第 2 回 STAMP ワークショップ発表概要

タイトル

Extending STPA をベースとしたプロセスモデル抽出の工夫

An idea how to derive Process Models based on Extending STPA

著者・発表者

日本ユニシス　福島　祐子

Nihon Unisys Ltd.　Yuko Fukushima

概要（日本語）

STAMP/STPA では、よくある事故の原因は、プロセスモデル（システムが認識するシステムの状態）とシステムの状態との不一致により “安全ではないコントロールアクション”（UCA）が実行されることにあるとしている。そのため、プロセスモデルが重要であるが、プロセスモデルの抽出方法は提示されておらず、分析者がアドホックに抽出するしかないという課題がある。

この課題に対し、MIT の Thomas 博士は Extending STPA という手法を発表している。この手法では、ハザードからハイレベルなコンテキストを捉え、プロセスモデル階層により詳細化したプロセスモデルを UCA の最初のコンテキストとして捉える。そして、そのコンテキストを分解することでプロセスモデルを具体化し、プロセスモデルを組み合わせることで UCA を識別する。

Extending STPA は強力な手法であるが、ハザードのコンテキストからプロセスモデル階層による詳細化を行う過程でプロセスモデルが抜け漏れてしまう可能性がある。そこで、コントロールアクションを対象として 6W3H を適用することにより、コンテキストを幅広く捉える改良案を考えた。

発表では、STAMP/STPA の課題、Extending STPA の概要と課題、6W3H を適用してコンテキストを特定する改良案と試行した結果について説明する。

キーワード

(1)　Extending STPA

(2)　プロセスモデル

(3)　コンテキスト

(4)　UCA

(5)　6W3H