第 2 回 STAMP ワークショップ発表概要

タイトル

コントロールストラクチャの状態遷移仕様とガイドワードを用いたシミュレーションによる STAMP/STPA の非安全コントロールアクション識別方式の提案

A Proposal to identify unsafe control actions in STAMP/STPA by simulation using State Transition Specification of Control Structure and guide word

著者・発表者

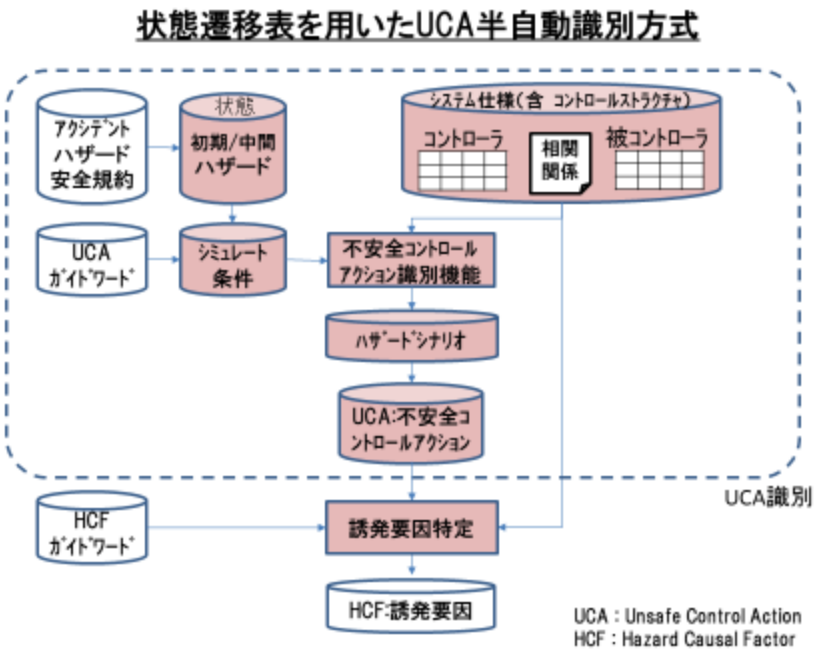
大阪工業大学　福澤　寧子

Osaka Institute of Technology　Yasuko FUKUZAWA

概要

システム安全解析手法 STAMP/STPA は、構成要素であるソフトウェアの異常や、コンポーネント間のインタラクション異常を特定できることから、コンポーネント間・システム間連携が高度化、複雑化する Internet of Things/Cyber-Physical Systems の安全・セキュリティ分析手法として期待されている。本手法では、システム間構成を示すコントロールストラクチャから、ガイドワードに則ってハザードにつながる非安全なコントロールアクション（UCA）を識別する工程と、ガイドワードに則って UCA 毎のハザード要因を特定する工程から成る。しかし、ガイドワードを使いこなして網羅的に分析することが困難であることから、コントロールアクション(CA)が与えられる状況を系統的に定義することで、UCA 識別検討範囲を絞ることが提案されているが、更なる効率化が望まれる。

そこで、本発表では、コントロールストラクチャにおけるコントローラおよび被コントローラの仕様を状態遷移仕様で表し、その状態遷移仕様に対して、ハザードとなる状態への到達可能性を、ガイドワードに則ってシミュレートすることで、UCA を半自動的に識別する方式を提案する。さらに、中間状態などの制約条件を与えることで、シミュレーションの効率化を行う。提案方式の有効性と取組を報告する。



キーワード

(1) システム安全・セキュリティ解析

(2) STAMP/STPA

(3) 有限状態マシン

(4) 状態遷移表

(5) 到達可能性解析