第 2 回 STAMP ワークショップ発表概要

タイトル

STAMP／STPA を用いた Cyber-Physical Systems の検証

Verification of Cyber-Physical Systems Using STAMP / STPA

著者・発表者

日本ユニシス　青木　善貴、信州大学　小形　真平、大阪大学　中川　博之

Nihon Unisys, Ltd.　Yoshitaka Aoki,　Shinshu University　Shinpei Ogata,　Osaka University　Hiroyuki Nakagawa

概要

CPS(Cyber Physical System)は様々な分野において活用が進んでおり，今後多くのシステムが何らかの形で CPS を包含することになる．CPS システムは，サイバー世界と物理世界をまたがることにより外部環境のゆらぎを受ける．そのためシステムの振る舞いに不確かさがあり，安全性の検証が難しい．

複雑なシステムの安全性解析の手法として STAMP/STPA が注目されている．STAMP/STPA はシステム理論に基づく事故モデルであり，構成要素の相互作用の中から非安全な制御を見つけることによりハザード分析を行う．また STAMP/STPA は，動的な外部環境も事故モデルに含むことができるため，外部環境の影響が大きい CPS システムの解析にも適している考えられる．ただし，CPS は複数のデバイスが競合して動作するため，コントロールストラクチャが複雑になることが想定される．

本発表では，複雑になるコントロールストラクチャを整理する方法と，そのコントロールループの安全な状態をモデル検査により検証する手法を提案する．例題として Vehicle-to-Device (V2D)システムを利用した車の交通制御システムの安全性の解析を行う。STAMP/STPA と本提案を組み合せは，振る舞いの予測が困難な CPS システムの安全性の検証に役立つと考える．

キーワード

(1)　STAMP/STPA

(2)　Cyber-Physical Systems

(3)　モデル検査