# 第 2 回 STAMP ワークショップ発表概要

## タイトル

意図・要求記述レベルの STAMP/STPA 手法

The STAMP/STPA method of intentions and requirements description level

## 著者・発表者

株式会社ジェーエフピー　中村　洋

JFP,Inc.　Hiroshi　Nakamura

## 概要

組込みシステム技術協会における安全仕様化 WG では、安全が関わる要求を仕様化するプロセスとして「安全誘導型設計」に取組んでいる。この安全誘導型設計は、開発意図とシステム仕様をもとに安全性分析を行い、その結果に基づいて意図記述とシステム記述を繰返すことを特徴とし、「意図を書けば、安全性が高まる」ことを目指す。試行事例として仮想的な電動アシスト自転車開発を選び、この適用を試み、安全性分析を STAMP/STPA 手法を使用して実施した。

安全誘導型設計では意図と要求の記述を重視し、SSQL と呼ぶ意図記述言語を使用する。安全性分析に STPA 手法を適用するに当たって、システムアーキテクチャを記述する前に、SSQL で記述された、製品開発に関する意図とそれを反映する最初の要求をもとにして、次のようにして制御構造を描いた:

1)システムコンテキスト図からコンポーネントを抽出する

2)ユースケース図から人と機械の相互関係を識別する

3)意図・要求記述から機械内部の相互関係を識別する

非安全な制御行動の識別では、制御行動の非安全さは、自転車の運転状況に依存すると考え、状況変数を次のように抽出し、状況ごとに非安全な制御行動の識別を試みた：

1)フィードバックデータ

2)制御行動の結果を表すデータ

その結果、いくつかのハザードシナリオを識別することができ、得られた対策案の中から、意図の実現に適する推奨策を導出することができた。安全誘導型設計に STPA 手法は適していると考え、開発意図を STPA で分析し、製品の安全性、健全性を高めるために活用してゆきたい。

## キーワード

(1)　開発意図

(2)　安全性分析

(3)　電動アシスト自転車

(4)　状況変数