

第 2 回 STAMP ワークショップ^o発表概要

タイトル

Freedom from interference に着目した STAMP/STPA の活用
Using STAMP/STPA focusing on “freedom from interference”

著者・発表者

長崎県立大学 日下部 茂

University of Nagasaki Shigeru Kusakabe

概要

ハザード分析を主眼に提唱された STAMP/STPA は、そのモデル化にあたって必要なアクシデントの定義を、人命の損失といったものだけでなくミッションの失敗といった広範なものとして行うことができる。そのため、比較的汎用性の高い方法論であると同時に、その汎用性の高さが、逆に具体的な使い方の検討する際の絞込みの難しさにつながっている可能性もある。発表者は、ISO26262 でも言及されている “Freedom From Interference” (FFI) を関心事として STAMP/STPA のモデル化と分析を行うアプローチを提案する。ソフトウェアアーキテクチャの分野でも、ビューやパースペクティブを活用する方法論が提唱されている。同様の考えは、システムアーキテクチャの記述にも当てはまると考え、FFI を関心事として着目した上でシステムアーキテクチャの記述や分析を行うことで開発プロセスにおける STAMP/STPA の活用も促進されると考える。今回は、AADL(Architecture Analysis & Design Language)のエラーモデルアネックス EMV2 でのエラー伝搬と関連付けたモデル化と分析のプロセスでの活用について述べる。

キーワード

- (1) Freedom from interference
- (2) Architecute description and analysis
- (3) Perspective
- (4) ISO26262