第2回STAMPワークショップ発表資料

意図・要求記述レベルの STAMP/STPA手法
--安全誘導型設計におけるハザード分析--

2017年11月28日
組込みシステム技術協会(JASA)　安全仕様化WG主査
株式会社ジェーエフピー　顧問
中村　洋

はじめに

◆背景

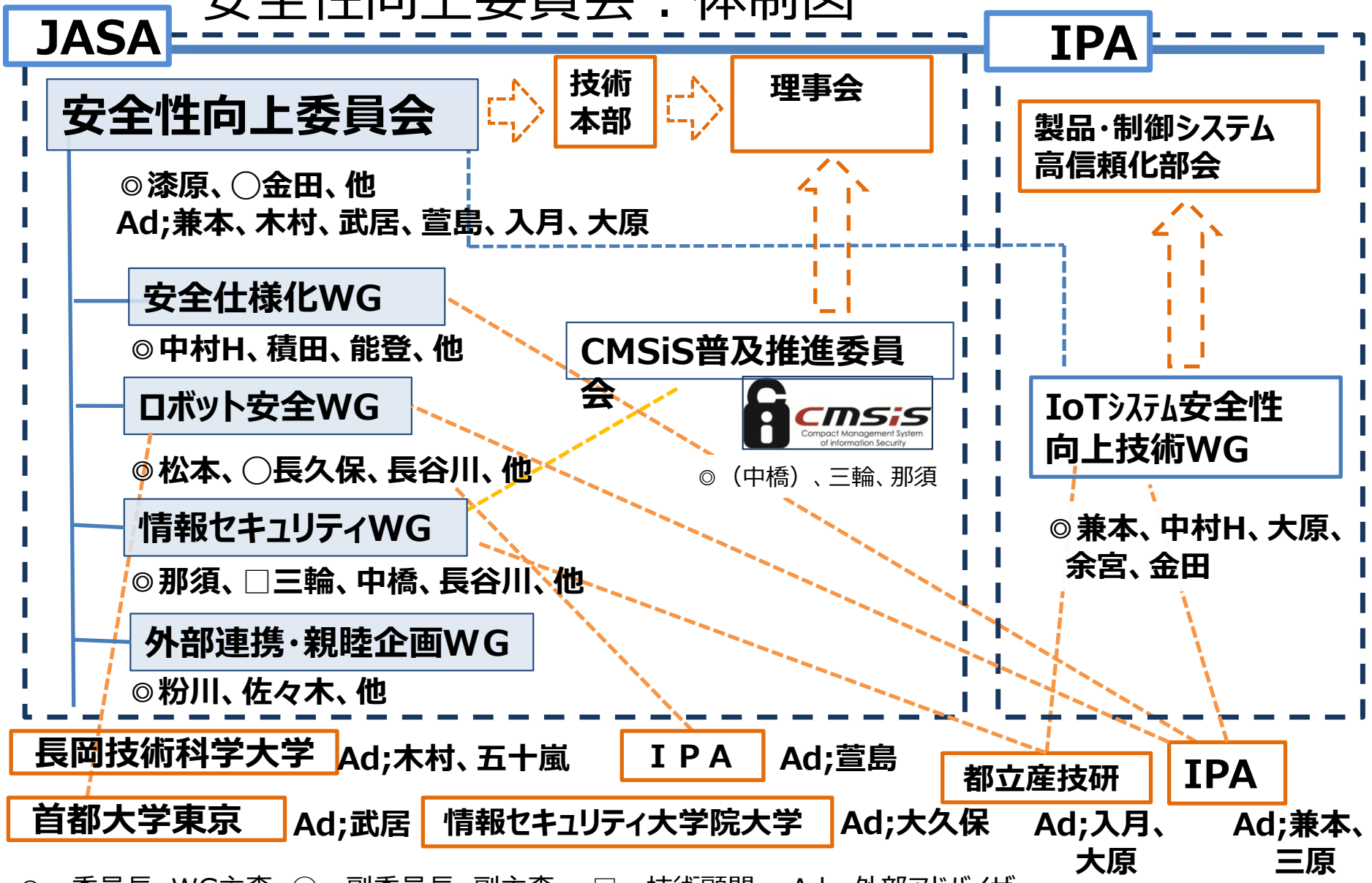
- JASA(組込みシステム技術協会)の安全性向上委員会は、2012年度から3年間、意図したものが実現できる要求定義を求めた活動に取組んだ。
- 2015年度からは安全仕様化WGに衣替えし、安全が関わる要求を仕様化するプロセスを研究し、安全誘導型設計と呼ぶプロセスモデルを提案した。
- その試行事例として、仮想的な電動アシスト自転車開発を選び、STAMP/STPA手法を使用してハザード分析を試みた。

◆発表内容

- 安全仕様化WGの紹介
- 電動アシスト自転車開発に関する意図・要求の記述
- 意図・要求記述レベルのSTPA分析の流れと結果

安全性向上委員会：体制図

2017/4/21 R3



◎；委員長、WG主査　○；副委員長、副主査　□；技術顧問　Ad；外部アドバイザー

2017年度活動計画：安全仕様化WG

改訂:5/19/2017

◆目的
- 安全が関わる要求を仕様化するプロセスの研究
- その仕様化を支援する方法論(プロセスモデル又は手法)の提案

◆方針
- 重点課題を共有し、自主的に活動し、相互啓発を図る。
- IPA/SECの関連WG等との連携を図る。

◆重点課題
- 安全誘導型設計を支援する手法及びツール
- 特に、STAMP/STPA、FRAM、SSQL、Sim4stamp

◆題材
- 電動アシスト自転車(メーカとの交流、連携を含む)
- ロボット安全WGの題材(交流、連携を図る)

◆活動方法
- 月1回の会合で活動成果を報告・討議する。
- 常時、メールを利用して情報・意見交換を進める。
- 適宜、勉強会を計画する。

要求の仕様化に関する現状と課題

◆意図が示されない

- 2012年度から3年間、意図したものが実現できる要求定義を求めた活動に取組み、要求の仕様化に関する開発現場における課題をまとめた。
- 顧客との関係では、顧客の意図が示されないこともあるが、それでもソフトウェアは作成できてしまうという課題があった。仕様の間違いに気づきにくいことが問題。

◆暗黙知は要求として書かれない

- 顧客側の暗黙の了解、技術的又はビジネス的常識、慣習などが伝わらない現状が、未解決。
- 開発側のオープン化が進むにつれて、意思疎通が一層の課題。

◆安全実現性の検証が難しい

- 技術と社会の高度化、複雑化が進展。
- 要求段階において意図する安全の実現性を検証したいが、適切な手法が定着していないのが現実。

その解決策：安全誘導型設計

◆適用分野
- 組込み製品を対象とするシステム開発
- 一般的に、安全が関わるシステム開発

◆適用プロセス
- システム開発においてコンポーネント設計に先立ち、システム全体の要求を分析し、構造を設計するプロセス

◆利点
- 要求分析段階において、安全性の検証と安全の作り込みを支援。
- 要求仕様が意図したことを実現しているかという、意図実現性の検証を支援する。

意図を書けば、安全性が高まる

命名時の思い：
- 意図に照らして、安全か非安全かを判断し、
- 安全が実現する方向に進めば、要求と構造を適切に設計できる

試行事例の概要

◆対象システム開発
- ■ 仮想的な電動アシスト自転車の開発

◆対象機能
- ■ バッテリーと自転車本来の機能を除き、電動アシスト機能に限定

◆安全誘導型設計の適用範囲
- ■ 意図記述　(、システム記述の一部)
  - ●意図体系テンプレートを作成
  - ●SSQLを用いて意図・要求を記述
- ■ ハザード分析
  - ●STAMP/STPA手法を適用

◆参照資料
- ■ ヤマハ製電動アシスト自転車　PASナチュラL取扱説明書

SSQL : SSQ's intentions describing Language

参考：電動アシスト自転車の事故が相次ぐ

経済産業省によると、2014年の出荷台数は約47万台。11年にはオートバイを超え、10年で約２倍になった。鹿児島市など多くの自治体が、高齢者の車の事故防止や環境への配慮のため、電動自転車の購入に補助金を出しているほか、「レンタサイクル」での導入も進んでいる。

普及にともなって事故も増加した。警察庁によると、電動自転車による交通事故件数は15年に1394件。この10年で500件増えた。

公益財団法人「交通事故総合分析センター」（東京・千代田）の調査では、自転車事故の死者数は全体では11年に578人で01年から４割減ったが、電動自転車に限ってみると11年に50人となり、10年間で３倍と急増している。

特に、片足だけペダルに乗せ、もう片足で地面を蹴って勢いをつけて乗り出す「ケンケン乗り」での事故が目立つという。体全体が自転車に乗りきっていない不安定な姿勢のままでモーターが作動し、急加速してしまうことがあるためだ。

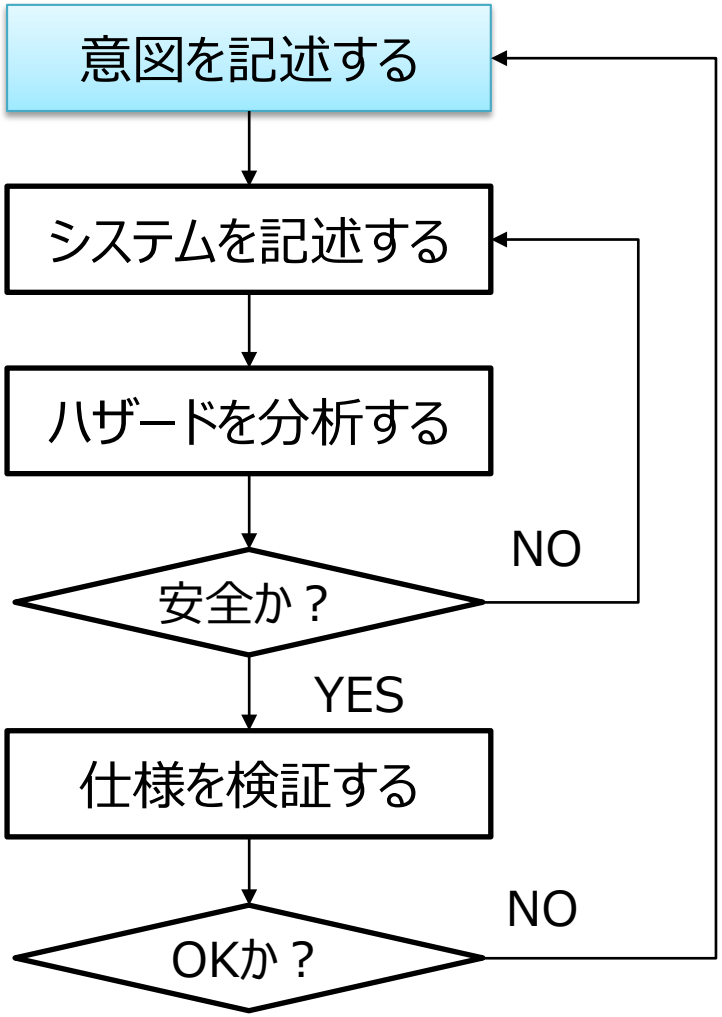
アシスト機能が優れていることで、車体の重さに気付きにくくなる点も危険という。車体は25～30キロの重量があり、自転車の専門家らでつくる「自転車の安全利用促進委員会」（東京・渋谷）の一員で自転車ジャーナリストの遠藤まさ子さんは「子供２人と親子で乗れば、全体で100キロを超える。アシスト機能によりスピードも出るので、ぶつかった時の衝撃が大きい」と指摘する。

出典:5/10/2016付けの日経電子版

まず、意図を記述する

==手法==

意図体系と意図構文に基づいて
安全が関わる
開発意図を記述する
意図記述手法



システム視点から
要求と構造を記述する
仕様記述手法

システム仕様をもとに
ハザードを分析する
安全解析手法

システム仕様に関して
SSQの実現を検証する
仕様検証手法

SSQ:Safety,Security and Quality

SSQL：意図記述言語

◆目的
- システム開発に関する意図を記述するための構文を提供する。
- 意図体系テンプレートの記述を可能にする。
- 既存の処理系の活用を可能にする。

◆特徴
- テンプレートに沿って意図とそれに関連する要求を記述できる。
- EARSパターン相当の要求記述構文が使用できる。
- SLPテキストへの変換によってSLP処理系が活用できる。

◆意図・要求構文
- 一般型2種：意図と要求の記述構文
- EARS型4種：EARSパターン準拠の要求記述構文

◆コメント構文
- SSQLコメント：意図体系テンプレートを記述するため
- SLPコメント：SLP言語に同じ

SSQL：SSQ's intentions describing Language
SLP：株式会社ジェーエフピーが開発し販売している要求記述言語

意図記述のための構文規則

		構文規則	SLP表現
一般型		x/P	Do <x>を{P}とせよ
		if(y/Q) x/P	if <y>が{Q}ならば Do <x>を{P}とせよ else Do nothing endif
EARS型	事象型	when(y/Q) 一般型	if <y>が{Q}という事象が発生したならば 一般型表現 else Do nothing endif
	状態型	while(y/Q) 一般型	if <y>が{Q}という状態にあるならば 一般型表現 else Do nothing endif
	環境型	where(y/Q) 一般型	if <y>が{Q}という環境にあるならば 一般型表現 else Do nothing endif

備考：xとyは「意図対象」。Pはxを目的語とする述語部、Qはyを主語とする述語部。
ここで、「述語部」とは、一つの文の中で主語又は1つの目的語を除く残りの部分とする。

例： if(アシスト力/急に大きくなる) アシスト機能/利用者が慣れないと感じる

意図・要求の記述-1

1.開発計画
1,1　納期
1.1.1　発売時期
　新年度セールスの目玉/本製品にする
(:　要求
　販売開始時期/3月後半とする
1.2　コスト
1.2.1　販売価格
　購入可否/主婦が一人で判断できる
(:　要求
　販売価格/10万円未満とする
1.3　品質を検査する手段
1.4　安全を検査する手段
2.開発目的
2.1　達成目標
2.1.1　競争優位
　ブランド地位/トップ状態に維持する
(:　要求
　連続アシスト距離/40kmとする
(:　業界最高水準を達成すれば、ブランド地位を維持できる

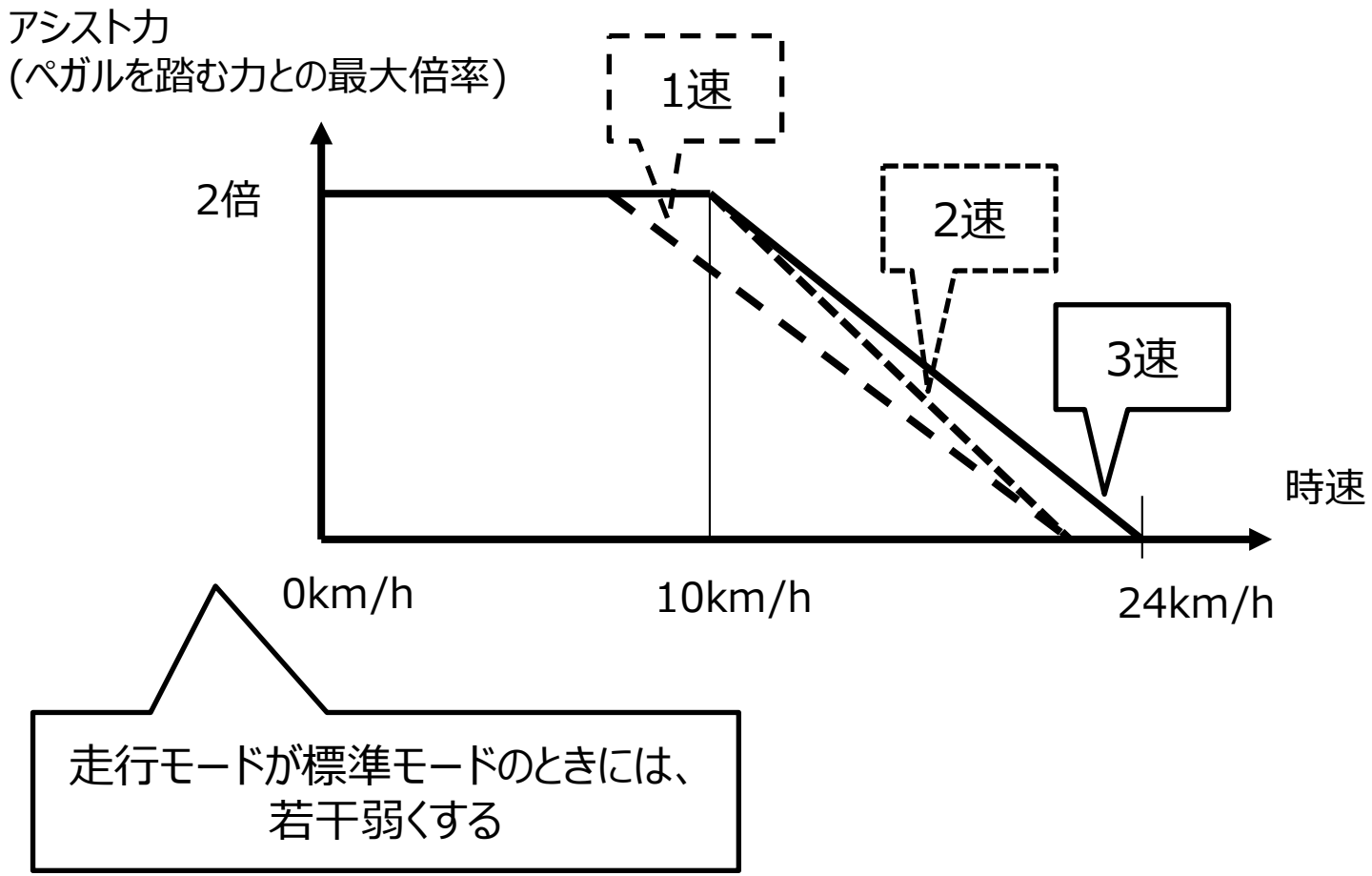
意図体系

コメント

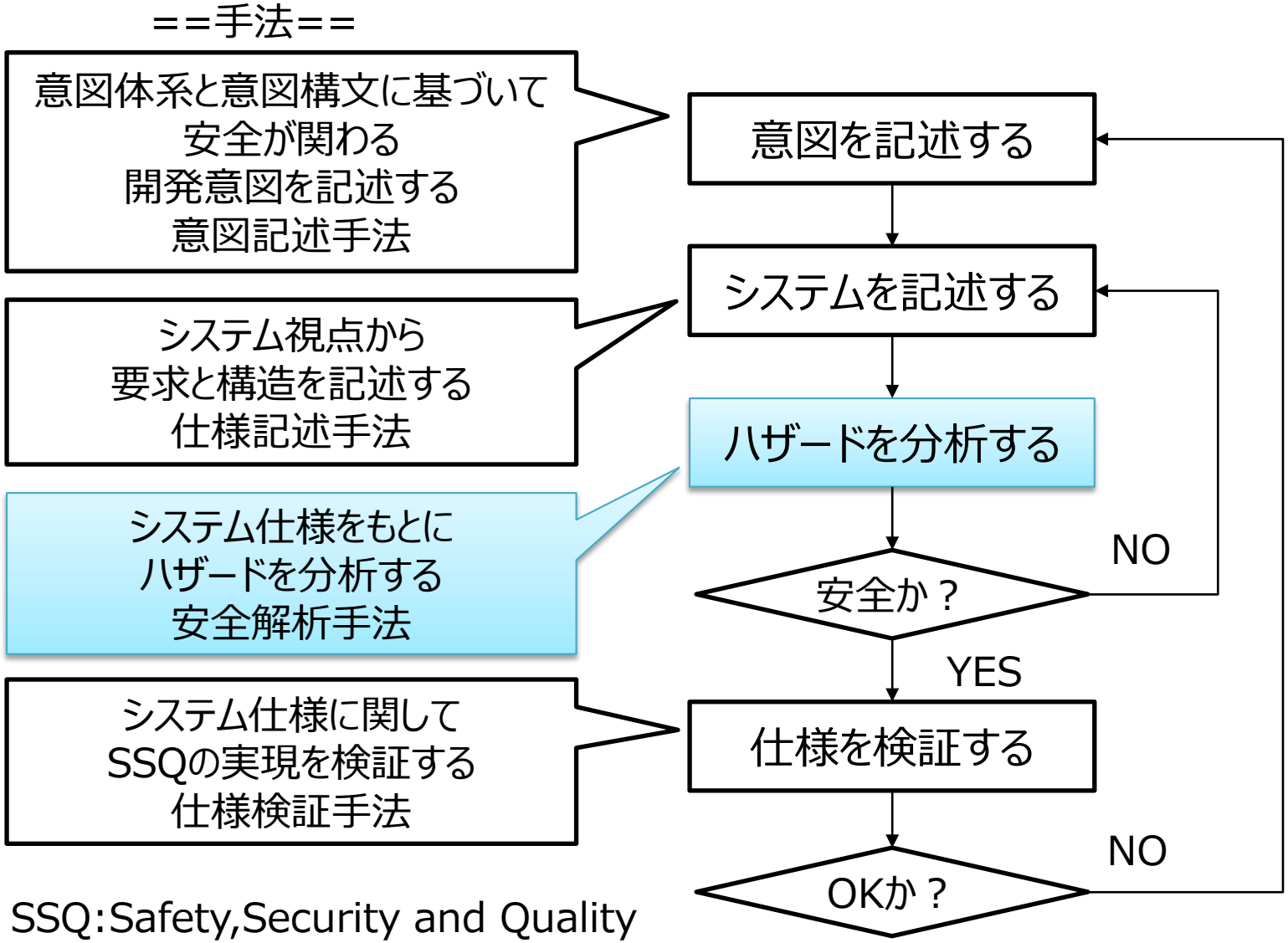
意図・要求の記述-2

2.2 システムに対する要求・制約
2.2.1 機能の利点
乗り心地/自然で滑らかにする
乗り心地/坂道でもパワフルで滑らかにする
(: アシスト基準
while(走行速度/時速10km以下) アシスト力/ペダルを踏む力1に対して最大で2まで
while(走行速度/時速10km超で24km未満) アシスト力/順次弱める
while(走行速度/時速24km以上) アシスト力/ゼロにする
(: SPEC3制御
while(変速位置/1速) アシスト力/時速10kmの手前で弱め始め、24kmの手前で止める
while(変速位置/2速) アシスト力/時速24kmの手前で止める
while(変速位置/3速) アシスト力/基準どおりにする
(: 走行モード
while(走行モード/強モードにある) アシスト力/標準モードより強い
when(電源/オンになる) 走行モード/標準モードにする
2.3 使用者に対する要求・制約
(: これ以降、略

アシスト基準



次に、ハザードを分析



SSQ:Safety,Security and Quality

アクシデント、ハザード、安全制約の識別

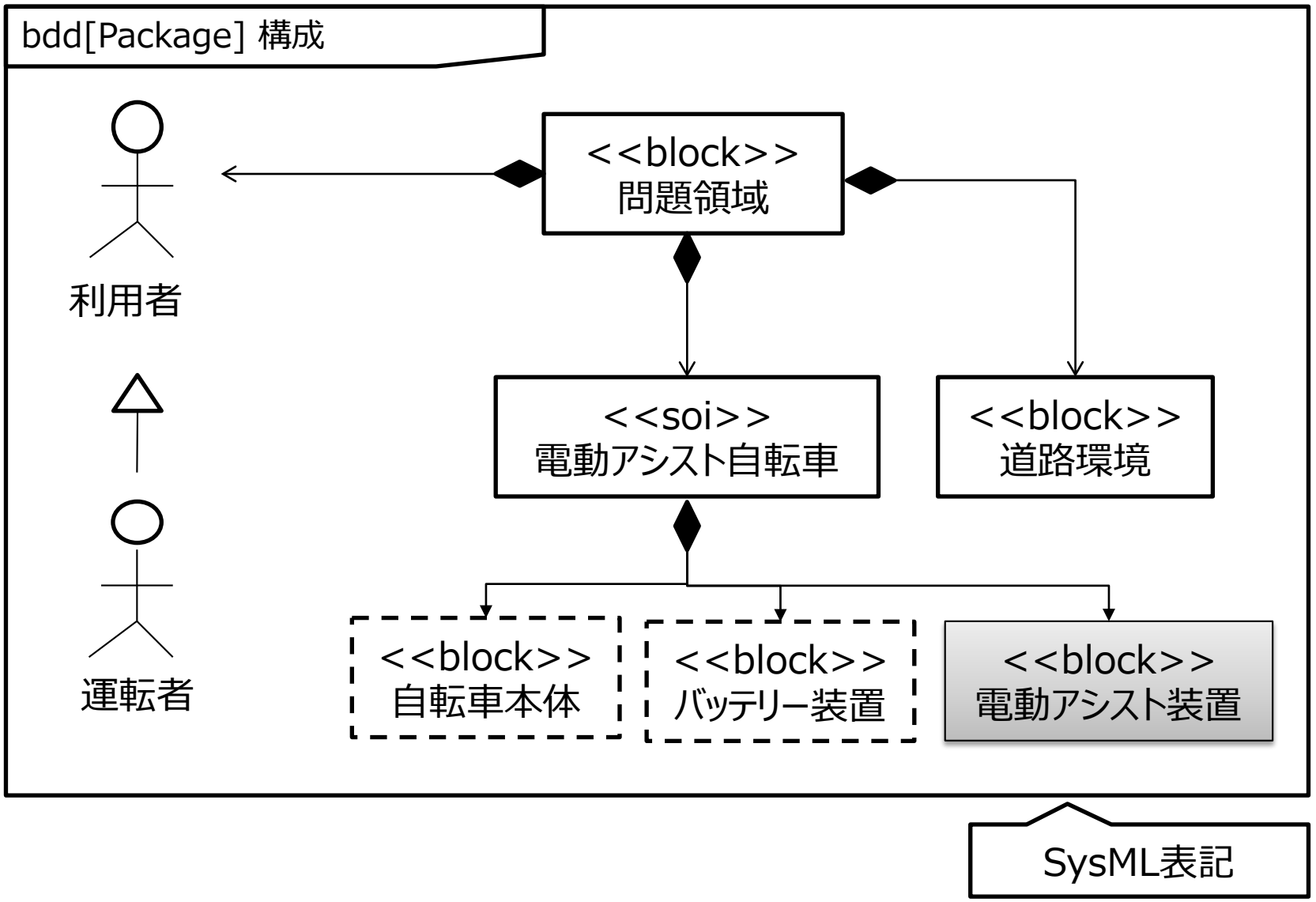
アクシデント	ハザード	安全制約
運転中の転倒又は衝突によるけが	意図しない急加速	意図しない急加速を防止する

次の意図記述から識別:

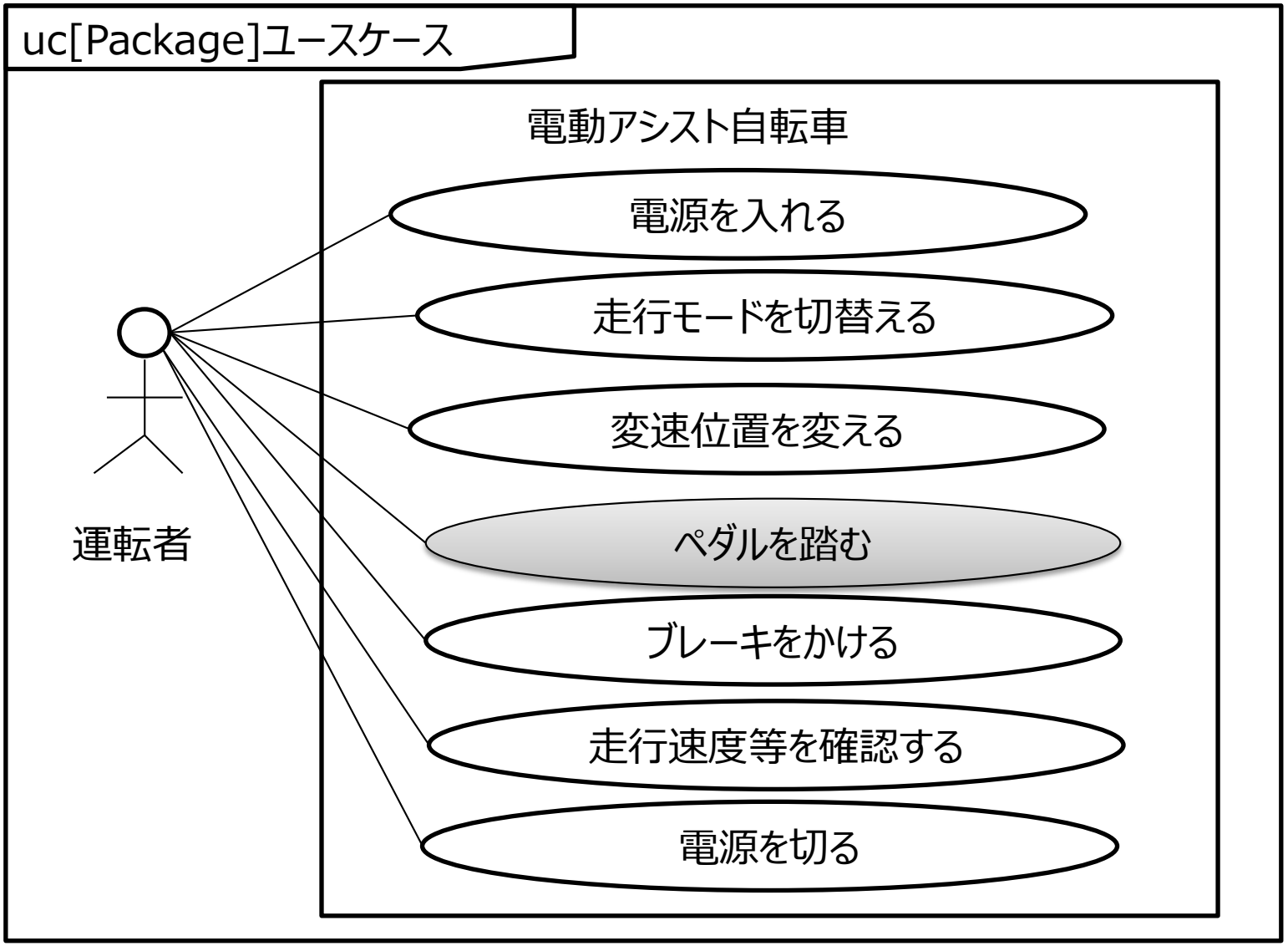
2.5　事故に関する情報
2.5.1　多発事故
　転倒によるけが/避ける
　衝突によるけが/避ける
(:　要求
　予期しないアシスト/急に作動させない
　速度の出し過ぎ/防止する

前提事項:
バッテリ関係、本来の自転車機能は分析の対象外とする

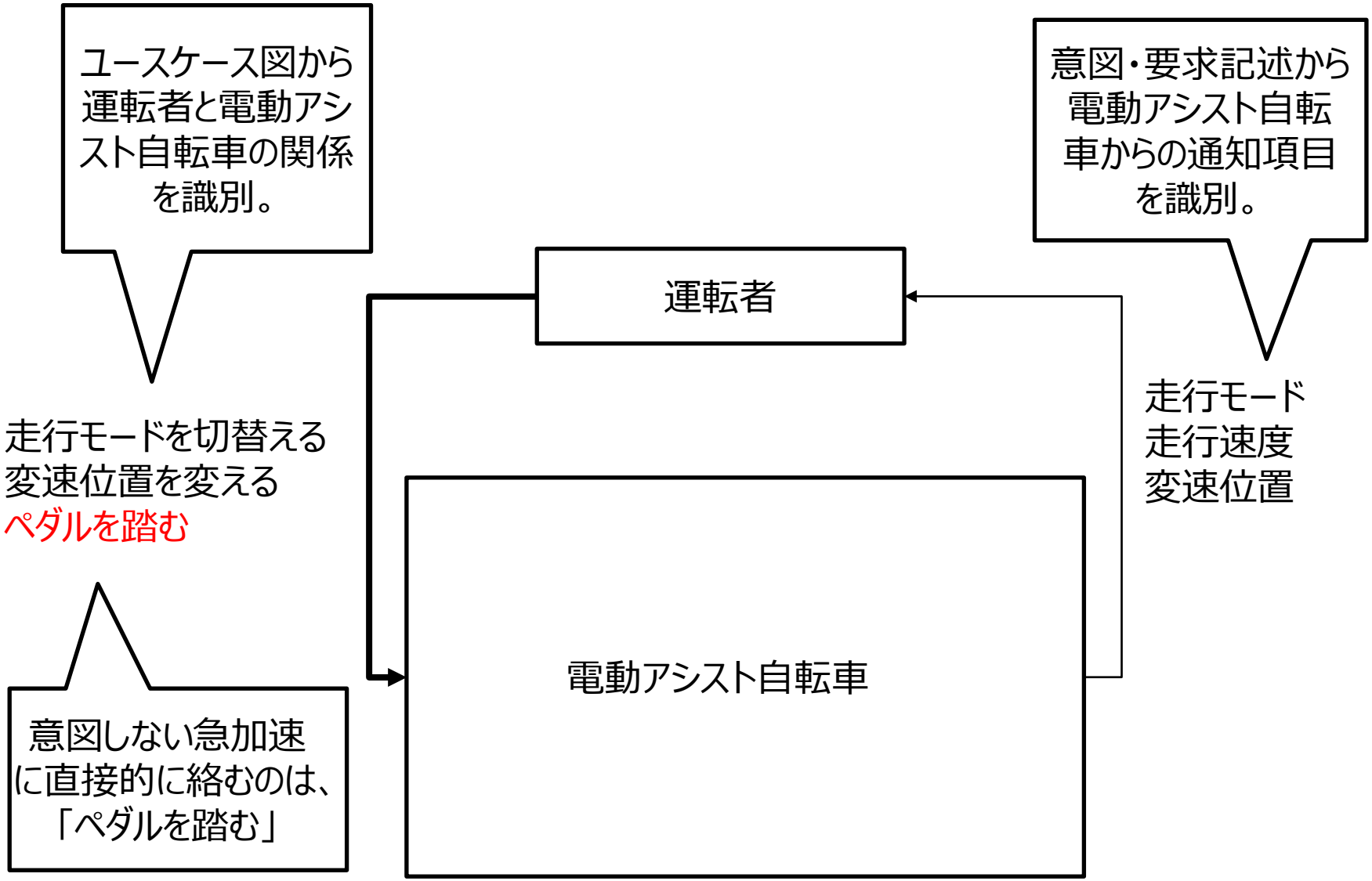
システムコンテキスト図：分析の範囲



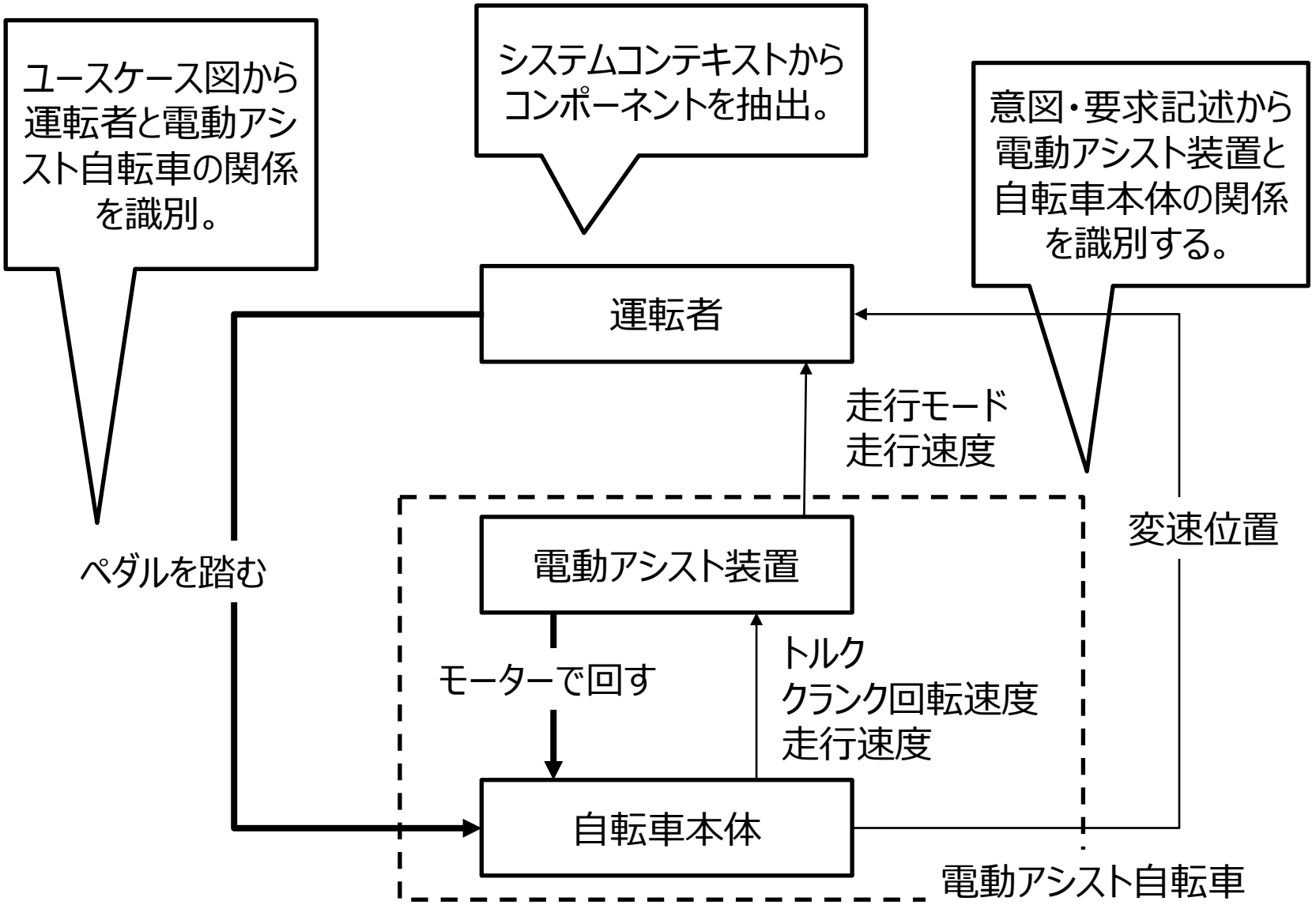
ユースケース図：運転者は何ができるか



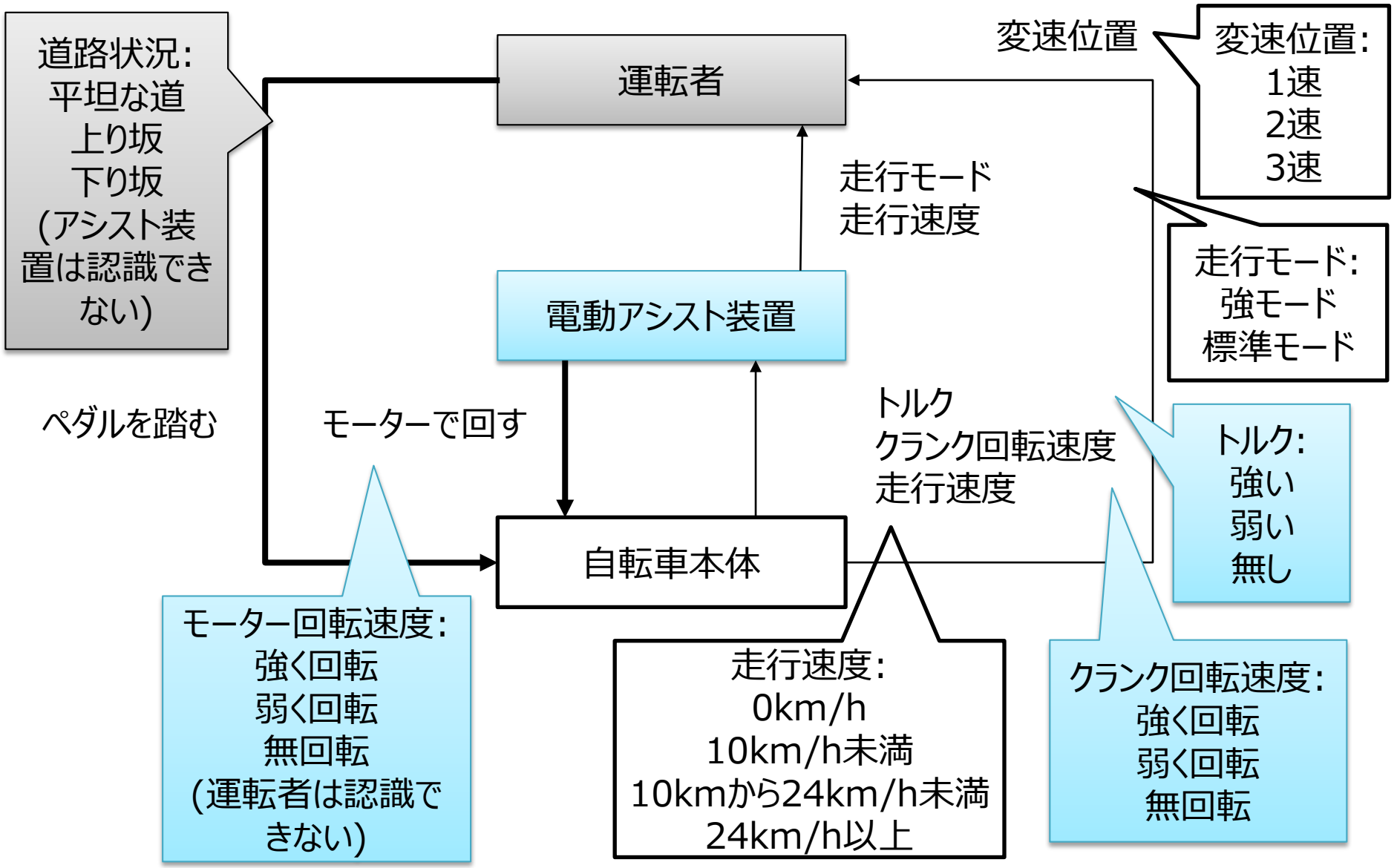
運転者と電動アシスト自転車の相互作用



制御構造図



制御行動に影響を及ぼす運転状況



状況変数の抽出

状況変数	制御行動を反映		フィードバックに対応	運転者認識の可否	同値分割数
	ペダルを踏む	モーターで回す			
トルク	✓		✓	X	3
クランク回転数	✓	✓	✓	X	3
走行速度	✓	✓	✓	○	3
モーター回転速度		✓		X	3
走行モード			✓	○	2
変速位置			✓	○	3
道路状況				○	3

「ペダルを踏む」に関しては：

- トルクとクランク回転数はモーター回転速度を変化させるので、モーター回転速度で代用できる。
- 走行モード、変速位置、道路状況は、ペダルの踏み方に影響されない。

状況数は1458とおり

UCAを識別する：最大アシスト基準の場合

変速位置:3速、走行モード:強モード、道路：平坦な道

与えられないとハザードは安全側

状況		運転者：ペダルを踏む
走行速度	モーター速度	与えられるとハザード(P)
0km/h	無回転	乗り出し時にペダルを強く踏むと、急加速が行われてハザードになる(UCA1)
10km/h未満	強く回転	強く踏んでも、加速されない
	弱く回転	ペダルを回しながら急に強く踏むと、加速されるが、急加速にはならない
	無回転	ペダルを回していても、いなくても、急に強く踏むと、急加速が行われてハザードになる(UCA2)
10km～24km/h	強く回転	N/A(強く回転することはない)
	弱く回転	急加速にはならない
	無回転	急加速にはならない

ペダルが回っていても、モーターが回っていないときもあると仮定

UCAを識別する：上り坂の場合

変速位置:1速、走行モード:強モード、道路：上り坂

与えられないとハザードは安全側

状況		運転者：ペダルを踏む
走行速度	モーター速度	与えられるとハザード(P)
0km/h	無回転	乗り出し時にペダルを強く踏むと、急加速が行われてハザードになる(UCA1)
(10-α)km/h未満	強く回転	強く踏んでも、加速されない
	弱く回転	ペダルを回しながら急に強く踏むと、加速されるが、急加速にはならない
	無回転	N/A(常にペダルを踏んでいるから、モーターは回転している)
(10-α)km～(24-β)km/h	強く回転	N/A(強く回転することはない)
	弱く回転	急加速にはならない
	無回転	N/A(常にペダルを踏んでいるから、モーターは回転している)

UCAを識別する：下り坂の場合

変速位置:2速、走行モード:標準モード、道路：下り坂

与えられないとハザードは安全側

状況		運転者：ペダルを踏む
走行速度	モーター速度	与えられるとハザード(P)
0km/h	無回転	乗り出し時にペダルを強く踏むと、急加速が行われてハザードになる(UCA1)
10km/h未満	強く回転	強く踏んでも、加速されない
	弱く回転	ペダルを回しながら急に強く踏むと、加速されるが、急加速にはならない
	無回転	ペダルを回していても、いなくても、急に強く踏むと、急加速が行われてハザードになる(UCA2)
10km～(24-β)km/h	強く回転	N/A(強く回転することはない)
	弱く回転	急加速にはならない
	無回転	急加速にはならない

最大アシスト基準の場合に同じ

ハザードシナリオを識別し、対策を考える

UCA	ハザードシナリオ	対策
UCA1: 走行速度0km/h モーター無回転 ペダルを強く踏む	1. 乗り出しのときに、運転者が慌ててペダルを強く踏んでしまう。(スリップ) 2. トルクが急に大きくなる。 3. それを検知して、アシスト装置がモーターを急に強く回す。 4. 自転車が急に加速され、ハザードを引き起こす。	モーターが無回転のときには、トルクが急に大きくなっても、モーターを強く回さない。
UCA2: 走行速度10km/h未満 モーター無回転 ペダルを強く踏む		

人に関する制御行動

1. オミッションエラー：適切な指令を行わない
2. ミステイク：適切でない指令を行う
3. スリップ：指令は適切だが、間違えて実施する

ヒューマンエラーの分類に基づくガイドワード

ハザードシナリオの識別と対策

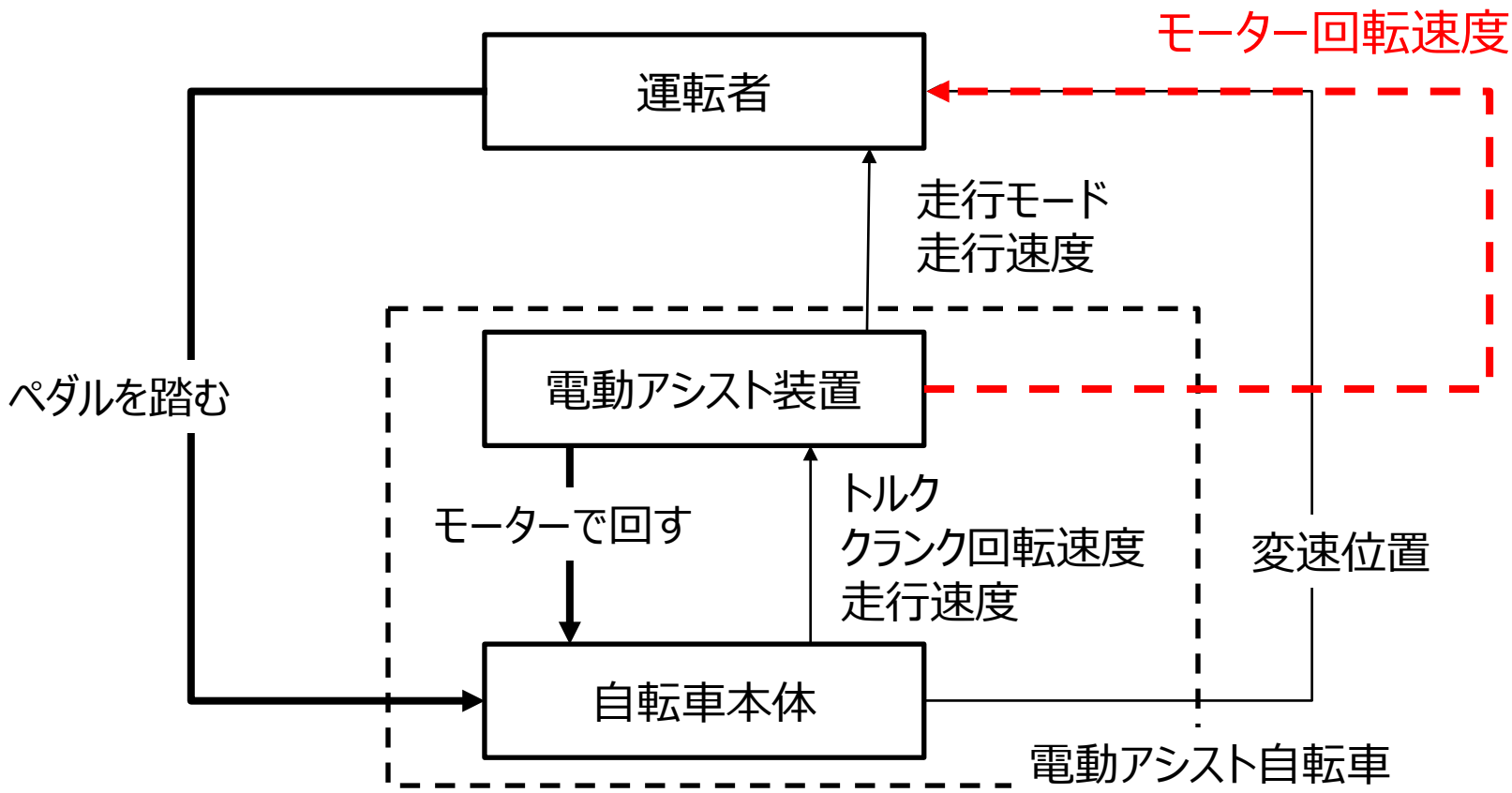
UCA	ハザードシナリオ	対策
UCA1: 走行速度0km/h モーター無回転 ペダルを強く踏む	1. 乗り出しのときに、運転者が慌ててペダルを強く踏んでしまう。(スリップ) 2. これ以降はUCA2に同じ。	対策1に同じ
UCA2: 走行速度10km/h未満 モーター無回転 ペダルを強く踏む	1. ゆっくりと走っているときに、加速しようとして、運転者がペダルを強く踏んでしまう。(ミステイク) 2. トルクが急に大きくなる。 3. それを検知して、アシスト装置がモーターを急に強く回す。 4. 自転車が急に加速され、ハザードを引き起こす。	対策1： モーターが無回転のときには、トルクが急に大きくなっても、モーターを強く回さない。 対策2： 運転者がモーター回転速度を認識できるようにし、無回転時には強くペダルを踏まないように注意喚起する。

両ケースとも、
モーターが回転せず、
アシストが働いていない

「乗り心地を自然で滑らかにする」という意図の実現には、対策2が推奨策。

対策2：フィードバックの追加

電動アシスト装置の動作状態を反映するフィードバックがなかった



まとめ

- JASA　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。
- 安全誘導型設計は、開発意図とシステム仕様をもとにハザード分析を行い、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。
- ハザード分析に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、意図記述とそれを反映する要求記述をもとにして、次のように制御構造を識別した：
  - システムコンテキスト図からコンポーネントを抽出
  - ユースケース図から人と機械の相互関係を識別
  - 意図・要求記述から機械内部の相互関係を識別
- 制御行動の非安全さは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を識別した:
  - フィードバックデータ、制御行動の結果
- ヒューマンエラー分類をガイドワードとしてハザードシナリオを識別し、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できた。
- 安全誘導型設計にSTPA手法は適すると考え、開発意図をSTPAで分析し、製品の安全性や健全性を高めるために活用してゆきたい。

参考資料

1. 平成26年度成果報告書「要求の仕様化に関する課題、プロセス及び手法」、JASAホームページ
2. 「意図を記述すれば、安全性が高まる」、日経テクノロジーオンライン
3. 「安全誘導型設計の特徴と試行」、ET2016　JASA技術本部セミナー
4. 「意図記述言語SSQLの狙いと特徴」、ET-WEST2017　JASA技術本部セミナー
5. 「STAMP支援シミュレーター開発」、ET2017　JASA技術本部セミナー
6. SLPについて、https://www.jfp.co.jp/slp/index.html

ご清聴ありがとうございました

問合せ先：
中村　洋
hiroshi19.nakamura@nifty.com