

第 3 回 STAMP ワークショップ発表概要

タイトル

STPA の損失シナリオ特定時におけるシナリオ記述への木構造の導入

Introducing a Tree Structure to a Scenario Derived in STPA Analysis

著者・発表者

日立製作所 竹下若菜、峯博史

Hitachi, Ltd. Wakana Takeshita, Hiroshi Mine

概要

本発表では、STPA 分析中の損失シナリオ特定時のシナリオの記述において、木構造による記法の導入を提案する。従来、シナリオの記載では、自然言語による文章、あるいは、ヒントワードを横軸、UCA を縦軸とした表形式による記法が主流であった。そのような記法において、1 つのシナリオは 1 つの文章として記載される。そのため、検討したシナリオの一部を別の分析時に再利用するのが困難であった。また、人に依存した記法であるため、網羅性の把握が難しく、他者によるレビューが困難という課題も生じていた。本発表では、シナリオの記載における木構造の導入を提案する。本提案において、木構造は FTA と似た構成をとる。木構造は各事象を表すノード、AND/OR ゲート、ゲートとノードをつなぐエッジによって構成される。1 つのシナリオは複数のノード、複数のゲート、複数のエッジから構成される。1 つのシナリオを複数のノードに分割して記載可能であるため、シナリオの一部を他の分析において再利用することが可能となった。また、ヒントワードとノード、あるいは、コントロールアクションとノードを 1 対 1 に対応させることによって、全ヒントワードおよび全コントロールアクションを検討したかどうかを即座に示すことができるため、レビュー容易性も向上した。我々は本提案を自動運転システムに試行し、シナリオを木構造にて記載可能であること、および、同じシステム内の異なる UCA の分析過程で再利用が可能なこと、ヒントワードの検討範囲を確認可能であること、を確認した。

キーワード

- (1) STPA
- (2) 損失シナリオ
- (3) 木構造