第 3 回 STAMP ワークショップ発表概要

タイトル

STAMP/STPA とモデル検査との連携について-鉄道踏切「とりこ検知」例題をもとに-

Collaboration between STAMP/STPA and model checking – Based on STAMP analysis example “Fallen Barrier Trap at Railroad Crossing”–

著者・発表者

信州大学　岡野浩三、小形真平、楊盼、辛島凜

Shinshu University　Kozo Okano, Shinpei Ogata, Pan Yang, Rin Karashima

概要

近年の情報システムはますます大規模複雑になり，情報システムの事故原因分析やその対策構築に関する技術研究の需要が高まっている．Systems Theoretic Accident Model and Processes (STAMP)では，システム構成要素の不具合や人間のミスなどに限らず，構成要素の間や構成要素と人間の間の相互作用のエラーなども分析できる特徴を持つ．STAMP モデルに基づいた解析手法 STAMP based Process Analysis (STPA)では，コントローラーと被コントローラーの相互作用に対して，システムのアクシデントの可能性を事前に分析する．STAMP/SPTA は形式手法との連携を意識しているものではないが，モデル検査の連携により，より有効なアクシデント分析が期待できる．本発表では STAMP 解析例題である鉄道踏切「とりこ検知」を例題として，時間オートマトンのモデル検査器 UPPAAL との連携の方法について考察する．とりわけ，時間変数のレンジ導出の数理計画法を用いた可能性について考察する．また，実際に UPPAAL を用いて解析した結果についても述べる．以上の結果から，STAMP/STPA ツールである STAMPWorkbench とモデル検査器との連携方法についても考察する.

キーワード

(1)　STAMP/STPA

(2)　時間オートマトン

(3)　モデル検査

(4)　数理計画法

(5)　とりこ検知