワードなどを利

用し特定していく。STAMP/STPAでハザードが特定された後は、ハザードに至る具体的シナリオの導出がされる。一般にこのシナリオ導出においては時間コストを要する。この原因の1つとして、各コンポーネントの内部動作をブラックボックスのままにしていることを仮説として挙げる事ができる。

この仮説に基づけば、シナリオ導出作業においては各コンポーネントの振舞いをブラックボックスのままにしておくよりは、ある程度振舞いを仮定しておいたほうが望ましいと考えられる。その観点にたち、著者らは各コンポーネントの振舞いモデルを記述し、モデル検査を活用してシナリオ導出を行う方法をいくつかのケーススタディに対して適用してその有効性を示してきた [4], [5], [6]。一方で、各コンポーネントの振舞いを最初から与えることは一般論としては、STAMPの考え方に反する。そこでは、本稿では、適切な解析手順を与え、また、一般に高コストである振舞いモデル導出の結果を有効利用する方法についてさらに考察をする。

2. 提案手順

提案手順の最初はSTPAと同じである。StampWorkbench [3] などを利用して、解析を進めていく。UCAを特

¹ 信州大学
IPSJ, Chiyoda, Tokyo 101-0062, Japan
^{a)} okano@cs.shinshu-u.ac.jp