

# 第 2 回 STAMP ワークショップ発表概要

## タイトル

自動運転系の安全・セキュリティ解析のための自動化ヒューマンファクタに基づく STPA ガイドワードの提案

A Proposal of The Refinement STPA Guide Words on Human Factor of Supervisory Control Systems for Safety (Security) Analysis of Automated Vehicles

## 著者・発表者

日立製作所 永井 康彦

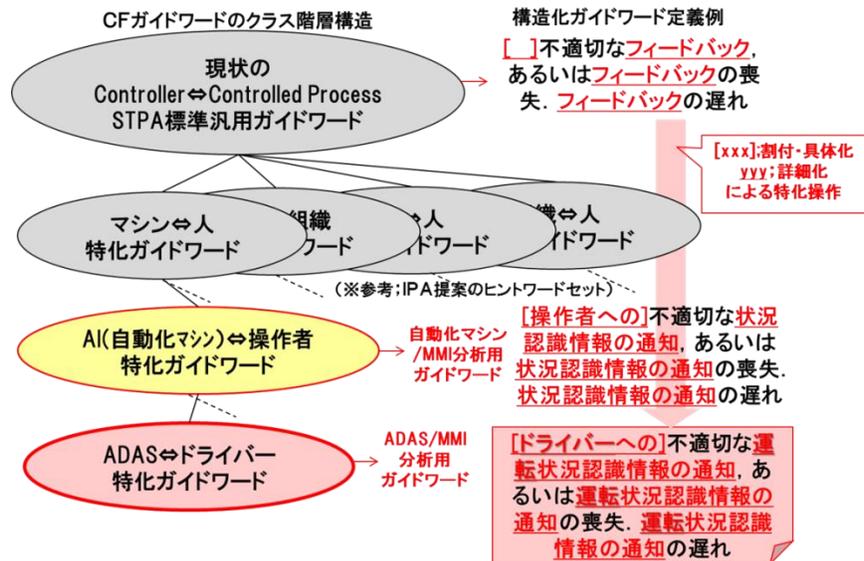
Hitachi, Ltd. Yasuhiko NAGAI

## 概要

新たなシステム安全（セキュリティ）解析手法 STAMP/STPA が、従来手法では見出せない構成要素のソフトウェア異常や要素間のインタラクション異常等のシステム特性に関する異常も特定できる手法であることから、IoT/CPS 時代の複雑化したシステムの解析に適した手法と注目され始めている。特に今後は、A I 等自動化利用の監視制御系（S V C ; スーパーバイザリコントロールシステム）の M M I （マンマシンインタラクション）環境の増加に伴い、この環境のヒューマンファクタ問題の解決のために STPA 利用の安全・セキュリティ解析が有効になると考える。しかしながら、現状の C F ガイドワードでは汎用過ぎて S V C 系ヒューマンファクタ問題の要因を一般的エンジニアが適切な粒度で網羅的に抽出することは困難である。

そこで、本発表では、今後の IoT/CPS の中でも、AI 応用の知的システム利用において重要課題となる、人間とのインタラクション異常の分析への STPA の有効活用を目的に、先行航空分野の S V C 系ヒューマンファクタの知見をベースに、下図のように C F ガイドワードを構造化展開して S V C 系解析向けに特化し、容易に S V C 系ヒューマンファクタ要因を抽出可能とするガイドワードを提案する。また、自動運転車へのセキュリティ攻撃の簡単な事例を想定し、提案ガイドワードを用いた解析結果例について報告する。

# STPA/CFガイドワードの階層的クラス構造化定義



## キーワード

- (1) STAMP/STPA
- (2) システム安全 (セキュリティ) 解析
- (3) 監視制御系
- (4) マンマシンインタラクション
- (5) ヒューマンファクタ