# 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

2017年11月28日
会津大学　名誉教授　兼本　茂
JASA安全性向上委員会

1

## 背景

- 日常生活に、高度な機能を持った人・機械協調制御型の工学製品が使われつつある
  - 訓練を積んでいない人の挙動は想定できないこともある
  - 事前の完全な検証ができない高度なソフトウェアによる制御が使われる可能性がある（AI、機械学習、画像認識、音声認識など）
  - 想定外のハザードや、外部状況によって矛盾する安全制御行動の分析が必要になる
- 現状の安全規格は、AIアルゴリズムや人間・機械協調型の安全機能は対象としていない

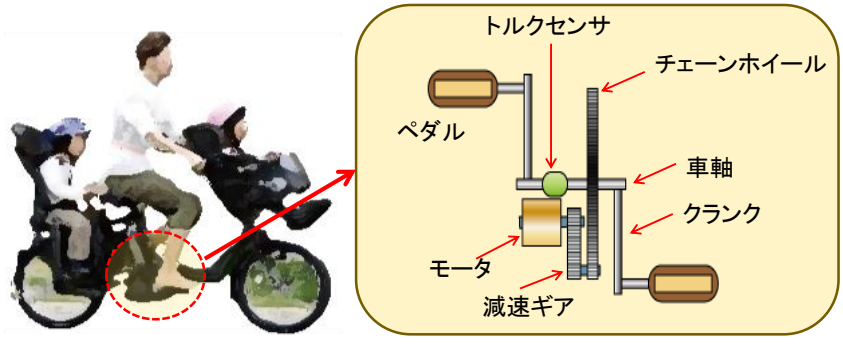
2

# 目的

- 人間・機械協調システムの事例として、「電動アシスト自転車」を取り上げ、STAMP/STPAによるハザード解析と安全設計の可能性を探る
- STAMP/STPAによる定性的なハザード分析と定量シミュレーションによる分析の役割分担を事例に基づいて検討する

3

# 電動アシスト自転車

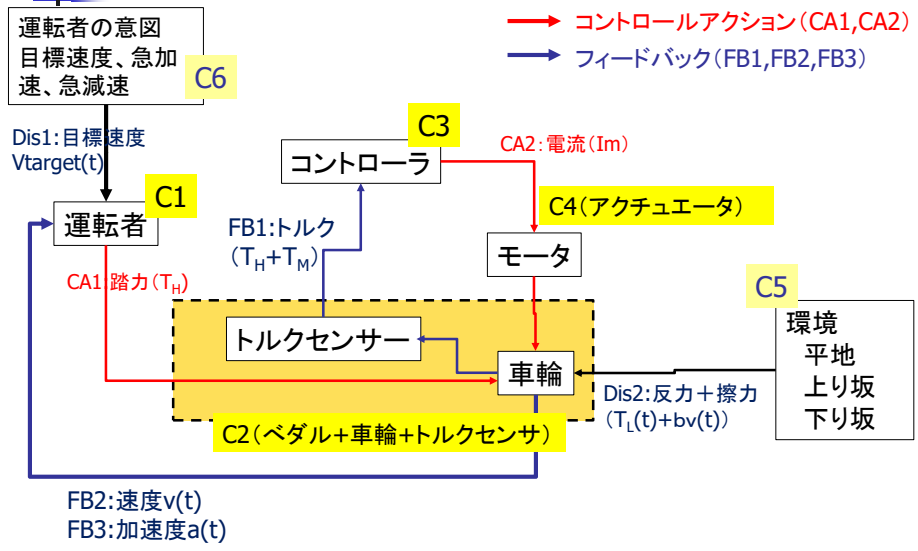



使用環境（Context）の理解
・スタート、走行、停止
・荷物で全重量は異なる
・段差、坂道など道路環境は多様

まずは、機能についての抽象的な理解が必要
「クランクのねじれから力（トルク）を計測して、力に応じたアシストをモータを使って行う」

4

# 電動アシスト自転車の制御構造図




# 抽象化／人間の挙動

- 運転者の意図（目標速度、加速、減速）を外部要因（Context)として分離。道路状況（段差や坂道）の運転者による認識は、捨象してモデルから外した。
- 運転者の行動を、意図と自転車の状況（速度、加速度）から踏力を決めるコンポーネントとしてモデル化

6

# 抽象化／自転車の挙動

実際のパラメータは、
重さ、タイヤ径、ギア比、ペダル半径・・・

抽象的理解
重さと推進力・負荷で速度を評価
キーパラメータは、アシスト力、人間とモータの応答速さ

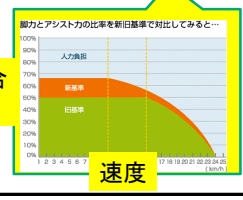
$$M\frac{dv(t)}{dt} = T_H(t) + T_M(t) - T_L(t) - b*v(t)$$

$$\tau_H\frac{dT_H(t)}{dt} = V_{target}(t) - v(t)$$

$$\tau_M\frac{dT_M(t)}{dt} = -T_M(t) + (T_H(t) + T_M(t))*R(v)$$

$$= -T_M(t) + T(t)*R(v)$$

アシスト割合
(0-0.5)




## シミュレーション パラメータの考察

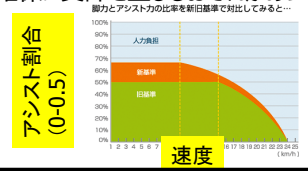
- 質量： 80kg <= 人間(60kg) + 自転車(20kg)
- 自転車のタイヤ 24インチ(24*25.4mm = 609.6mm)
  円周 = 2 * π * 609.6 mm/ 2 = 1.9m
- 自転車のギア比は 2.4～3.2のこと、ここでは 2.5 とする
- 定常スピードを10km/hとする → 10 * 1000m / (60*60) = 2.77 m/s
- 通常加速度：停止から20秒で定常スピードとなると仮定
  2.77m/s = α * 20s
  α = 2.77 / 20 = 0.1385 m/s²
- その時の力
  80kg * 0.1385 m/s² = 11.08(kgm/s²) → 11.08 N
- ペダル半径：160mm, ギア比2.5とすると
  ペダル倍率 = 1.9 m * 2.5 / (2 * π * 0.16m) = 4.75
- 体重60kgの人間の体重による力は 60*9.8m/s² = 588 N
- ペダル回転数：10km/h → 2.77(m/s) / 1.9 m = 1.457 回/s
  ギア比2.5では、1.457 (回/s) / 2.5 = 0.5828 回/s

# 規格の理解(1)
# JIS D 9115 (2013年)　駆動補助出力の抜粋

- 人力によるクランク回転出力を正確に検知する装置，　電動機の出力を正確に制御する装置などを備え，附属書 **A** に規定する走行速度及び駆動補助比率に関する基準を逸脱しないよう管理できる構造とする。
- 経年変化によって駆動補助比率などが，附属書 **A** に規定する基準を逸脱するおそれのない構造とする。
- 人力によるクランク回転出力に対して電動機が速やかに応答し，クランク回転出力の波形に対する電動機の出力波形が，おおむね相似であることによって，円滑で通常の自転車と同様のペダリング感覚を維持する構造とする。
- 電動機による駆動補助出力がクランク回転出力に対して円滑かつ比例的に発生することによって，運転者のペダリングに連動しない急発進，加減速など，安全な運転の確保に支障を生じるおそれがあってはならない。
- 走行する道路の勾配，積載重量の大きさなどによる乗員のペダリング運動負荷，体力的状態などに応じて，駆動補助比率を選択又は自動調整できる構造であることが望ましい。
- クランク回転出力がゼロとなった場合及び走行速度が，**A.1 c)** に規定する上限速度，又はその上限速度の範囲内で設定された駆動補助機能停止速度に達した場合，電動機による駆動補助出力を発生しない構造とする。

## 規格の理解(2)
## 附属書 A （規定）人の力を補う原動機の基準

- **A.1** 人の力を補うために用いる原動機が，次のいずれにも該当するものとする。
- **a)** 電動機とする。
- **b)** 24 km/h 未満の速度で自転車を走行させることとなる場合において，人の力に対する原動機を用いて人の力を補う力の比率が，次の **1)** 又は **2)** に掲げる速度の区分に応じ，それぞれ **1)** 又は **2)** に定める数値以下とする。
- **1)** 10 km/h未満の速度の場合は 2 とする。
- **2)** 10km/h以上，24 km/h 未満の速度の場合は，走行速度をキロメートル毎時（km/h）で表した数値から 10 を減じて得た数値を 7 で除したものを 2 から減じた数値とする。
- **c)** 24km/h以上の速度で自転車を走行させることとなる場合において，原動機を用いて人の力を補う力が加わらないものとする。
- **d)** **a)**~**c)** のいずれにも該当する原動機については，**a)**~**c)** のいずれかに該当しないものに改造することが容易でない構造とする。
- **A.2** 電動アシスト自転車は，原動機を用いて人の力を補う機能が円滑に働き，かつ，当該機能が働くことによって安全な運転の確保に支障を生じるおそれがあってはならない。




## Step-0 アクシデント、ハザードの定義

- 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
  - 転倒・衝突に至る意図しない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

# Step-1 UCA表(1)

| CA | 安全責任 | Not Providing | Providing causes hazard | Inappropriate Timming | Inappropriate Duration | Context |
|---|---|---|---|---|---|---|
| CA1: 踏力 | バランスを崩さないように急なトルク付加を避ける、高速すぎるトルク付加を避けるブレーキ操作については検討の対象外とする | 走らないので安全 | UCA1-P-1：急に強いトルクをかけ、コントローラアシストでさらなる急加速になって転倒<br>UCA1-P-2：意図に反してペダルを踏んで加速してしまって転倒 | 意図に沿ったトルクしかかけられないので対象外 | 対象外 | スタート時（道路状況はシナリオの中で考える） |
| | | 意図的な停止は安全 | UCA1-P-3：段差で急減速してバランスを崩して転倒 | 意図に沿ったトルクしかかけられないので対象外 | 対象外 | 走行時 |
| | | 意図的な停止は安全 | UCA1-P-4：停止時に間違えてペダルを踏んで加速して転倒 | 意図に沿ったトルクしかかけられないので対象外 | 対象外 | 停止時 |

# Step-1 UCA表(2)

| CA | 安全責任 | Not Providing | Providing causes hazard | Inappropriate Timming | Inappropriate Duration | Context |
|---|---|---|---|---|---|---|
| CA2: コントローラ指示 | 急な加減速による転倒を起こさない、高速になりすぎた際のアシストはしない | アシストがなくなってもゆっくりとしか加速しないので安全 | UCA2-P-1:運転者のトルクなしでアシストし、意図に反した加速で転倒 | UCA2-T-1:スタート時にアシストが早くかかりすぎて転倒<br>アシストが遅れるのは急加速ではないので安全 | 対象外 | スタート時 |
| | | UCA2-N:登坂で急にアシストが切れてバランスを崩して転倒 | UCA2-P-2:高速走行でさらなるアシストがかかって早くなりすぎて衝突、転倒 | UCA2-T-2:登坂時にアシストが遅れてバランスを崩して転倒 | 対象外 | 走行時 |
| | | 停止時にアシストが切れても安全 | UCA2-P-3:停止時に急にアシストが作動して加速して転倒 | 停止時はアシストのタイミングは関係なし | 対象外 | 停止時 |

## ハザードシナリオ（運転者の踏力、CA1）

- UCA1-P-1:(スタート時）急に強いトルクをかけ、コントローラアシストでさらなる急加速になって転倒
  - HS1:ヒューマンエラーによる急加速で転倒
    - →乗り方の訓練＋停止時からの急なアシストによる加速を避ける機構の追加
- UCA1-P-2:(スタート時）意図に反してペダルを踏んで加速してしまって転倒
  - HS1:ヒューマンエラーによる想定外の加速で転倒
    - →乗り方の訓練＋停止時からの急なアシストによる加速を避ける機構の追加
- UCA1-P-3:(走行時）段差で急減速してバランスを崩して転倒
  - HS1:段差に減速せずに突っ込んで転倒（アシストに関係なく起こる事象だが、アシストがあることで油断してわずかの段差で想定以上の減速になりうる）
    - →段差の前で減速する習慣づけ
- UCA-P-4:（停止時）に間違えてペダルを踏んで加速して転倒
  - HS1：停止時に間違えてペダルを踏んで加速して転倒
    - →乗り方の訓練＋停止時からの急なアシストによる加速を避ける機構の追加

## ハザードシナリオ（コントローラ指示、CA2）

- UCA2—P-1:(スタート時）運転者のトルクなしでアシストし、意図に反した加速で転倒
  - トルク誤計測、コントローラ故障で、意図に反した急加速指示をする（モータは停止故障のみ）
    - →トルクセンサーを安全側故障の機構にする、故障検知機構を追加する、コントローラの設計時の検証を十分に行う、定期的保守を行う
- UCA2-T-1:(スタート時）にアシストが強くかかりすぎて転倒
  - アシスト機構の設計が不十分で、過大なアシストがかかってしまう
    - →最大限のアシスト制限（速度Xm/Hrで50%、それ以上でアシストなしなど）。低速でのアシスト制限（速度Ym/Hrまでは徐々にアシストを増やす）
- UCA2-N:(走行時）登坂で急にアシストが切れてバランスを崩して転倒
  - 登坂中にトルク誤計測、コントローラ故障、モータ故障で、急にアシストがなくなる。
    - →定期的な保守。アシストが切れる際の慣性機構も可能であれば、ゆっくりアシストが切れる
- UCA2-P-2:(走行時）高速走行でさらなるアシストがかかって早くなりすぎて衝突、転倒
  - 高速走行でアシストがかかって、さらに高速になり制御付加で衝突または転倒
    - →速度Xm/Hr以上で徐々にアシストを低減させる
- UCA2-T-2:(走行時）登坂時にアシストが遅れてバランスを崩して転倒
  - 登坂時にアシストが遅れてバランスを崩して転倒
    - →アシストは、X秒以下の遅れで行う。重い荷物の際にアシストが弱くなったり遅れないように設計する
- UCA2-P-3:（停止時）に急にアシストが聞いて加速して転倒
  - 停止時にトルク誤計測、コントローラ故障で急なアシストがかかって転倒ないし衝突
    - →停止時の故障で加速しないようなフェイルセーフ設計

## STAMP/STPA論理モデル
## ～トレーサビリティの確保のためのデータ構造～

- Accident:＜A1＞:＜転倒・衝突＞
- Hazard:＜H1＞:＜急加速・急減速＞of〈C1、C2・・〉LeadTo＜A1＞
- SafetyConstraint:＜SC1＞:＜意図しない急加速・急減速をしない＞for〈H1〉

- Component:＜C1＞:＜運転者＞
  - Property：＜人間、制御装置、物理プロセス、外乱など＞
  - ProcessModel::＜コンポーネントの状態、入力と出力の因果関係＞
- ControlAction:＜CA1＞:＜踏力を加える＞from＜C1＞to＜C2＞
  - ErrorOntology：＜コンポーネント組合せに応じたガイドワード＞
  - UCA-N/P/T/D：＜UCA1-P＞:＜急加速＞LeadTo＜H1＞＆＜CSC1＞
    - HS:＜HS1＞：＜意図しない急加速で転倒＞LeadTo＜CSC1＞
- Feedback:＜FB1＞:＜速度＞from＜C2＞to＜C1＞
- Disturbance:＜Dis1＞:＜意図的な加速＞from＜C6＞to＜C1＞
- ComponentSafetyConstraint：〈CSC1〉：＜内容＞

## 定量シミュレーションによる分析

動的モデル

運動方程式
（走行速度と質量）

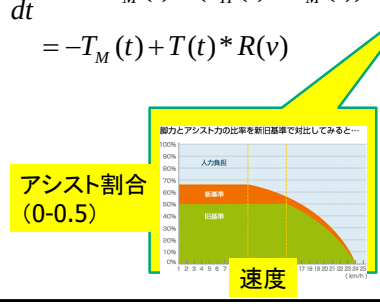
$$M\frac{dv(t)}{dt} = T_H(t) + T_M(t) - T_L(t) - b*v(t)$$

踏力$T_H$の制御
（目標速度への追随）

$$\tau_H\frac{dT_H(t)}{dt} = V_{target}(t) - v(t)$$

アシストカ$T_M$の制御
（踏力と速度に応じた
アシストカ）

$$\tau_M\frac{dT_M(t)}{dt} = -T_M(t) + (T_H(t) + T_M(t))*R(v)$$
$$= -T_M(t) + T(t)*R(v)$$



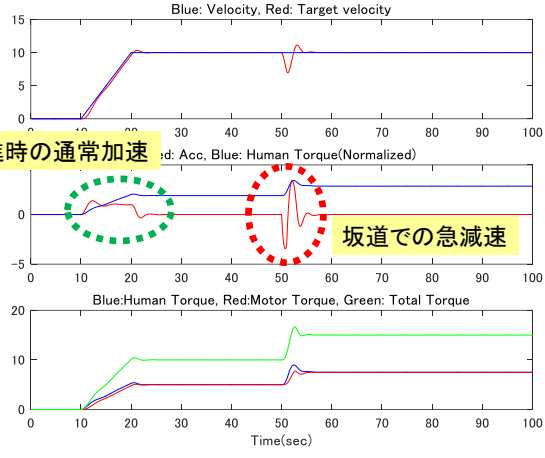
# 定量シミュレーション例
# ～スタート加速と、段差での急減速～

速度ゼロから開始し、10km/hに加速、途中で道路負荷をステップ状に増加

青：目標速度
赤：速度

青：人間の踏力
赤：加速度

青：人間の踏力、
赤：モータトルク
緑：全トルク




発進時の通常加速

坂道での急減速

標準値：tauH=1.0、tauM=0.5、b=1.0、M=0.5、dt=0.1

17

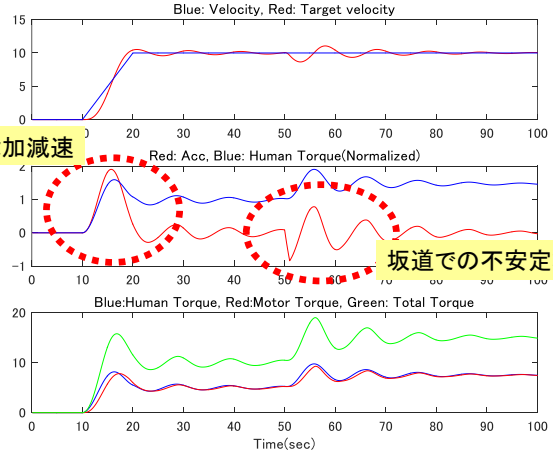
# 定量シミュレーション例
# ～スタート加速と、段差での急減速～

速度ゼロから開始し、10km/hに加速、途中で道路負荷をステップ状に増加

青：目標速度
赤：速度

青：人間の踏力
赤：加速度

青：人間の踏力、
赤：モータトルク
緑：全トルク




不安定な加減速

坂道での不安定な加減速

質量を10倍：tauH=1.0、tauM=0.5、b=1.0、M=0.5*10、dt=0.1

18

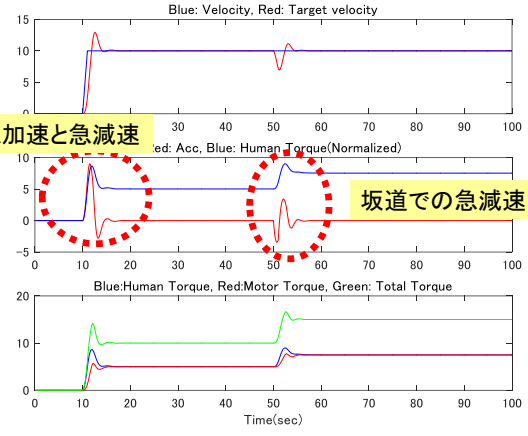
# 定量シミュレーション例
# ～スタート加速と、段差での急減速～

速度ゼロから開始し、10km/hに急加速、途中で道路負荷をステップ状に増加

青：目標速度
赤：速度

青：人間の踏力
赤：加速度

青：人間の踏力、
赤：モータトルク
緑：全トルク




発進時の急加速と急減速

坂道での急減速

標準値：tauH=1.0、tauM=0.5、b=1.0、M=0.5、dt=0.1

19

# 定量シミュレーションのまとめ

- 定性的挙動は妥当。急な坂道では、急減速で転倒の可能性がある、質量を重くすると遅れて加速しオーバーシュートして落ち着く、など。
- ハザード（加速度の状態）の定義が必要、例えば、下記
  - 緑丸の場所（最初の始動時）は、ゆっくりと加速するので、人の意図（踏力）と加速度は、整合性がある（安全側）。
  - 赤丸の場所（ステップ状で急に坂道になったとき）では、人間の踏力は追いつかず、急激な減速が起こっている。これが転倒につながる。
  - 急発進でも、同様に、急加速、速度のオーバーシュートが起こって転倒につながる
- 各コンポーネントの定性的挙動（入力が増加すれば出力がどうなるかといったこと）を定義すれば、ハザードの定性的予測はできそう（定性推論によるハザード分析／インパクト解析）
- HCF（ハザード誘発要因、シナリオ）は、UCAごとに人が考えるしかない
- 偏差注入（発進や急減速）の選択が、その変化速度と変化量を組み合わせると無限大になる

# 事例分析から何がわかったか？

STAMP/STPAは、
- 安全制御構造図の作成に際して定性的なシステム挙動の理解は必要
- 細部にとらわれすぎない抽象化モデルの作成が重要
- Worst caseを想定したハザード分析は案外と簡単
- 適用状況（Context)の分類分けなどは、「整理学」ともいえるが、これで分析がかなり容易になる。
- アクシデント、ハザード、システム安全制約、コンポーネント安全制約の間のトレーサビリティ（論理的整合性）を確保できる

***両者のベストミックスが大切***

定量シミュレーションは、
- 本当にハザードになるかは定量シミュレーションが必要
- 応答時間の速さや重量などは定量シミュレーションでの感度分析が有用

しかし
- ハザードの定量基準を設定するのは簡単ではなく、最終的なハザード判定には定性的判断が入ってしまう

21

# 今後の課題

- 「これからの」複雑システムの安全論証の課題
  - 複雑システム（人と高度なソフトウェアを含んだシステム）の安全とセキュリティは創発特性を持つ（N.G.Leveson)、また、想定外の事故・故障も起こっている
  - しかし、創発特性や想定外事象は論理的・還元論的には説明できない・・・
  - 現状の規格では、この人と高度なソフトウェアを含んだ安全論証は避けられている
- 複雑システムのプロアクティブな安全論証
  - 現状は、事故の発生後の原因究明と対策という後追い（リアクティブ）の論証（説明）になっているが、システム開発時に予見的（プロアクティブ）な安全論証をすることが望まれる
  - STAMPの基本コンセプトは、複雑システムを、抽象化・階層化によって理解し、安全制約を構築するものであるが、これが、プロアクティブな安全論証を可能にするかは、実践による裏付けが必要（コンセプトフェーズでの論証）
  - 他の複雑システムの安全分析法（FRAM、Safety-II、Safety2.0など）との組み合わせ
  - モデル化と形式手法による証明、使用実績による論証（Proven in use）など、複雑なものをそのまま捉えた論証法との組み合わせ
  - 論証結果の表現法（可視化、ツール化）・・Safety Case、GSNなど

22