第 3 回 STAMP ワークショップ発表概要

タイトル

STAMP/STPA を用いた自動運転車両の安全解析　～操舵系に関するミスユース～

Safety analysis of autonomous driving vehicles using STAMP / STPA ~ Misuse related to steering system~

著者・発表者

(株)ジェイテクト　森木　紘平

JTEKT CORPORATION　kohei MORIKI

概要

自動運転車両の安全設計を考える上で、自動車分野向けの電気・電子システムの故障に関する機能安全規格 ISO 26262 がある。また、システム故障以外の安全上のリスクを想定した、性能限界・ミスユース（誤使用、誤操作）時の安全性の標準である SOTIF（Safety Of The Intended Functionality）に対応することも必要である。

自動運転車両（自動化レベル 3）のミスユースでは、ドライバが運転する手動運転の状態があり、自動運転システムとドライバの間のコミュニケーションで不整合があると、自動運転車両が不安全な状態になることがある。例えば、システム設計者が推奨する使い方と異なった不適切な使い方をドライバがしたときのような状況（誤使用）や、システム設計者が推奨する使い方をする意志があるが、結果的にドライバが操作を誤ってしまう状況（誤操作）が発生するときである。

上記のようなミスユースの中でも、自動運転システムとドライバの間でコミュニケーションの不整合が表れやすい状況として、自動運転と手動運転が切り替わる際のミスユースに着目する。このミスユースの状況下において、ジェイテクトが専門とする操舵システムと HMI（Human Machine Interface）を含む自動運転システムとの複雑な相互作用に対して、網羅的かつ効率的な安全解析が可能となる STAMP/STPA を活用した。

本稿では自動運転と手動運転が切替る際のミスユースに対して STAMP/STPA で安全解析を行い、このミスユースを解決すべき課題を抽出することを目的とする。また、抽出した課題の中から、操舵系に関与する課題について、実施した実機検証についても報告する。

キーワード

(1) 自動運転

(2) SOTIF

(3) ミスユース

(4) STAMP/STPA

(5) ステアリングシステム