第 2 回 STAMP ワークショップ発表概要

タイトル

電動アシスト自転車を対象にしたハザード分析/STAMP・STPA と数値シミュレーションの特徴比較

Hazard analysis for power assist bicycle/Comparison of STAMP/STPA and numerical simulation analysis

著者・発表者

会津大学　兼本　茂

The university of Aizu.　Shigeru Kanemoto

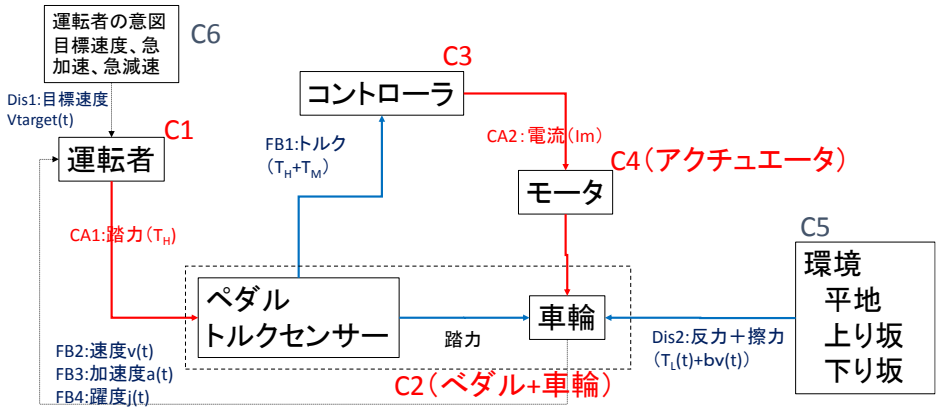
概要

STAMP/STPA は、従来の信頼性工学の FTA や FMEA によるハザード分析と異なり、対象システムの機能を抽象化・階層化したトップダウンの安全解析法として注目されつつある。人間と機械の協調による安全制御、インターネット接続や高度なソフトウェアなど複雑化したシステムの安全制御といった近年の新しい複雑システムの安全確保には、コンポーネント故障を最小化するという従来の信頼性工学的手法では十分でなく、コンポーネント間のコミュニケーションエラーまで含めたハザード要因をどのように抑制・制御するかというトップダウンの抽象的機能レベルでの安全設計が大事になる。

このような考え方の効用を具体的に検証するには、具体的事例に基づいた実践的検証が大事になる。本稿では、電動アシスト自転車という人間・機械の協調制御システムを例にとって、STAMP／STPA を適用して、どのようなハザード要因が分析可能かを検討する。さらに、SIMULINK に代表される数値分析によるハザード分析との比較により、STAMP/STPA の有用性を示す。

下図は、電動アシスト自転車の制御構造図とアクシデント、ハザード、安全制約の定義であるが、運転者、自転車本体（ペダル＋車輪）、アシストコントローラの加えて、運転者の意図と道路環境を外部コンポーネントとして定義し、制御アクションとして、運転者の踏力（CA1）とアシストトルク（CA2）を想定して分析をした。また、分析に際してのアクシデント、ハザード、安全制約も図に示したとおりであるが、人間の行動分析も大事であるため、コンテキストとして、スタート、走行、停止という三つの状況下でそれぞれ分析を行う。数値シミュレーションの結果は発表時にゆずる。

電動アシスト自転車の制御構造図



- アクシデント
  - 転倒、衝突による自損
  - 衝突による他損（こちらは今回は対象外とする）
- ハザード
  - バランスを崩した状態→転倒・衝突に至る意図しない（または想定外の）急加速または急減速
  - 転倒、衝突にいたる過大な速度
- 安全制約
  - 意図しない急加速、急減速をさせないアシスト機構
  - 過大な速度を出すアシストをしない
- コンテキスト
  - スタート時、走行時、停止時を考慮して分析。路面状態（段差、登坂）はシナリオの中で考慮。下り坂や凍結路面は今回は考慮しない

キーワード

(1) STAMP/STPA

(2) Power assist bycicle

(3) Numerical simulation

(4) Human-machine system

(5) Hazard analysis