Title	インホイールモータ搭載超小型電気自動車の操縦安定化制御システムに対する安全解析
Sub Title	Safety Analysis for Vehicle Stability Control System in a Micro Electric Vehicle with In-wheel Motors
Author	Drifidianto, Ilham(Nishimura, Hidekazu) 西村, 秀和
Publisher	慶應義塾大学大学院システムデザイン・マネジメント研究科
Publication year	2014
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2014年度システムエンジニアリング学 第155号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40002001-00002014-0011

修士論文　　2014 年度

インホイールモータ搭載超小型電気自動車の操縦安定化制御システムに対する安全解析

ドリフィディアント イルハム
（学籍番号：81234578）

指導教員　教授　西村 秀和

2014 年 9 月

慶應義塾大学大学院システムデザイン・マネジメント研究科
システムデザイン・マネジメント専攻

論　　文　　要　　旨

学籍番号	8124578	氏　名	ドリフィディアント　イルハム

論　文　題　目：

インホイールモータ搭載超小型電気自動車の操縦安定化制御システムに対する安全解析

（内容の要旨）

本研究はインホイールモータを搭載する超小型電気自動車（MEV）の操縦安定化制御システム（Vehicle Stability Control System，以下，VSCS）に対する安全解析を実施することを目的としている．MEV をはじめ電気自動車などの安全性に関する研究では，モータなどのコンポーネントの故障にのみ着目することが多い．これに対して本研究では，駆動・制動トルク制御と前輪舵角制御により構成される VSCS により制御された MEV 全体をシステム対象として安全性を解析する．

システムレベルで行う安全解析の方法として，システム理論に基づくハザード分析手法（STPA）があるが，本研究では，STPA で不安全な制御アクションを特定する際に，システムの構成要素間の相互作用を明確するためにシーケンス図を用いる．SysML (Systems Modeling Language) の図であるシーケンス図を用いることで，コンポーネント，または，パート間のメッセージのやりとりのタイミングと順序を明確に表すことができる．このシーケンス図の中で検討した相互作用に STPA のガイドワードを適用し，不安全な制御アクションの特定を行う．その結果，STPA の制御構造図で特定できない順序に関する不安全な制御アクションをシーケンス図による特定ができる．また，着目する制御アクションごとのコントロールループ上のガイドワードを適用し，不安全な制御アクションに繋がる潜在的原因の特定を行う．さらに，シミュレーションを用いて，特定した不安全な制御アクションを除去・抑制するために，システムとしての事故に至らないように安全を確保するために満たすべき条件である安全制約，および，被害の大きさのレベルの特定を行う．被害の大きさのレベルは軽度，および，重度に分けられる．軽度の不安全な制御アクションがある場合には VSCS を用いて対応し，一方，重度の不安全な制御アクションがある場合に安全に MEV を停止するという機能を検討する．

以上より特定した安全制約，および，被害の大きさのレベルに基づいて，MEV の操縦安定性に対する耐故障制御システム（Fault-tolerant Control System，以下，FTCS）の検討を行う．SysML を用い，FTCS の機能要求，および，インタフェースを明確にし，FTCS のアーキテクチャを構築する．また，VSCS と FTCS との関係を明確にする．その上で，FTCS が不安全な制御アクションの被害の大きさを判断し，対応するコントローラを選択するアーキテクチャを提案する．

キーワード（5 語）

操縦安定化制御システム，超小型電気自動車，モデルベースシステムズエンジニアリング，システム理論に基づくハザード分析手法，耐故障制御

SUMMARY OF MASTER'S DISSERTATION

Student Identification Number	81234578	Name	Drifidianto Ilham

Title

Safety Analysis for Vehicle Stability Control System in a Micro Electric Vehicle with In-wheel Motors

Abstract

This paper presents safety analysis for vehicle stability control system (VSCS) in a micro electric vehicle with in-wheel motors (MEV). Although there have been many researches on safety of electric vehicles in terms of the vehicle component's fault, the system safety or the functional safety must be very important for vehicles. This paper discusses the system safety analysis of a micro electric vehicle with in-wheel motors (MEV), equipped with a vehicle stability control system (VSCS). VSCS consists of the front steering angle control and the drive/braking torque control.

System-Theoretic Process Analysis (STPA) is a safety analysis method which is conducted in system level. In this thesis By combining sequence diagram and STPA, the unsafe control actions are identified. By using sequence diagram of SysML (System Modeling Language), the sequence and timing of the exchanged messages, between components or parts, can be described clearly. To identify the unsafe control action, STPA guide words are applied to the sequence diagram examined and obtained. Thus, unsafe control action which cannot be identified by the control structure diagram of STPA, now can be identified by the sequence diagram. After that, the causal factors of unsafe control action are identified by applying the guide word in the control loop. Furthermore, simulations are conducted to obtain the safety constraint and the severity level of each unsafe control action. Safety constraint is the condition that has to be satisfied in order to ensure the system's safety and avoid any accident in the system. Severity level is divided into a mild level and a severe level.

Based on the safety analysis, fault-tolerant control system (FTCS) for MEV with VSCS is introduced. The FTC's functional requirements are clarified and the derived functions are allocated to the components of FTCS. From the simulation results, it is verified that VSCS are effective enough to maintain vehicle safety in the mild-fault condition. Also in the severe-fault condition, the safety stop function is considered.

Key Word(5 words)

Vehicle Stability Control System, Micro Electric Vehicle , Model-Based Systems Engineering, System-Theoretic Process Analysis, Fault-tolerant Control

目次

図目次

表目次

第 1 章　序論

1.1 背景

現在，環境問題や省エネルギーの観点から，電気自動車の普及が期待されており，また，近年では，普通サイズの電気自動車だけでなく，超小型電気自動車が注目を浴びている．超小型電気自動車とは自動車よりコンパクトで，地域の手軽な移動の足となる 1 人から 2 人乗り程度の車両（エネルギー消費量は，通常の自動車に比べて 1/6，電気自動車の 1/2 程度である）のことを指す[1]．超小型電気自動車は，省エネルギー・低炭素化社会の実現に寄与する．また，狭い場所でも気軽に利用できるため，高齢者等の移動支援や子育て支援に役立つ．現状では，一般に使われている自動車は最少 4 人乗りであるが，実際には 1 人から 2 人しか乗っていないケースが多い．そのため，エネルギーやスペース等が無駄になっている．さらに，約 6 割の自動車が短距離移動で 10 km 以内で利用されている[1]．この実態と航続距離が短いという電気自動車の弱点を考慮し，「超小型電気自動車」の導入が始まった. 国土交通省は超小型電気自動車の普及のために, さまざまな取組みを始めている．

一方，タイヤのホイール内にモータを配置するインホイールモータ[2]を用いることにより，モータを車体内に配置しドライブシャフトでタイヤへ駆動力を配分する従来の電気自動車に比べて，設計の自由度を高めることができる．このため，超小型電気自動車に対しては，省スペースの観点から，インホイールモータの導入が盛んである．著者らは，これまで MBSE（Model Based Systems Engineering）に基づき，インホイールモータを搭載する超小型電気自動車の操縦安定化制御システム設計に関する研究を行ってきた[3][4].

さらに電気自動車を社会に普及させるためには，電気自動車の安全性を確保することが重要である．そのためには，安全解析，および，ハザードへの対策が必要である．電気自動車の安全性に関する研究では，モータをはじめとするコンポーネントの故障に着目している場合が多い[5][6]．しかし，電気自動車は複雑なシステムであるため，コンポーネント毎に安全性を検討するだけでは不十分であり，システムレベルで安全性を検討する必要がある．特に，インホイールモータを搭載する超小型電気自動車に対しては，システムレベルでの安全性に関する検討はまだ実施されていない.

ここで，表 1.1 に，主な安全解析手法の一覧を示す．これらの安全解析手法の中で，FTA(Fault Tree Analysis)と FMEA(Fault Mode and Effect Analysis)が最も多く利用されている．しかし，FTA/FMEA を用いたのでは，コンポーネント故障に関連しないハザード原因を特定することは難しい．HAZOP (Hazard and　Operability Study）は化学プラントなどで広く

Table 1.1 The differences between safety analysis method

FTA (Fault Tree Analysis)	・木構造を用いて，ハザードの発生経路，原因および確率を解析する. ・コンポーネント故障の原因を特定する.
FMEA (Fault Mode and Effect Analysis)	・システムを構成する全てのコンポーネントに対して故障モードを調べ，故障モードが及ぼす影響を解析する手法.
HAZOP (HAZard and OPerability studies)	・化学プラントが起こす事故の可能性を網羅するために，ガイドワードを用いてシステムの異常を調査する. ・異常の起こる部分およびその原因を明確にするために，各部のプロセスを調査する. 事故はパラメータの逸脱から考える. ・物理コンポーネント図を用いる. ・他の安全解析手法と組み合わせて使用する場合がある.
SHARD (Software Hazard Analysis and Resolution in Design)	・HAZOP をもとにしてガイドワードをソフトウェア向けに整理した手法.
STAMP (Systems-Theoretic Accident Model and Processes) STPA (STAMP - Based Process Analysis, Systems Theoretic Process Analysis)	・STAMPとはシステム理論に基づくシステムとしての事故モデルである．システムとしての事故は不安全・不十分な制御から発生する. ・因果関係モデルをもとに潜在的原因を特定する．これらは設計のエラー，ソフトウェアの失陥，コンポーネント相互作用によるシステムとしての事故，操作する人間が起こすエラー，およびシステムとしての事故に影響するマネジメント，組織，社会という原因である. ・STPAには制御構造図にガイドワードを適用する. ・コントロールループ（因果関係モデル）をもとに潜在的原因を特定する．潜在的原

	因にはコンポーネント相互作用に関するハザードが含まれる. ・安全ガイドの設計に使用することができるように，事前に定義されている. ・故障よりも，コンポーネント同士の相互作用によるハザードに重点を置いている

使用されている安全解析手法[7]であり，安全関連の質問，一連のガイドワードを適用し，システムについての仮説を構築する．HAZOP は，他の安全解析手法と組み合わせて使用する場合があるが，多くの専門知識が必要である．

マサチューセッツ工科大学（MIT）の Nancy Leveson は STAMP/STPA の安全解析手法を提案し，近年，注目されている．STAMP（Systems-Theoretic Accident Model and Processes）とは，システム理論に基づく事故モデルである．STPA（STAMP-Based Process Analysis, Systems Theoretic Process Analysis）とは, システム理論に基づくハザード分析の手法である．STPA は, HAZOP のようにガイドワードを適用し, システムのモデルを解析する．しかし，STPA は STAMP の因果関係モデル「causality model」をもとに解析し，新しい潜在的原因を特定する．これらの原因としては，設計のエラー，ソフトウェアの失陥，コンポーネント相互作用によるシステムとしての事故，操作する人間が起こすエラー，および事故に影響するマネジメント，組織，社会の原因などが挙げられる[8]．この手法はコンポーネント単一の故障よりも，コンポーネント同士の相互作用によるハザードを分析することに重点を置いている．

ハザードの分析は，定性分析および定量分析に大別される．前者はハザードにより引き起こされる時間やコスト等を考慮する場合に適している[9]．後者は高精度な分析や複雑な分析を行う際に適している．STAMP/STPA は定性分析に含まれる．

一方，安全解析手法を用いるのみならず，MBSE によるアプローチも安全解析には有効である．たとえば， SysML (System Modeling Language) を用いて安全解析を行う方法が提案されている[10]．また，状態遷移図に着目して安全解析をする研究が行われている[11][12]．しかしながら，SysML にはシステムの振る舞いの記述方法として，システムの要素間の相互作用に着目するシーケンス図があるものの，コンポーネント間の相互作用に着目した安全解析は実施されていない．

1.2 目的

本研究では，4 輪インホイールモータ搭載超小型電気自動車（以下，MEV）の交通環境における安全性の確保を目指し，操縦安定化制御システム（Vehicle Stability Control System，以下，VSCS）に関する安全解析を行い，その対策を検討する．安全解析を行う際には，コンポーネントのみに着目するのみでは不十分であり，システム構成要素間の相互作用を検討する必要があると考えられる．そこで，本研究では，システムモデリング言語である SysML のシーケンス図を用いてシステム構成要素間の相互作用を記述し，その上で STAMP/STPA で提案されているガイドワードを用いて安全解析を実施する．さらに，不安全な制御アクションへの対策として， VSCS に対する耐故障制御システムの検討を行う．

以下に具体的な研究内容を述べる．

1. 不安全な制御アクションを抑制・除去するための安全制約を特定する．
    - システムの相互作用に基づいた不安全な制御アクションの特定
      制御構造図だけでなく，アクションの順序およびタイミングを表すシーケンス図で相互作用を検討する．検討した相互作用にガイドワードを適用し，不安全な制御アクションを特定する．
    - 不安全な制御アクションの潜在的原因の特定
      着目する制御アクションごとにコントロールループ上のガイドワードを適用し，不安全な制御アクションに繋がる潜在的原因を特定する．
    - シミュレーションによる安全制約の特定と被害の大きさの特定
      不安全な制御アクションを抑制・除去するための安全制約をシミュレーションにより特定する．導出した安全制約に対する対策を調査するために，各不安全な制御アクションの被害の大きさのレベルを特定する．

2. 特定した安全制約，および，被害の大きさのレベルに基づいて，MEV の操縦安定性に対する耐故障制御システム（Fault-tolerant Control System）の検討を行う．MBSE に基づき，耐故障制御システムの機能要求，および，インタフェースを明確にし，アーキテクチャを構築する．また，VSCS と耐故障制御システムとの関係を明確にする．

1.3 論文の構成

本論文は 5 章と付録で構成される．各章と付録の概要は以下の通りである．

第 1 章では，研究の背景と研究目的，および，本論文の構成について述べている．

第 2 章では，システムの要素の相互作用に着目した MEV の VSCS のハザード解析について述べている．要求分析に関して記述したのち，MBSE を適用し，システム構成要素の相互作用を検討する．これらの結果を用いて，ハザードと不安全な制御アクションを特定する．さらに，不安全な制御アクションの潜在的原因を特定する．

第 3 章では，MEV の VSCS に対する安全制約の検討について述べている．シミュレーションを実施し，不安全な制御アクションを抑制・除去するためのパラメータ制約を決定する．

第 4 章では, MEV の VSCS に対する耐故障制御システムアーキテクチャの構築を検討する．アーキテクチャ構築を検討するため，機能要求やインタフェースを明確にする．

第 5 章では，研究で得られた成果をまとめ，考察を実施している．

第 2 章

システム相互作用に基づくハザード解析

2.1　ハザード解析の対象

本研究では，4 輪インホイールモータ搭載超小型電気自動車（以下，MEV）の交通環境における安全性の確保を目指し，操縦安定化制御システム（Vehicle Stability Control System, 以下，VSCS）に関する安全解析を行い，その対策を検討する．これまでドライバ，道路，環境などのシステム内での環境性能の確保と，同時にエネルギー消費の最小化，操縦安定性といった要求を満たすため，MBSE（Model Based Systems Engineering）に基づきシステムレベルで操縦安定化制御システムの設計に関する研究を行ってきた[3][4].

VSCS の振る舞いを表現したアクティビティ図を図 2.1 に示す．アクティビティ図は，入力，出力，および，制御の使用可能性に基づくアクションの順序付けと，データの流れを表すことに適した図である. アクティビティ図では, 角の丸い四角を用いてアクション, 実線の矢印出を用いてオブジェクトフロー, 破線の矢印を用いて制御フローを表す. また, 各アクションを縦の実践で区切ることにより，システムのサブシステムやコンポーネントのアクションの範囲を示すことができる.

ここでは，アクティビティ図を用いて，操縦安定化制御システムの機能アーキテクチャを導く． VSCS は車両の状態，および，ドライバの入力に関する情報を用い，「車両の状態を計測する」,「ドライバの入力を計測する」というアクションを行う.「ドライバの意図を推定する」,「車両の状態を計測する」というアクションの結果より得られる情報を用いて,「前輪操舵角制御入力と独立駆動・制動モータトルク制御入力を統合した制御」アクションを行う．生成した制御入力に関して，配分，制限のアクションを行った後，制動を動作させるアクションを行う[16]．この結果に基づき，ステアリング，および，モータを作動させる．各アクションに割り当てる物理要素は「アクチュエータサブシステム」,「制御サブシステム」および「計測サブシステム」である.

$$\gamma_{ref} = \frac{K}{1+\tau s}\delta \tag{2.1}$$

図 2.2 は MEV の制御構造図を示す．これをもとにH_∞制御システムの設計が行われた．横滑り角β，ヨーレートγ，とその目標値γ_{ref}との誤差信号γ_eをフィードバック信号とし，前輪操舵角δ_f，4 輪独立駆動トルク τ_{ij}を統合して制御入力として用いる.

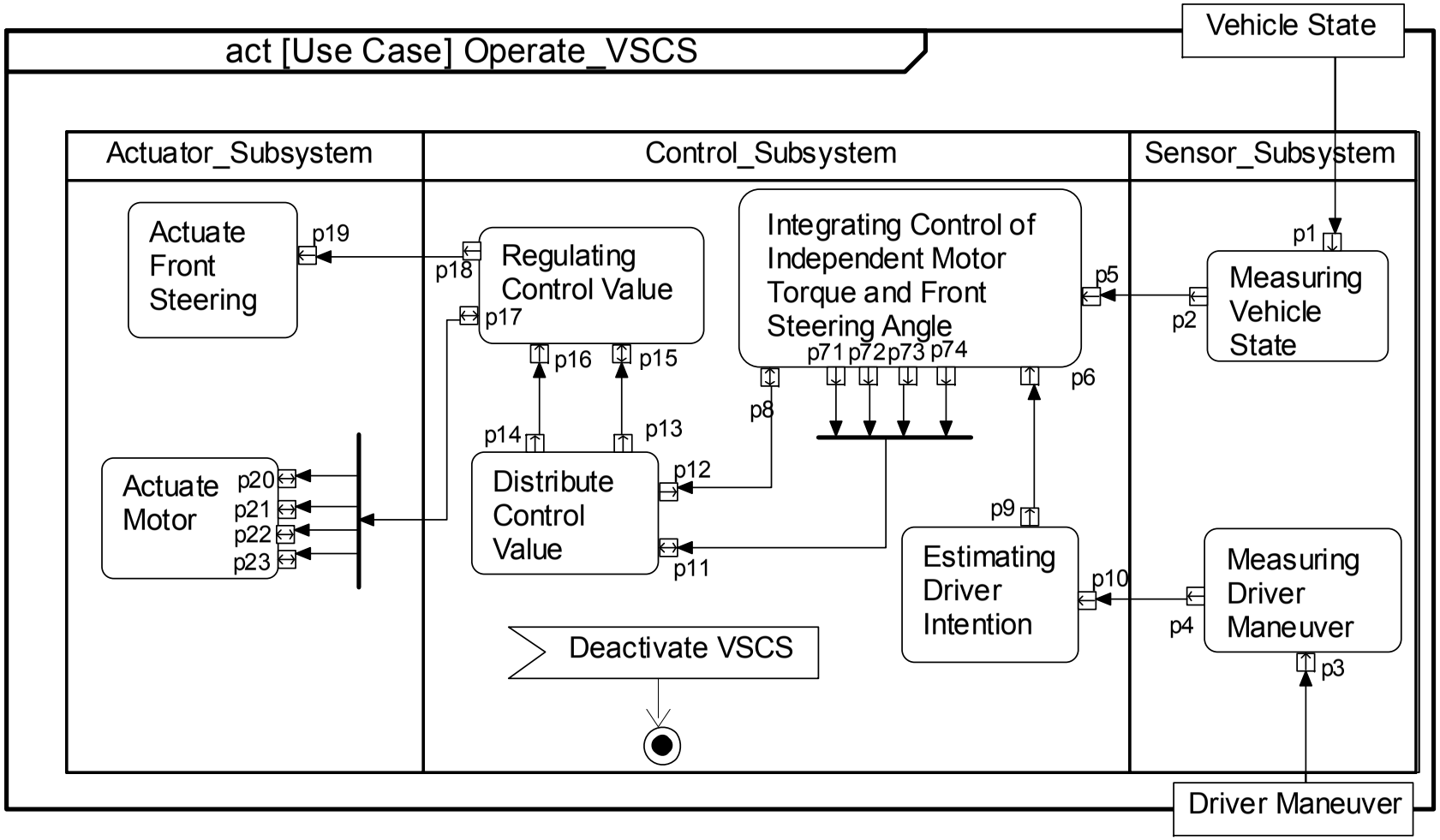


Fig. 2.1 Activity diagram of VSCS with actions allocated [16]

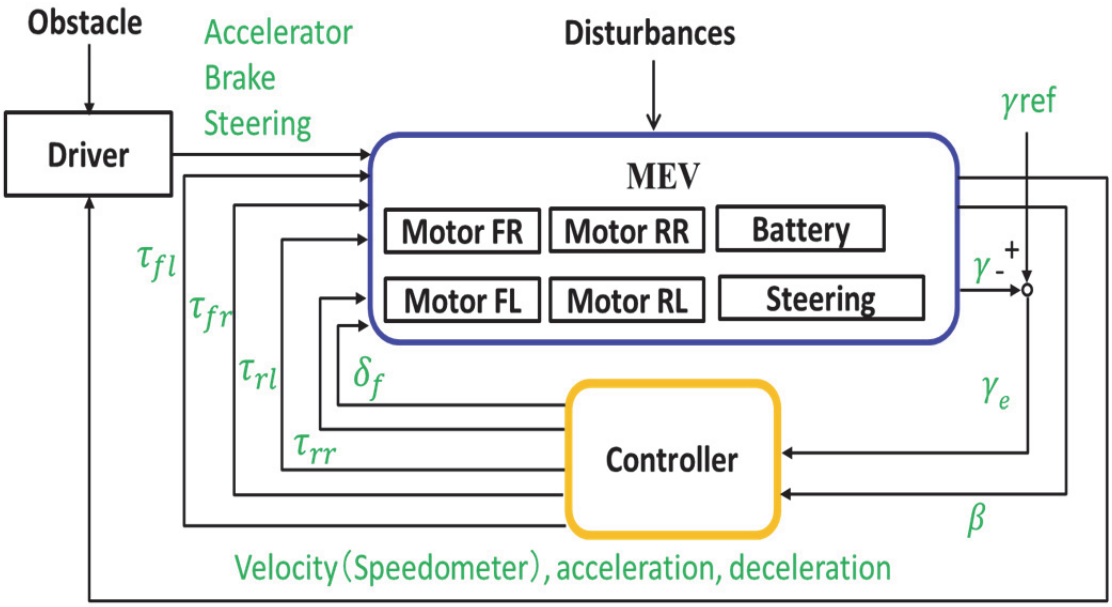


Fig. 2.2 Control Structure of MEV

MEV のヨーレート応答γの目標値γ_{ref}には，ドライバが与える操舵角δに対して従来車両が発生するヨーレートを与える．目標ヨーレートγ_{ref}はドライバの操舵角δと一次遅れ系の関係を有し，式(2.1)で表すことができる．ここで，K＝0.2377, τ ＝0.0903 とし，目標値 ref γ_{ref}に対して，ヨーレートγが定常偏差なく追従するようサーボ系を構成する[16].

2.2 安全解析手法

近年, システムの安全解析を行うために, STAMP/STPA が注目されている. 図 2.3 は STPA の概略図を示す. 安全解析を行う際には, 安全性をコンポーネント故障の問題のみならず, ダイナミックな制御問題として捉える必要がある．なぜなら，システムとしての事故はコ

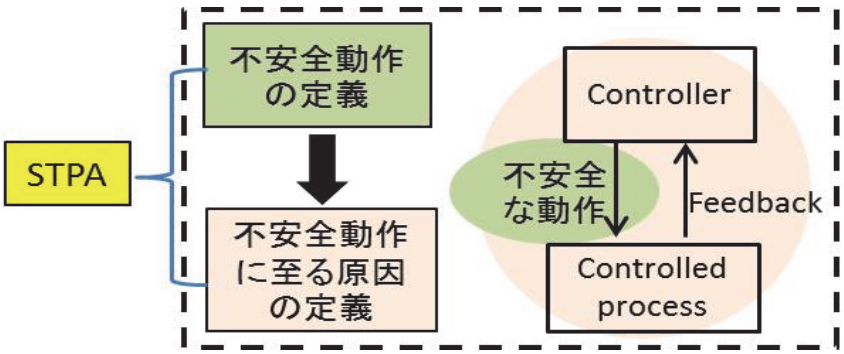


Fig. 2.3 STPA Analysis

ントロールが不十分である結果として起こるからである．例えば，コントローラの操作，あるいは，コントローラと制御対象の相互作用の不備が原因となる．このようなシステムとしての事故は適切な安全制約を課していなかったために起こると考えられる．これらのシステムとしての事故も故障イベントの順序だけでなく，複雑なダイナミックなプロセスの結果である．

STAMP は 3 つの基本コンセプトから構成される．

1. Safety Constraints（安全制約）：システムとしての事故に至らないように安全を確保するために満たすべき条件である．例えば，信号送信の遅れという不安全な制御アクションにおける安全制約は・・ms 以上遅れてはならないということである．
2. Hierarchical safety control structure：システム開発と運用フェーズそれぞれの利害関係者においてとるべき安全行動と実際の行動結果を表現する構成図である．
3. Process models：コントローラと制御対処(=プロセス)，ドライバを単純な制御ブロック図のように記述し，それぞれで想定と実現のずれやフィードバック遅れなどで発生する事故を表現する．

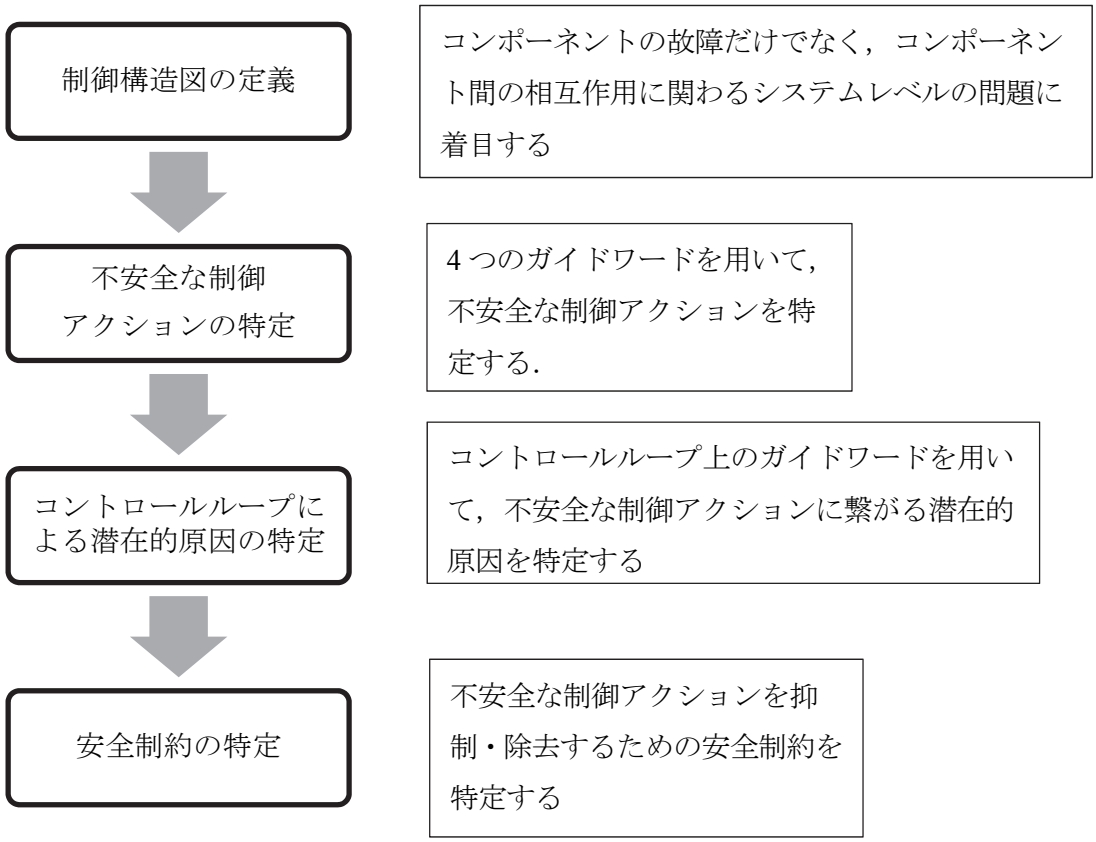


Fig. 2.4 STAMP/STPA process

図 2.4 は STAMP/STPA の手順を示す．STPA を用いたハザード解析手順では，まず要求分析を実施し，コンポーネントとその連携内容（アクション）を書き出す．つぎに，各アクションにガイドワードを適用し，不安全動作とハザード，ハザードシナリオ，安全制約を抽出する．また，不安全なアクション毎にコントロールループを作成する．これらの結果を用いて，抽出された安全制約，および，不安全な制御アクションに至る原因に対し安全設計を行う．

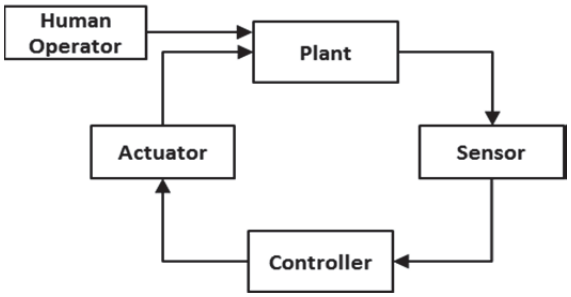


Fig. 2.5 The control structure

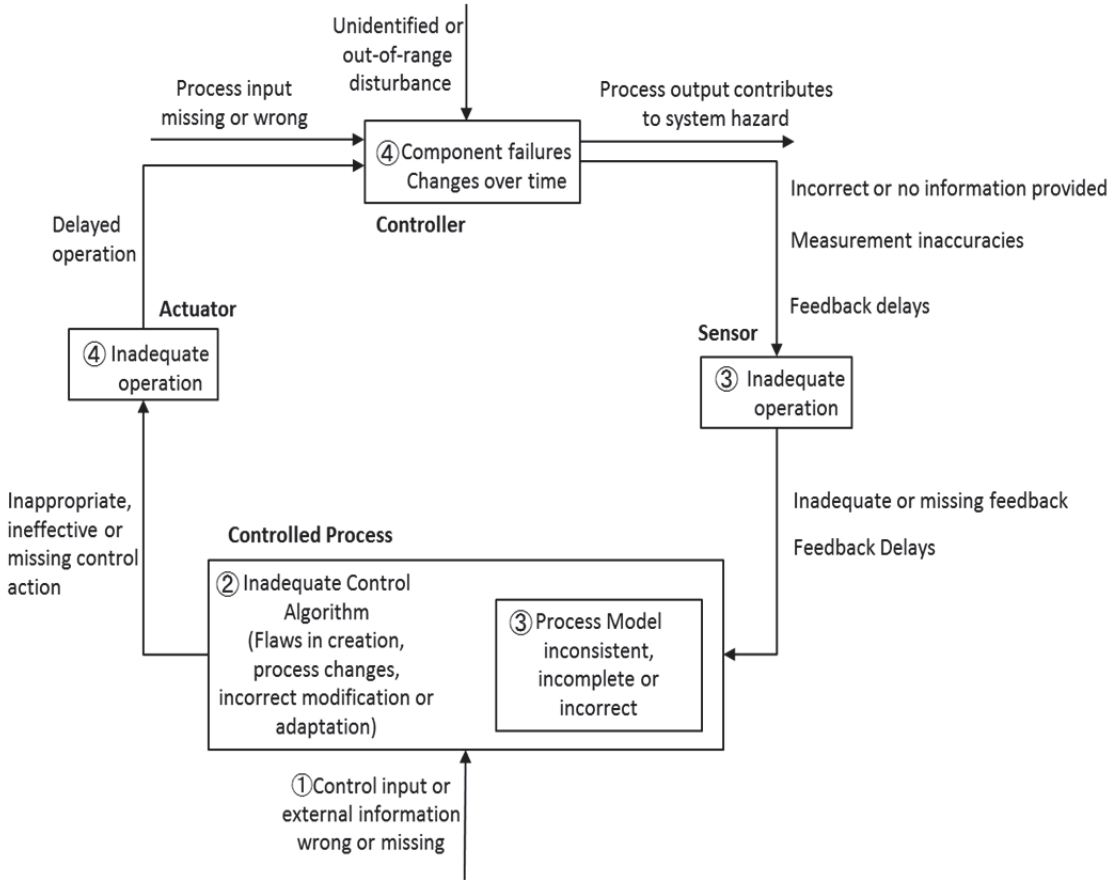


Fig. 2.6 Causal factor [8]

図 2.4 に示した STAMP/STPA のプロセスを以下に記す.

① 基本の制御構造を定義し「制御構造図」を作成する．図 2.5 は制御構造図の一つの例である.

② 不十分な制御アクション(Inadequate Control Action)によるハザードシナリオを特定する.

不十分な制御アクションは以下の４つのガイドワードに落とし込まれる.

(1) “Not Provided”,

安全性を確保するために要求される制御アクションが提供されない.

(2) “Incorrectly Provided”,

損失を発生させる不十分，あるいは，不安全な制御アクションが提供される.

(3) “Provided Too Early, Too Late, or Out of Sequence”,

十分な制御アクションの提供が早すぎる(too early)，遅すぎる(too late)，あるいは，順序から外れている.

(4) “Stopped Too Soon”,

適切な制御アクションの停止が早すぎる.

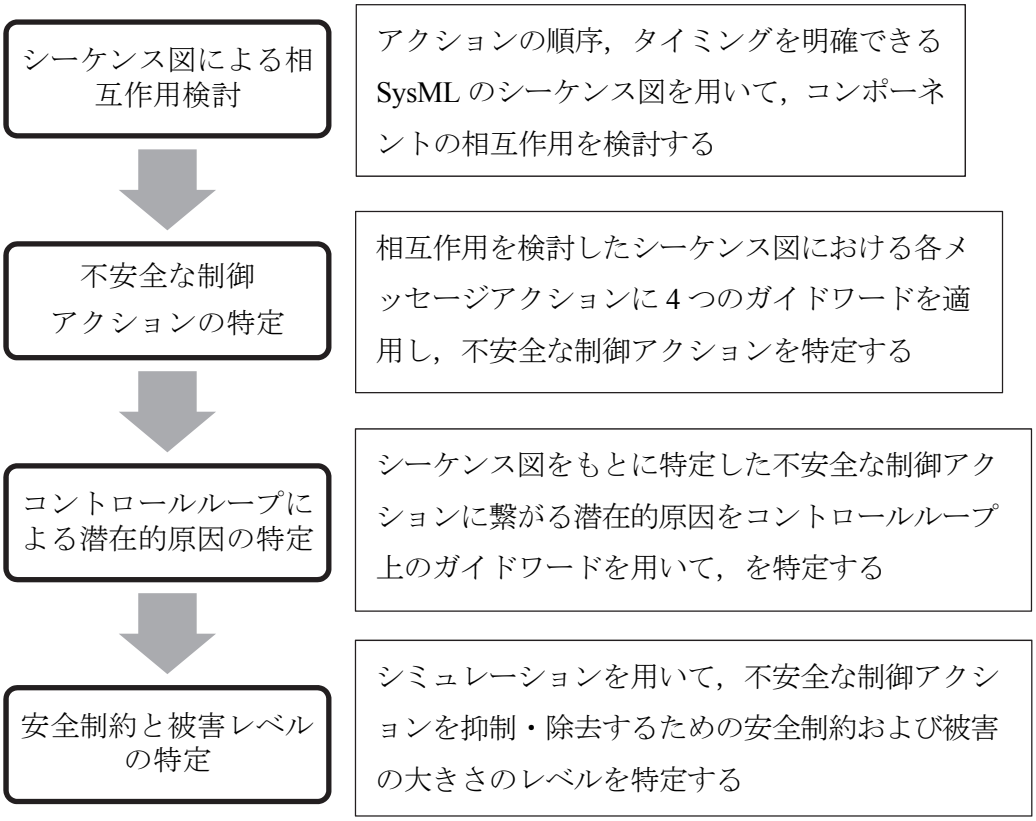


Fig. 2.7 Proposed approach

③ ハザードシナリオにつながる潜在的原因(Causal Factor)を特定する．図 2.6 は潜在的原因を特定するためのコントロールループを示す．STAMP/STPA のコントロールループは時計と反対周りの方向であるため，コントローラと制御対象の位置，およびループの方向を逆方向に変更した．検討しやすくために，制御工学に用いる制御構造図と合わせる必要がある．

④ 各不安全な制御アクションの安全制約を特定する．

本研究は従来の STAMP/STPA のプロセスに基づき，独自のアプローチを加えている．図 2.7 は本研究の内容を示す．STAMP/STPA は最初に制御構造図を用いて制御構造を解析する．しかし，本研究では制御構造図だけでなく，SysML のダイアグラムであるシーケンス図をあわせて用いることにより，不安全な制御アクションを特定する．シーケンス図を用いることで，制御アクションの順序，および，タイミングをさらに明確にできる．および，不安全な制御アクションを抑制・除去するために安全制約のみでなく，被害の大きさのレベルも特定する．

2.3 安全性に関する要求分析

MEV に対する安全解析を行う前に，要求分析を行う必要がある．図 2.8 は MEV に対する要求を SysML の要求図で示す．「〇」の中に「+」が書いてある記号の先に細分化された要求が示されている．また，「<<derive>>」は，矢印の元の要求が矢印の先の要求から導出されることを示している．この図に示すように MEV に関する要求は多種多様であるが，本研究では安全「Safety」という要求に着目する．既に MEV の操縦安定性の要求に関する先行研究は実施されている[3][4]．図 2.8 より，MEV は従来車両より小型・軽量化されているにも関わらず，従来車両と同等の走行性能が要求されていることがわかる．さらに，車両の小型・軽量化「Small and Light Weight」と操縦安定性「Driving Stability」の要求から，低転がり摩擦下での操縦安定性「Driving Stability on Low Rolling Resistance」という要求が導出されている．

操縦安定性により，MEV の交通環境における安全性を確保する必要がある．MEV の安全を実現するためには，MEV に障害が発生した際に正常な動作の維持，および，事故を防ぐことができるかという観点が特に重要であると考え，故障許容 「Fault tolerance」の要求

を導出した．故障許容の要求を満たすために耐故障制御に関する調査が必要になり，詳細は 4 章に述べる．一方，VSCS は駆動トルク制御，前輪操舵角制御，および，これら両方の統合制御の仕組みを備えている．それぞれの制御に起こり得る不安全な制御アクションを特定する必要がある．

MEV の安全性を確保するために，まず不安全な制御アクションを調査する必要がある．特に VSCS は MEV を制御するため，本研究では VSCS に対する安全解析を行う．コンポーネントの信頼性のみならず，コンポーネント間の相互作用より引き起こされる不安全な制御アクションを特定することが重要である．次に，この原因，および，対策を検討する必要がある．これらを行うために，STAMP/STPA の安全解析手法を用いる．STAMP/STPA は，制御構造図を定義し，不安全な制御アクションを解析するために用いる．しかし，制御構造図は明確に制御のアクションのタイミング, および, 順序を定めることが出来ない．システムのモデリングに用いる SysML には, システムの構成要素間の相互作用に着目するシーケンス図やシステムの外部のアクターがどの様にシステムを用いるのかを表すユースケース図がある．本研究では，SysML を用いて，STAMP/STPA と組み合わせて不安全な制御アクションを検討する．

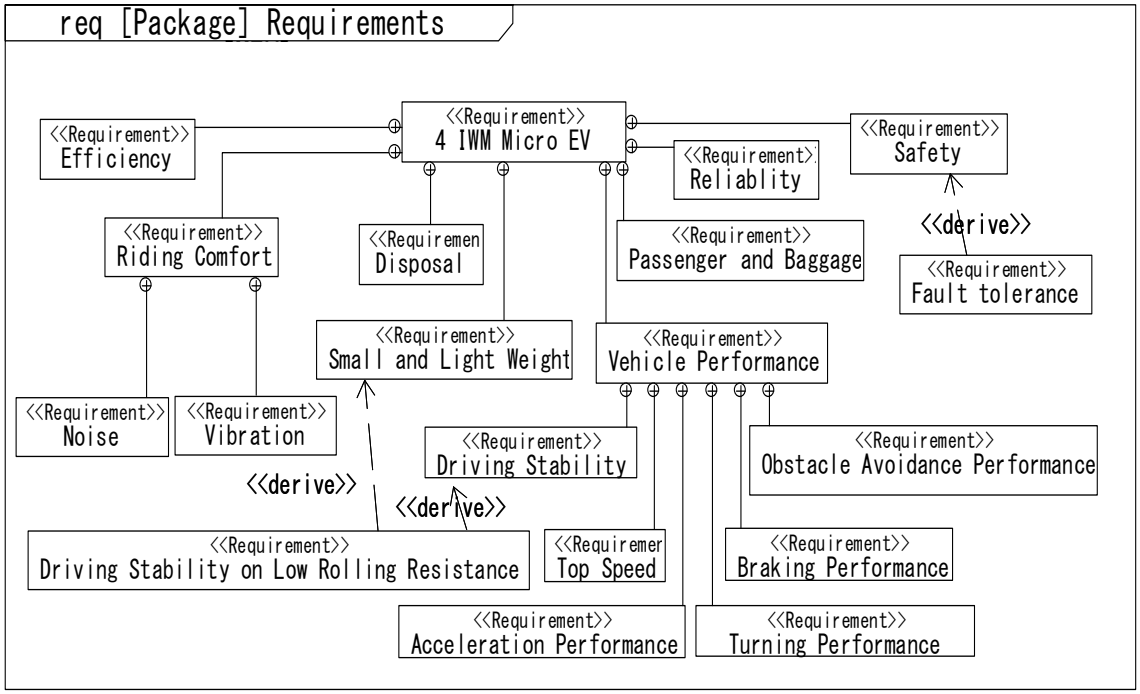


Fig. 2.8 Requirement diagram of MEV

2.4　相互作用の検討

ハザード分析を適切に実施するためには，ハザードシナリオが必要である．ハザードシナリオは，SysML のダイアグラムであるシーケンス図やユースケース図を分析することにより導く．図 2.9 は MEV の運用「Operate MEV」のユースケース図を示す．ユースケース図（Use case Diagram）はシステムとアクター間の相互作用に着目してシステムの機能を表現する図である．中央の四角く囲まれている部分は，分析対象のシステムである MEV の範囲を表すそのため，システムが外部システムに対してどのような機能を提供するかを明らかにすることができる. 図 2.9 に示す通り, 車両乗員「Vehicle occupant」, 乗客「Passenger」, とドライバ「Driver」はアクターである．このユースケースには乗車「Enter MEV」，　降車「Exit MEV」，　車両アクセサリーの制御「Control MEV Accessory」，　車両運転「Drive MEV」を含む．この 4 つのユースケースから，本研究は VSCS が MEV の運転の際に動作するため，MEV の運転「Drive MEV」というユースケースに着目する．

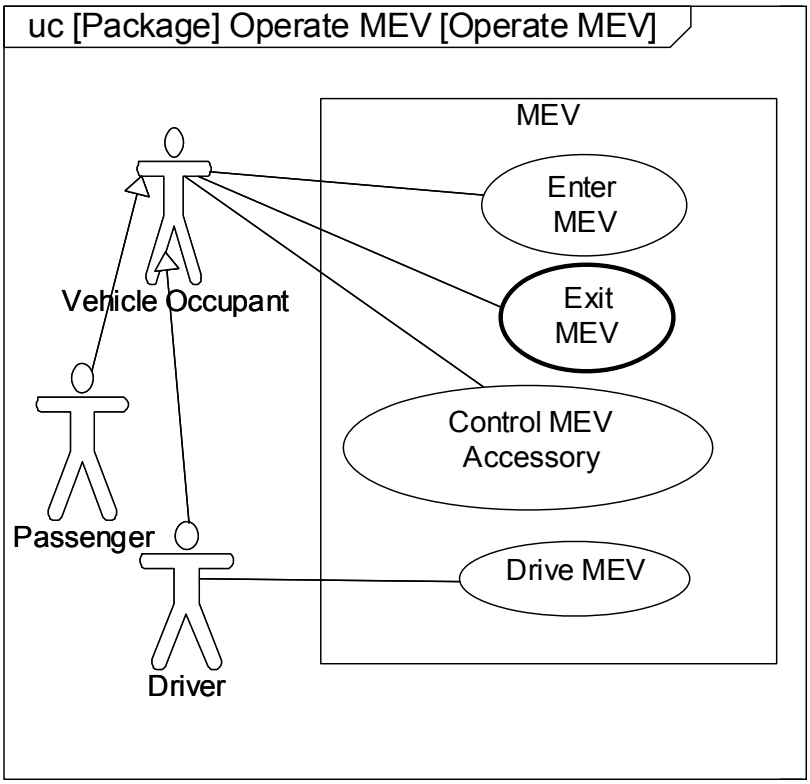


Fig. 2.9 Use case diagram for the operate MEV [19]

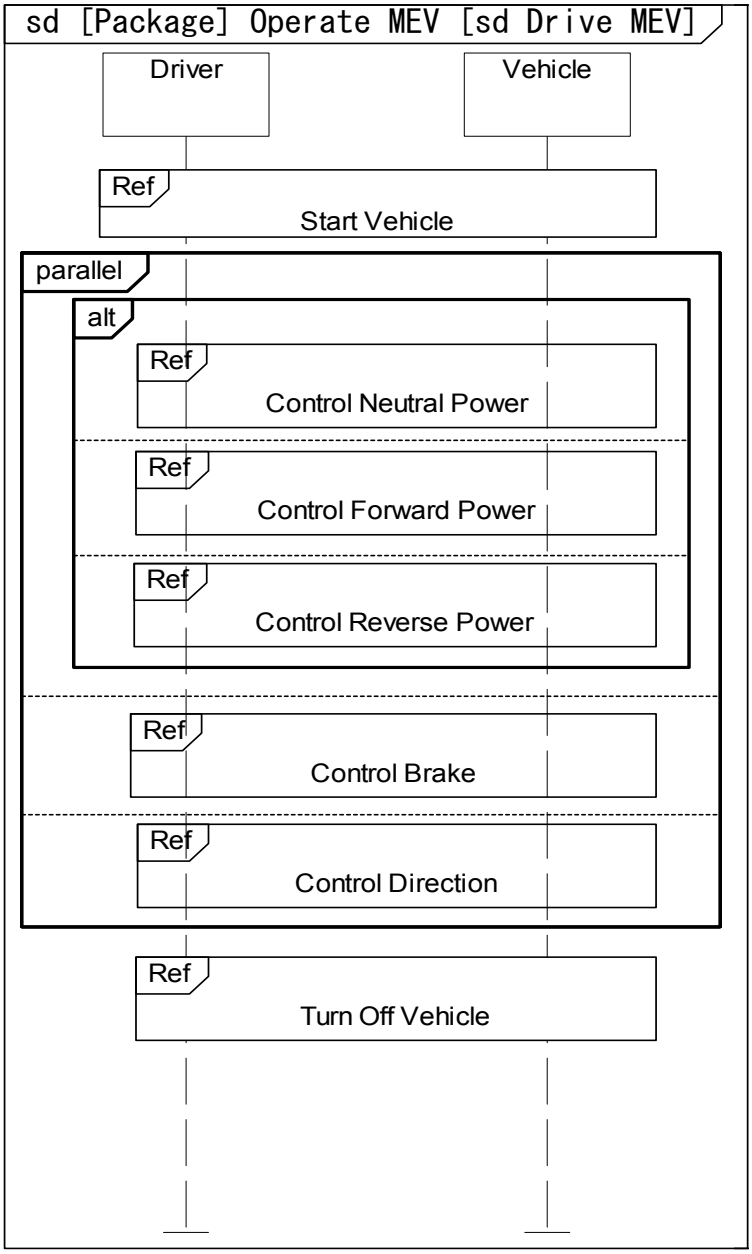


Fig. 2.10 Sequence diagram for the drive MEV [19]

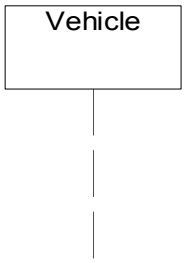


Fig. 2.11 Lifeline of Vehicle

Fig. 2.12 Combined Fragment

Table 2.1 The types of Combined Fragment

複合フラグメントの種類	概要
alt	条件分岐
loop	繰り返し
Ref	相互作用使用の参照
parallel	並列処理

図 2.10 はユースケース MEV の運転「Drive MEV」の振る舞いをシーケンス図により示している．シーケンス図(Sequence Diagram)は，SysML モデル内の構造的な要素間の相互作用を時系列に表現する図である．シーケンス図の中で相互作用を行う要素を表現するモデル要素をライフライン（Lifeline)と呼ぶ．図 2.z9 は車両「Vehicle」のライフラインを示す．ライフライン間のやりとりを表現するモデル要素をメッセージ（Message）と呼ぶ．メッセージは，操作の呼び出しや信号の伝達を矢印で表す．矢印はメッセージの送信側のライフラインから，メッセージの受信側のライフラインへ引く．また，シーケンス図で分岐やループ等の制御構造を表すためのモデル要素として，図 2.12 のような複合フラグメント(Combined Fragment)という要素がある．複合フラグメントの種類と概要を表 2.1 に示す．

図 2.10 よりニュートラルパワーの制御「Control Neutral Power」，前進パワーの制御「Control Forward Power」，後退パワーの制御「Control Reverse Power」，およびブレーキ制御「Brake Control」は駆動・制動トルク制御に，方向の制御「Direction Control」は前輪操舵角制御に関わっている．VSCS は駆動・制動トルク制御および前輪操舵角制御を統合した制御を行っている．そのため，MEV の VSCS に対する不安全な制御アクションを特定する必要がある．

図 2.2 は MEV の制御構造図に示すように，STAMP/STPA の解析では最初に制御アクションに関わる制御構造図「Control Structure」を作成する必要がある．従来のハザード解析手法のような，個々のコンポーネントの故障に着目することではなく，連携するコンポーネント間の相互作用に関するシステムレベルの問題に着目するために制御構造図を使う．しかし，アクションの順序およびタイミングはこのブロック図（制御構造図）では表現できないが，シーケンス図を用いれば表現できる．例えば，アクセル，ブレーキ，およびステ

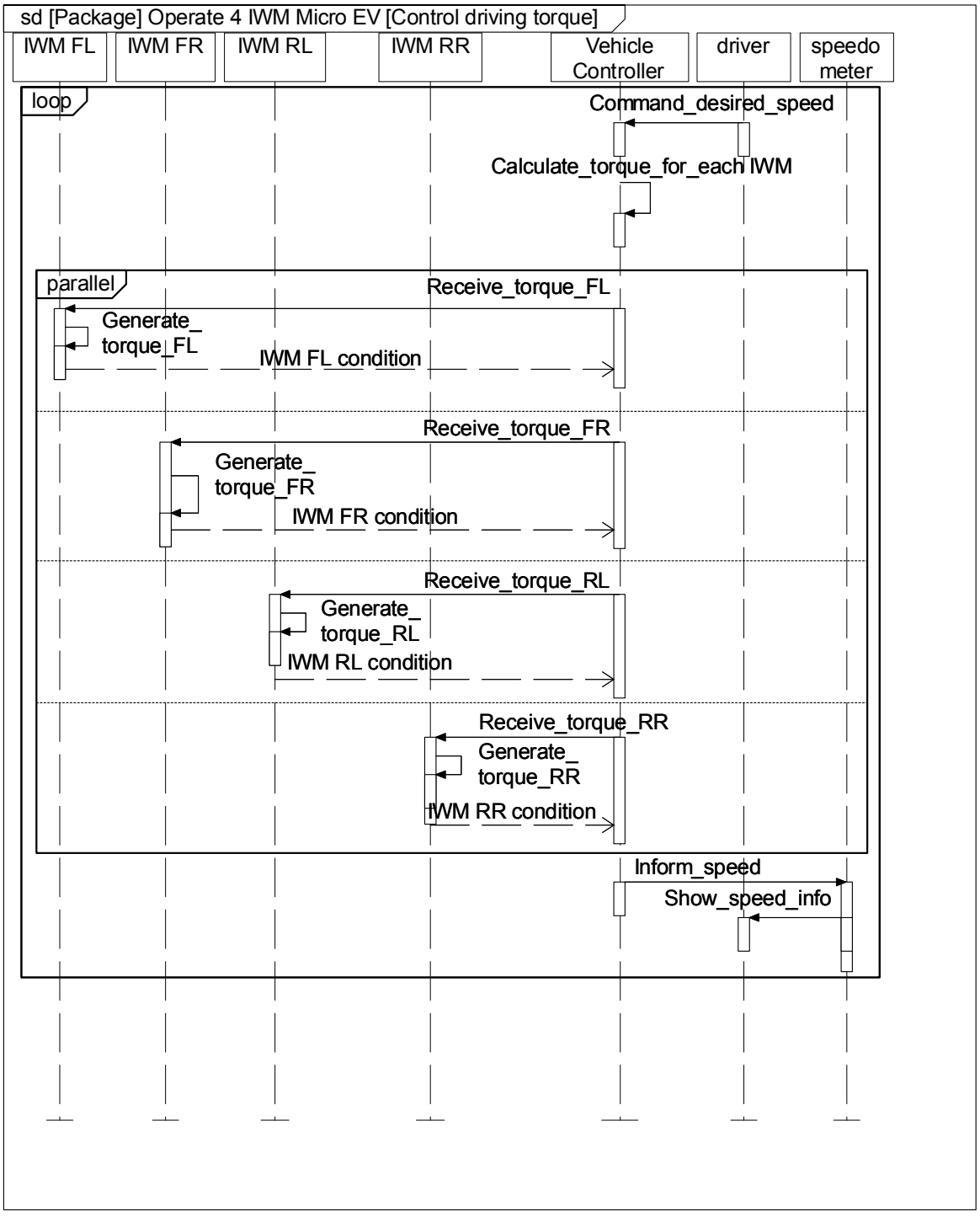


Fig. 2.13 Sequence diagram for the control driving torque

FL : front left; RL: rear left; FR: front right; RR: rear right

リングからの信号およびそれぞれのモータに送るトルク指令があり，両方の順序が明確でない．通常はドライバが最初に入力を与えるが，他の信号が先に出るという不安全な制御アクションが導出される．

図 2.13 は駆動・制動トルクの制御「Control driving torque」という点でシステムの振る舞いを分析したシーケンス図を示す．このシーケンスを作ることで，システムの構成要素間でどのようなアクションが行われているかを分析することができる. 図 2.13 では,「driver」から「Vehicle Controller」へのメッセージ「Command desired speed」は，ドライバがアクセルで期待する速度を入力することを表している.「Vehicle Controller」はこの入力に基づき，

速度の目標値を達成するために，各モータ（IWM FL，IWM FR，IWM RL，IWM RR）が必要なトルクを計算する．また,「parallel」の複合フラグメントが記述されており，車両のコントローラ「Vehicle Controller」はそれぞれの IWM にトルク制御の指令値を並行・同時に与えていることを示している．摩擦ブレーキでの制動制御も同様に実施されている．

さらに制御構造図と比較し，シーケンス図を用いることでさらに詳細な相互作用を解析することができる．従来の方法を用いても，システムレベルの故障に関してある程度分析は可能であるが, 相互作用に着目するシーケンス図を用いると, 解析がさらに容易になる．図2.13 に示すように, シーケンス図はそれぞれのコンポーネント間の相互作用だけでなく, メッセージの順序・タイミングも表すため，STAMP/STPA による不安全な制御アクションの特定をさらに導き出す．また，図 2.13 では車両のコントローラからそれぞれのモータにトルクの指令値を並行して送っている．この指令値の送信タイミングがずれると，システムの不安全な動作につながる. 次の節に不安全な制御アクションの特定に関して説明する．

2.5　不安全な制御アクションの特定

相互作用を検討した図 2.13 をもとに，2.2 節に記述された 4 つガイドワードを用いて，不安全な制御アクションを特定する．表 2.2 は不安全な制御アクションの特定によるハザードシナリオの分析結果を表す. 操縦安定性には駆動・制動トルク制御, 前輪操舵角制御, および両方の統合制御を用いることが考えられる．そのため，それぞれの制御アクションに 4 つのガイドワードを適用して導く．

下記は不安全な制御アクションを特定するための STPA に使われるガイドワードである．

① Not Provided

安全性を確保する制御アクションをしない

② Incorrectly Provided

不安全なアクションをする

③ Provided Too Early, Too Late, or Out of Sequence

誤ったタイミングあるいは順序の間違い

④ Stopped Too Soon

停止が早すぎる

以下に，一つのメッセージアクションにガイドワードを適用する一事例を示す.

Receive_torque_FL についての不安全な制御アクションの特定

1. Not Provided

安全性を確保する制御アクションをしない

1.1 コントローラからの指令値が来ない

- 以前の設定速度で走行
- 周辺の車に衝突
- 乗員に損傷

2. Incorrectly Provided

不安全なアクションをする

2.1 読み取り指令値が間違い

2.1.1 読み取り信号が指令値より小さい場合

- 操舵が困難になる
- 車両の操縦安定性が崩れる
- 隣車に衝突

2.1.2 読み取り信号が指令値より大きい場合

- 操舵が困難になる
- 車両の操縦安定性が崩れる
- 前車，後車，隣車に衝突

3　Provided Too Early,　Too Late,　or Out of Sequence : 誤ったタイミングあるいは順序の間違い

- 想定より遅く指令値がくる場合
- トルクの発生が遅れる
- 減速が遅れる

4　Stopped Too Soon : 停止が早すぎる

駆動あるいは制動トルク制御が停止指令を出す前に車両が停止する

本研究に着目する制御アクションは「駆動/制動トルク制御」,「前輪操舵角制御」，および「駆動/制動トルクと前輪操舵角を統合した制御」である．各制御アクションにそれぞれ4つのガイドワードを適用し，不安全な制御アクションを特定する．具体的には「駆動/制動トルク制御」に「安全性を確保する制御アクションをしない」のガイドワードを適用する．その結果，4つの不安全な制御アクションが特定された．これらは,「1a)　アクセルペダルを外してもアクセルコマンドが出る」,「1b)　摩擦ブレーキの圧力指令値が与えられない」,「1c)　ブレーキ制動ができない」，および「1d)　コントローラからの指令値が来ない」である．そして,「不安全なアクションをする」を適用し，3つが特定された．これらは「1e)　1，2，または，3台のモータが駆動力を出さない」,「1f)　誤った値を検出する．読み取り信号が指令値より小さい，あるいは大きい場合」,「1g)　電気が流れない」ということである.「誤ったタイミングあるいは順序の間違い」による特定した結果はもっとも多く，6つまで特定した．これらは「1h)　駆動，あるいは，制動トルクの発生が意図しているより遅れる，または，早すぎる」,「 1i)　アクセルペダルを踏まなくても，トルクの計算というアクションが始まる」,「1j)　ブレーキペダルを踏まなくても，摩擦ブレーキの圧力値計算が始まる」,「1k)　モータの指令が同時に与えられない」,「1l)　トルクの計算が実施する前に，トルク指令が与えられる」，および「1m)　トルク指令を受信する前に，トルクが発生する．

Table 2.2 STPA Analysis: Identify Unsafe Control Actions

制御 アクション	安全性を確保する制御アクションが動作しない	不安全なアクションをする	誤ったタイミング，あるいは，間違った順序	停止が早すぎる
駆動/制動トルク制御	1a)　アクセルペダルを外してもアクセルコマンドが出る. 1b)　摩擦ブレーキの圧力指令値が与えられない. 1c)　ブレーキ制動ができない. 1d)　コントローラからの指令値が来ない	1e)　1，2，または，3 台のモータが駆動力を出さない. 1f)　誤った値を検出する. 読み取り信号が指令値より小さい, あるいは大きい場合 1g)　電気が流れない.	1h)　駆動，あるいは，制動トルクの発生が意図しているより遅れる，または，早すぎる. 1i)　アクセルペダルを踏まなくても，トルクの計算というアクションが始まる. 1j)　ブレーキペダルを踏まなくても，摩擦ブレーキの圧力値計算が始まる. 1k)　モータの指令が同時に与えられない	1n)　駆動あるいは制動トルク制御が停止指令を出す前に車両が停止する.

			1l) トルクの計算が実施する前に，トルク指令が与えられる. 1m) トルク指令を受信する前に，トルクが発生する.	
前輪操舵角制御	2a) ステアリングが効かない.	2b) ドライバからのステアリング入力と前輪操舵角の実際の角度が異なる.	2c) 前輪操舵角制御の実行が意図しているより遅れる，または，早すぎる. 2d) ステアリングで入力する前に，ステアリングの指令が出る. 2e) ステアリング指令が出る前に，前輪操舵角が発生する.	2f) 前輪操舵角制御が停止指令を出す前に車両が停止する.
駆動/制動トルクと前輪操舵角を統合した制御	3a) VSCS が駆動/制動トルク，あるいは，前輪操舵角の制御のみ実施する.	3b) 駆動/制動トルクの配分が適切ではない.	3c) 統合した操縦安定化制御の実行が意図しているより遅れる，または，早すぎる	3d) 統合した操縦安定化制御が停止指令を出す前に車両が停止する.

STAMP/STPA のガイドワードを適用した結果，制御構想図に特定できなかった不安全制御アクションを，図 2.13 をもとに相互作用を検討すると特定できました．例えば，「1l)　トルクの計算が実施する前に，トルク指令が与えられる」および「1m)　トルク指令を受信する前に，トルクが発生する」は制御構造図では特定できなくて，図 2.13 のシーケンス図を用いることで，特定できた．図 2.13 に示すような駆動トルク制御アクションのシーケンス図を用いることで，相互作用は時間的・タイミングの分析が可能なため，一つのガイドワード，タイミング・順序の分析が容易になる．見つけにくい不安全な制御アクションを減らすことができる．相互作用のメッセージも記述されるため，実際に実施されるアクションも想定できる．

例えば「1e)　1，2，または，3 台のモータが駆動力を出さない」という場合は，駆動・制動制御アクションの不安全性がインホイールモータに関わることが大きいことがわかった．前輪操舵角制御アクションではパワーステアリングシステムに大きな影響があるという問題がある．そして，2.6 節に不安全制御アクションに至る原因を定義します．また，STPA はコンポーネント故障の対策方法を考えることではなく，分析した不安全アクションの安全制約を決めることである．駆動・制動トルクと前輪操舵角を統合した操縦安定化制御では，統合の問題が大きく．二つの制御を行うためには，上手く組み合わせることが重要である．

2.6　潜在的原因の特定

STPA はコントロールループ上のガイドワードを用い，不安全な制御アクションの潜在的原因を特定する．特に，ソフトウェアや人間が起因となる原因として，コントローラの想定するプロセスモデルが，実際のプロセスの状態と矛盾することで起きる原因を特定する．STPA により不安全な制御アクション毎にコントロールループを作る必要がある．本研究に着目する「駆動/制動トルク制御」，「前輪操舵角制御」，および「駆動/制動トルクと前輪操舵角を統合した制御」の制御アクション毎に，コントロールループを作成し，検討する．

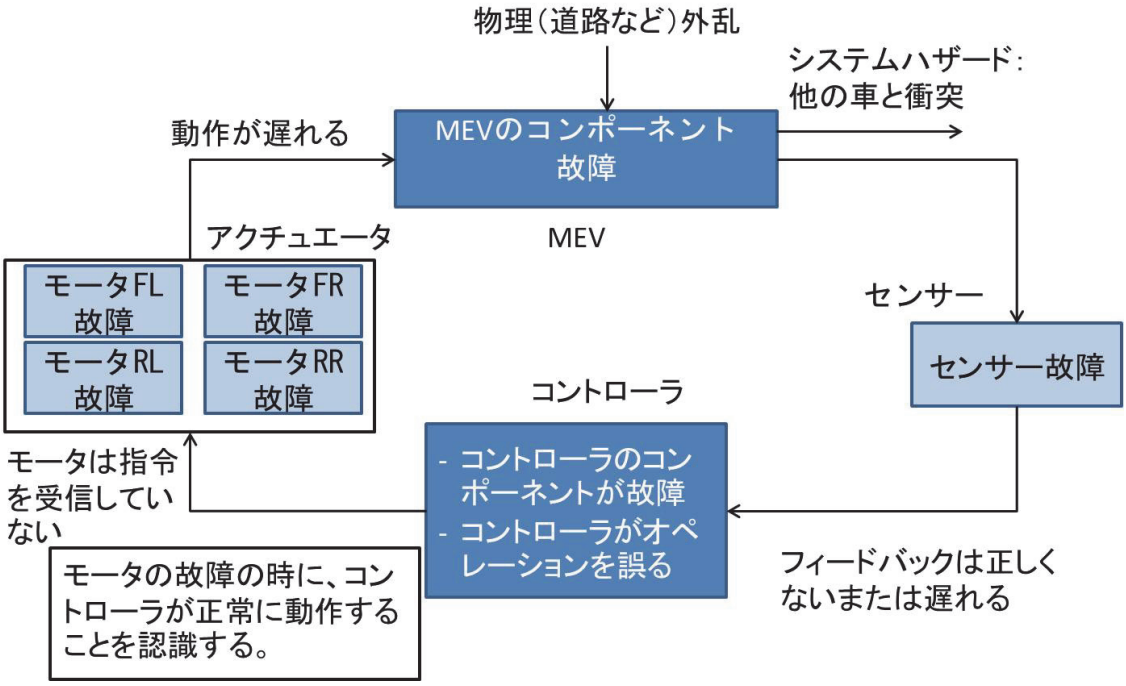


Fig. 2.14 Defining the causal factor of inadequate control action in torque driving control

図 2.14 は駆動・制動トルク制御における不安全な制御アクションの原因を特定するためのコントロールループを示す. コンポーネントや相互作用に起こり得る問題を明確にする. このコントロールループは図 2.6 をもとに作成する. 図 2.6 の上ガイドワードを適用し，不安全な制御アクションにつながる潜在的原因を特定する. 図 2.14 は制御工学によく使う制御ループと同様である. 図 2.2 と似ているが，不安全な制御アクションの潜在的原因をさらに明確にするものである. システムの 4 つの主な要素は，プラント・制御対象，センサー，コントローラ，およびアクチュエータである. それぞれの要素またはそれを繋ぐインタフェースは起こり得る不安全なアクションを導く. 要素によくある問題は故障することである. この故障に対して，冗長する必要があるかを検討する必要がある.

特定した潜在的原因を以下に記述する.

(1) コントローラにおける潜在的原因

- コントローラのコンポーネントが故障
- コントローラがオペレーションを誤る
- ステアリングとモータの故障の時に，コントローラが正常に動作することを認識する

(2) 制御対象，MEV，における潜在的原因

- MEV のコンポーネントの故障

(3) アクチュエータにおける潜在的原因

- インホイールモータの故障

(4) センサーにおける潜在的原因

- センサーの故障

(5) 相互作用に関する潜在的原因

- フィードバックは正しくないまたは遅れる
- ステアリングあるいはモータは指令を受信していない
- 外乱

図 2.15 は前輪操舵角制御における不安全な制御アクションの原因を特定するためのコントロールループを示す．両方の図から，主にアクチュエータが異なることがわかった．潜在的原因も，ほぼ駆動・制動トルク制御と同様であり，異なるところはアクチュエータ，ステアリングに関することである．駆動・制動トルク制御ではアクチュエータとして，インホイールモータを 4 台用いる．トルクを発生するためのアクチュエータを 4 台使うこと

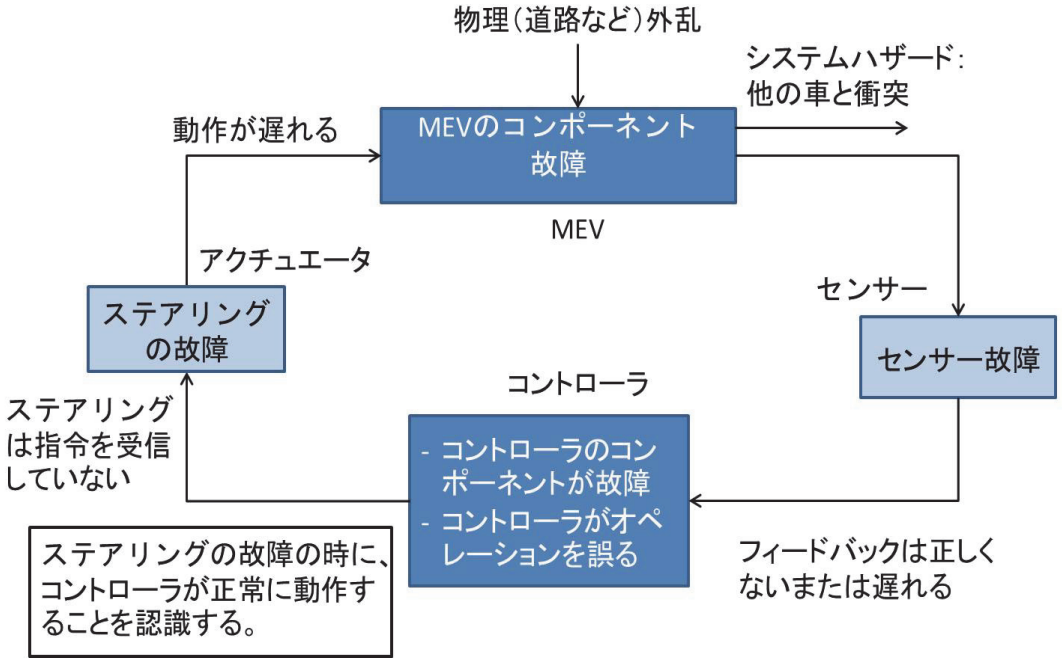


Fig. 2.15 Defining the cause of inadequate control action front steering control

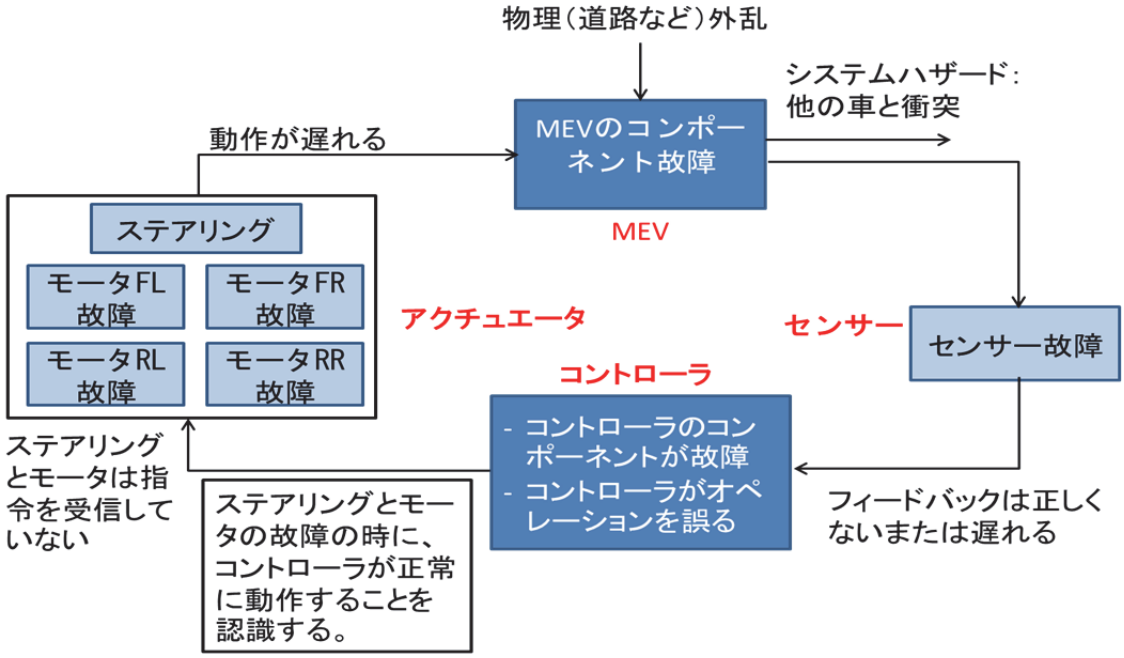


Fig. 2.16 Defining the cause of inadequate control action of integrating control for driving torque and front steering control

になるので，1，2，または 3 台が故障した場合に MEV の操縦安定性にどんな影響あるのかをさらに検討する必要がある．モータの故障に関して 3 章に述べる．インタフェース・相互作用に多くある問題は信号の送信の遅れまたは早すぎについても検討する．

図 2.16 は駆動・制動トルクおよび前輪操舵角を統合した制御における不安全な制御アクションの原因を特定するためのコントロールループを示す．アクチュエータの部分には 4 つのインホイールモータおよびステアリングがある．統合制御の潜在的原因は両方の潜在的原因の組み合わせである．

STPA はコントロールループ上のガイドワードを用い，不安全な制御アクションの潜在的原因を特定する必要がある．しかし，本研究にこの段階を行い，ほぼ 2.5 節に述べられた 4 つガイドワードで不安全な制御アクションを特定した結果とほぼ同様である．そのため，今度の安全解析を実施する時には，シーケンス図で相互作用を検討し，4 つのガイドワードを適用することで，十分だと考えられる．

SysML のシーケンス図およびユースケース図を用い，STAMP/STPA を適用することで，システムの相互作用に基づくハザードを分析した．その結果，コンポーネントのハザード

のみでなく, コンポーネントの相互作用におけるハザードが多数存在することがわかった. 特に時間的な問題やインタフェースに送られる信号の誤り等が導出された. ハザードの種類により対策の方法が異なるため, ハザードの分類を行う必要があることがわかった.

導出されたハザードを除去, あるいは, 抑制するために, 安全制約を特定する必要があることを示した. 不安全な制御アクションを想定してシミュレーションを行うことで, 各安全制約の適切なパラメータを導いた.

STAMP/STPA のプロセスと異なり, 制御構造図だけでなく最初にシーケンス図で相互作用も検討する. 制御構造図を使用すると, アクションの順序および時間がガイドワードで予想できる. 着目する制御アクションをシーケンス図に実現する. 最後のプロセスにダイナミックなシミュレーションを行う. このダイナミックなシミュレーションは安全制約および被害の大きさを特定するために使用する.

本研究で必要に応じて STAMP/STPA に MBSE によるアプローチを加えて実施する. 加えるところを以下に述べる.

(1) 制御アクションのタイミング, および, 順序を考慮した相互作用の解析・シナリオ検討のために MBSE を適用するシーケンス図, ユースケース図を用いる.
(2) 被害の大きさの特定を行う後に, 対策のために使用する.
(3) 潜在的原因の特定ためのコントロールループを制御工学に合わせる. 制御構造図と比べやすいために, 矢印の向きおよびシステムの要素の位置を制御構造図と同様にする.

第 3 章
安全制約の特定

3.1 概要

本章では，2.5 節で特定し不安全な制御アクションを抑制，あるいは，除去するために安全制約（Safety Constraints）を特定する必要がある．安全制約とはシステムとしての事故に至らないように安全を確保するために満たすべき条件である．例えば，「アクセルペダルから足を外してもアクセルコマンドが出る」という不安全な制御アクションに対しては，「アクセルコマンドはアクセルペダルを踏んだ時にのみ出力される」という安全制約が挙げられる．他には，「信号送信の遅れ」という不安全な制御アクションにおける安全制約は「・・ms 以上遅れてはならない」というように設定できる．なお，このパラメータの値は設計をする際に決めることとなる．

本研究では安全制約を検討するために，Dymola (Dynamic Modeling Laboratory)を利用してシミュレーションを実施する．Dymola は Modelica 言語をベースとした物理系複合モデリング・シミュレーションツールである．

図 3.1 は Dymola で記述したシミュレーションモデルの例を示しており, 車両モデル, ドライバモデル, 路面モデル, および, 天候モデルから構成されている. 図 3.2 は Dymola が提供するドライバモデルの構成を示す．ドライバモデルは，走行状態の認知(Perception)，目標経路点列の作成(Planning)，目標経路への追尾操作(Tracking)の 3 個のブロックから構成されている．認知ブロックは，ドライバが認知する現在の車両の状態（位置，速度，角度等）を算出する．前輪操舵角制御は，目標経路への追尾操作ブロックに関係する. 目標経路への追尾操作のブロックは, 操縦安定化制御システム, および, 速度のコントローラは車両モデルの外部に位置する．

図 3.3 は車両モデルの構成を示す．車両モデルはパワートレイン部，シャシ部とブレーキ部で構成されている．MEV のパワートレインは，それぞれの車輪にインホイールモータ が搭載されている．そのため，4 つの車輪がそれぞれ独立に駆動・制動することができる．シャシ部に含まれているタイヤは Magic Formula の非線形モデルであり, 従来車両のタイヤに比べて横剛性が低く, スリップ角に対して横力が早期に飽和する特性となっている[16]．車両モデルへの制御入力は，キャンバ角，前輪操舵角，各車輪モータトルクであり，出力としては車両の速度，横変位，横滑り角，ヨーレートなどが選定できる[16].

表 3.1 は MEV と従来の車両の比較を一覧としてまとめている．MEV は軽量化がされている一方で車両の高さは従来車両とほぼ変わらないという特徴を持つ.

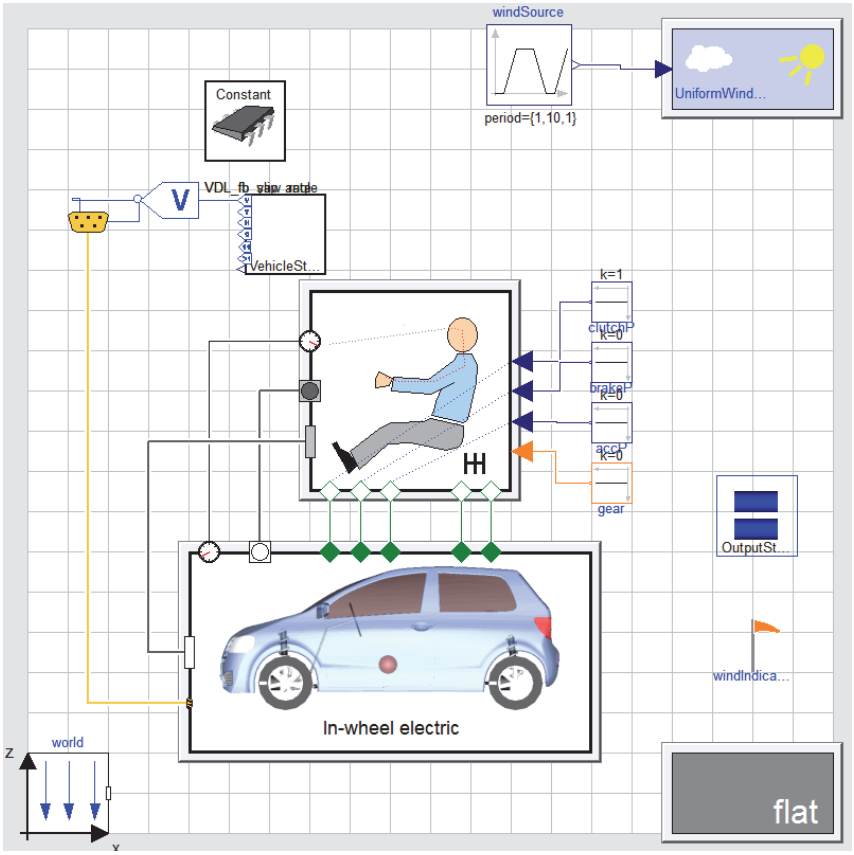


Fig. 3.1 Simulation model in Dymola

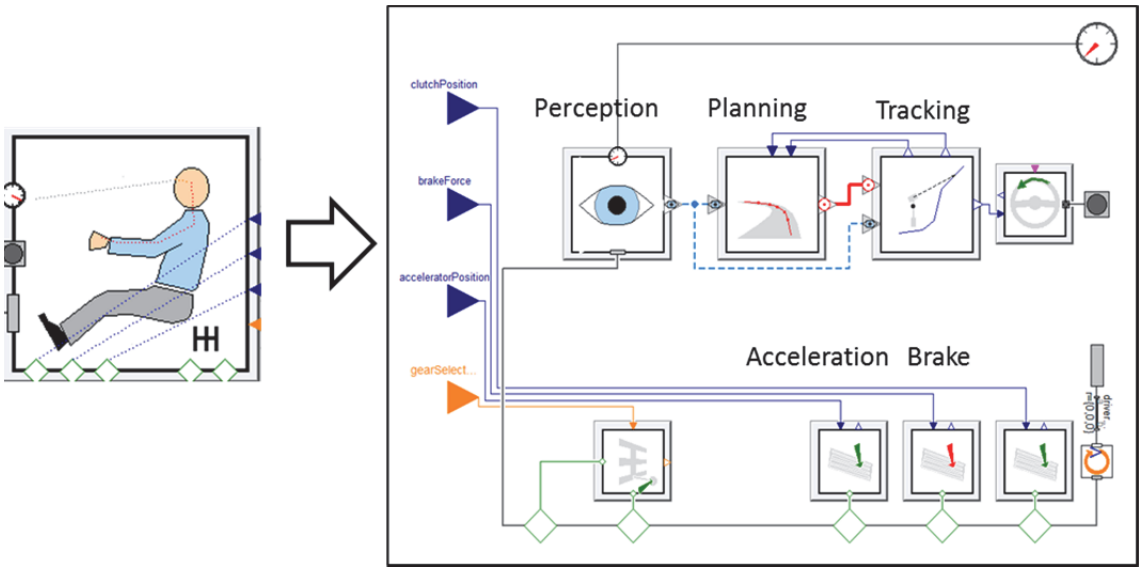


Fig. 3.2 Structure of driver model

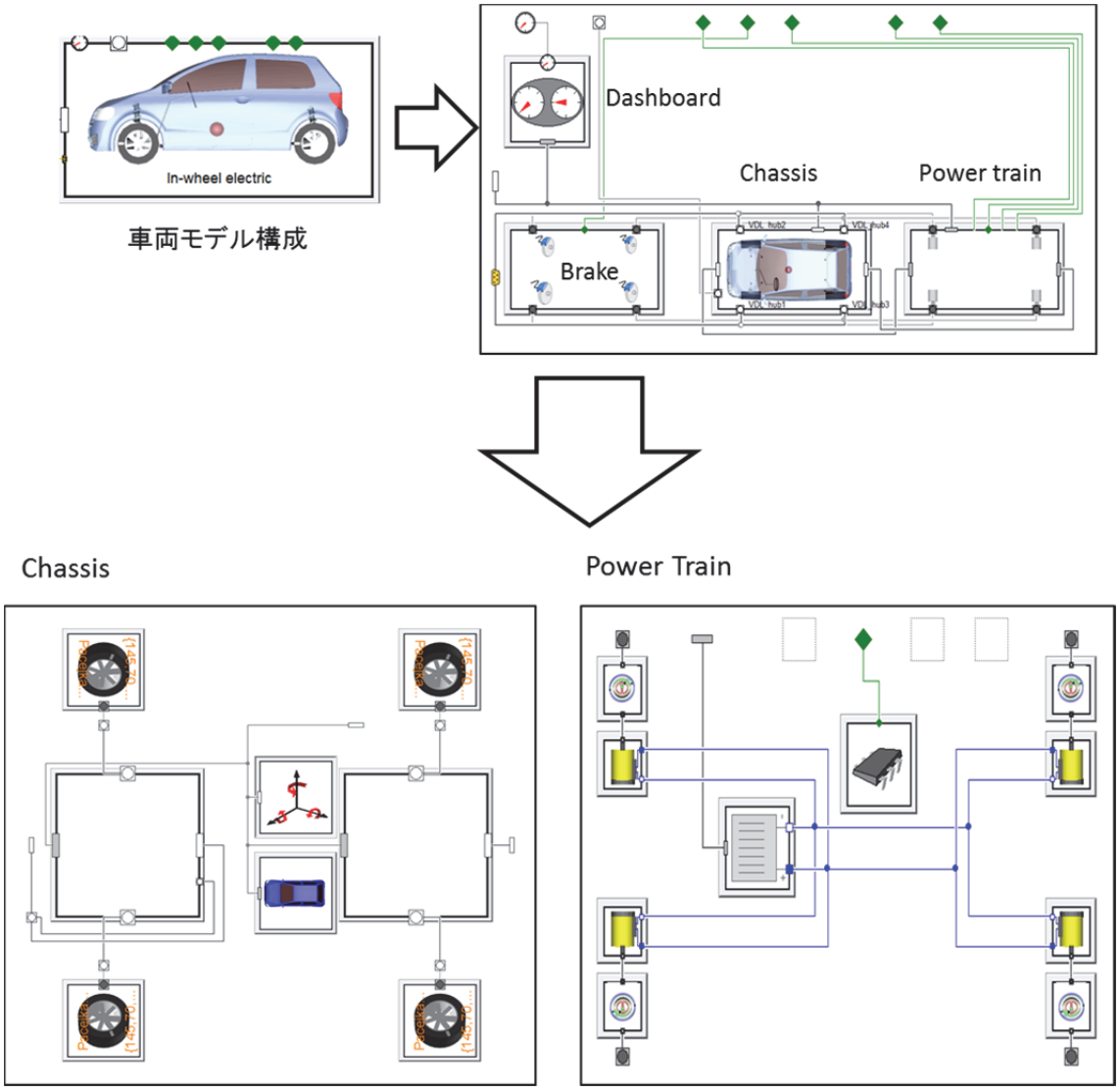


Fig. 3.3 Structure of vehicle model

Table 3.1 Vehicle Specification

	MEV	Conventional vehicle
Weight	510 kg	1300 kg
Wheel base	2000 mm	2600 mm
Width	1190 mm	1760 mm
Height	1460 mm	1515 mm

3.2　不安全な制御アクションのシミュレーション

本研究では操縦安定化制御システム[9]を用いる時と用いない時を想定して，不安全な制御アクションのシミュレーションを行う．本節では，3 種類のシミュレーション結果について述べる（図 3.4，図 3.5，図 3.6）．シミュレーションの実施条件は下記の通りである：

(1)　モータがトルクを発生しない場合のシミュレーション（図 3.4）の条件

- シミュレーション開始後 5 秒の時点からインホイールモータへのトルクが発生しなくなる．
- シミュレーション開始後 5 秒の時点からインホイールモータへのトルクが発生しなくなる．なお，トルクが発生しないインホイールモータはグラフによって異なる．

(2)　モータのトルクが発生しなくなるという状況下で MEV の制御の有無を比較するためのシミュレーション（図 3.5）の条件

- ドライバのステアリング指令の時間遅れが発生しない．
- 操縦安定性を確保するための独立トルク制御，前輪操舵角とトルクを統合した制御（VSCS）をそれぞれ用いる MEV，および，制御なしの MEV の利用．

(3)　ステアリング指令の遅れが生じる場合のシミュレーション（図 3.6）の条件

- ドライバのステアリング指令はシミュレーション時間内で何度か遅れる．
- シミュレーション開始後 3 秒の時点から，前左のインホイールモータへのトルクが発生しなくなる．

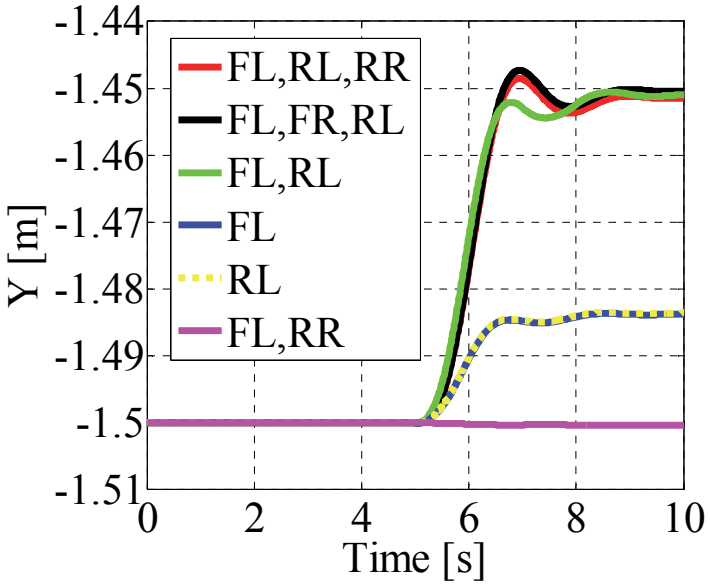
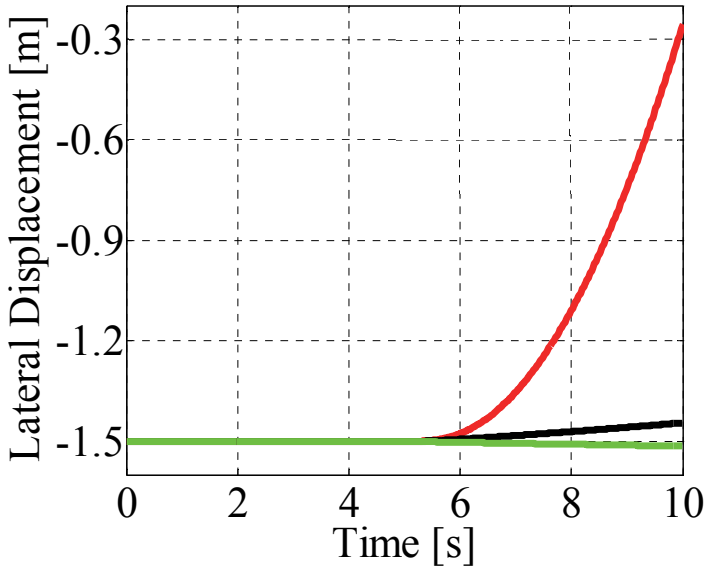
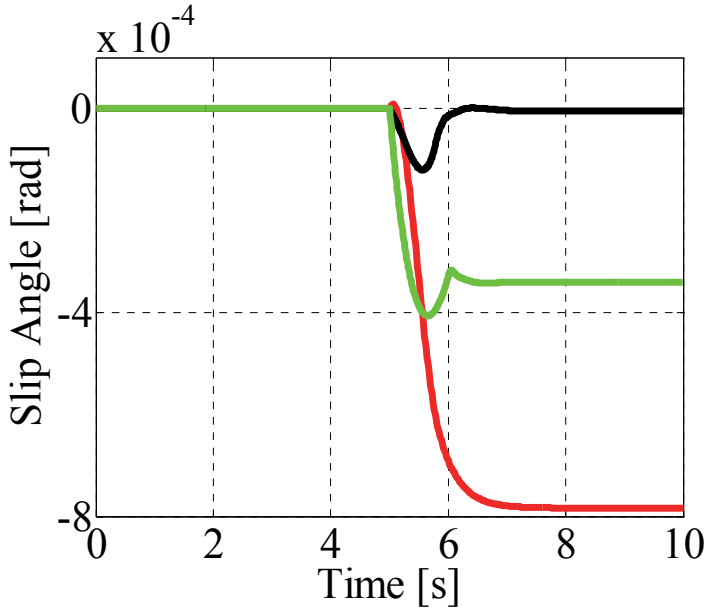


Fig. 3.4 Simulation result when motor can't generate torque

FL : Front left (前左); FR : Front right (前右); RL : Rear left (後左); RR : Rear right (後右)



(a) Trajectory

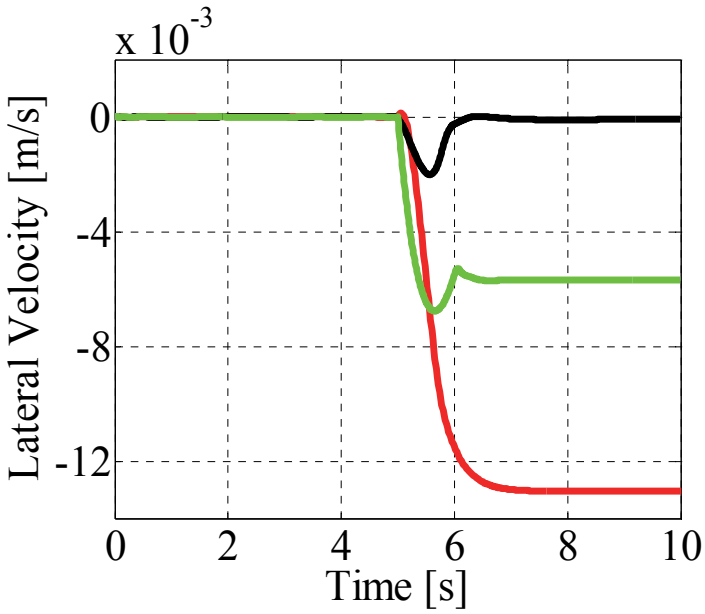


(b) Slip Angle

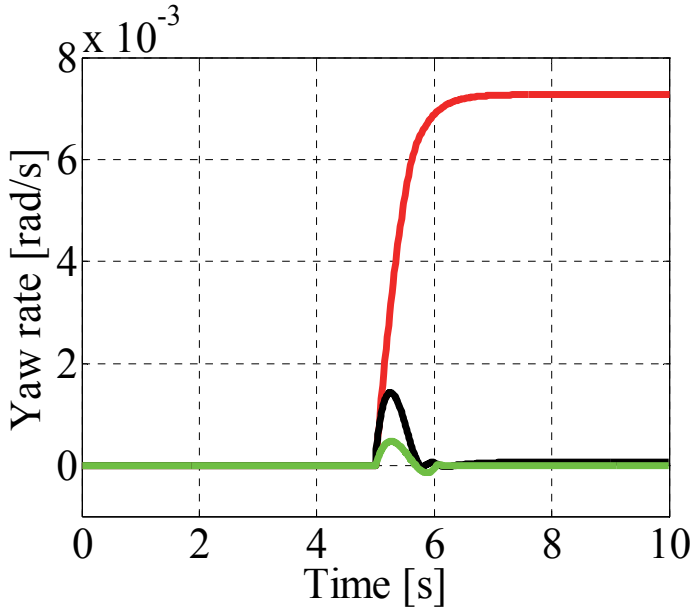
Fig. 3.5 Simulation result of MEV with control and not when motor fault happen

: without control, : torque control,

: torque and front steering control



(c) Lateral velocity

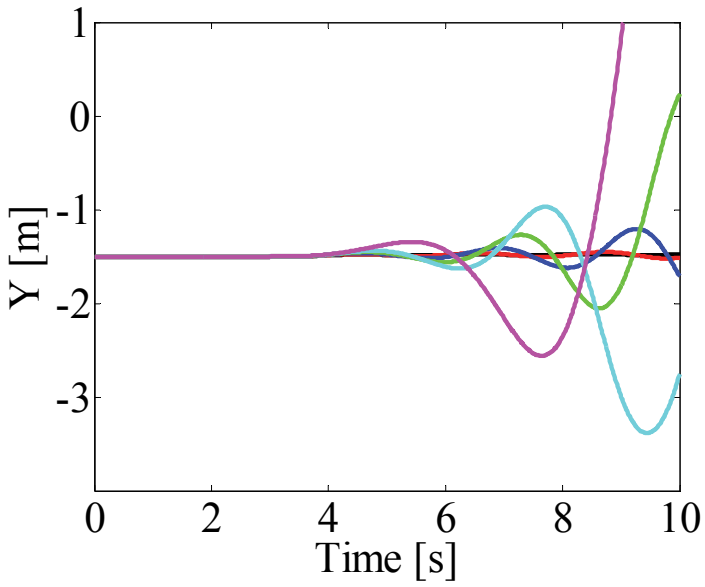


(d) Yaw rate

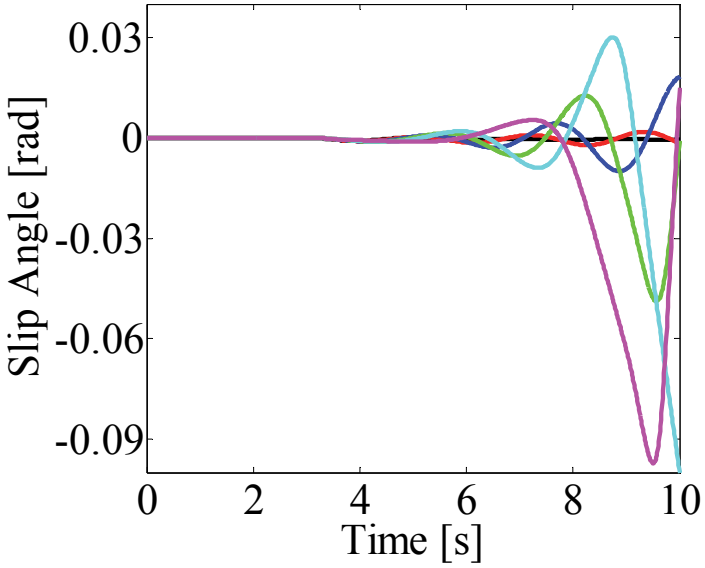
Fig. 3.5 Simulation result of MEV with control and not when front-left motor fault happen

: without control, : torque control,

: torque and front steering control



(a) Trajectory

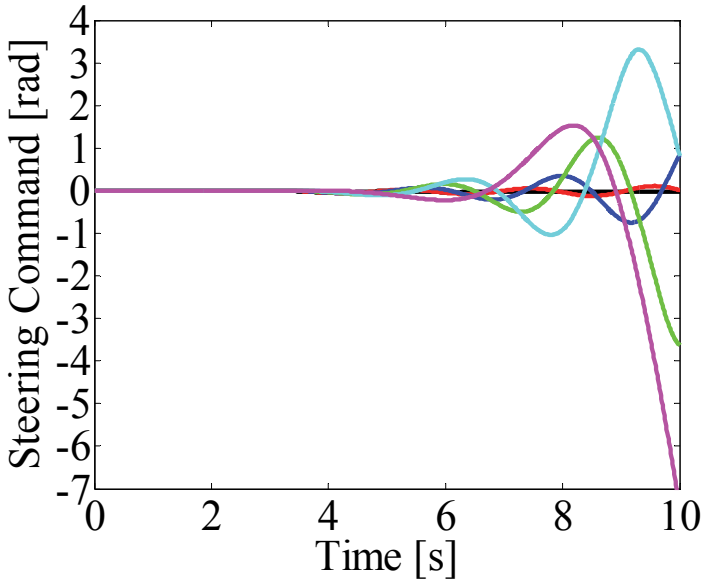


(b) Slip Angle

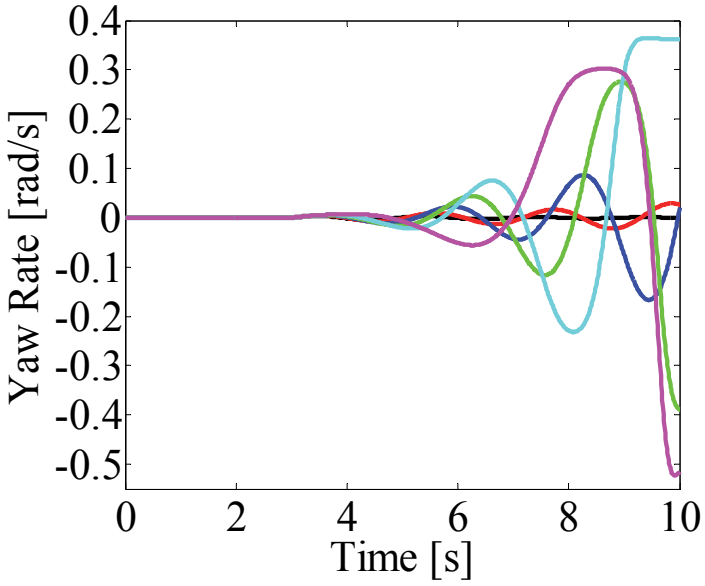
Fig. 3.6 Simulation result with steering command delay

: Delay 0.1 s ; : Delay 0.2 s ; : Delay 0.3 s ;

: Delay 0.4 s ; : Delay 0.5 s ; : Delay 0.6 s



(c) Steering Command



(d) Yaw Rate

Fig. 3.6 Simulation result with steering command delay

: Delay 0.1 s ; : Delay 0.2 s ; : Delay 0.3 s ;

: Delay 0.4 s ; : Delay 0.5 s ; : Delay 0.6 s

まず，表 2.2 で特定した「1e)　1，2，または，3 台のモータが駆動力を出さない.」という不安全な制御アクションに関するシミュレーションを行う．車速 60km/h で車両が走行し，開始後 5 秒の時点からインホイールモータへのトルクが発生しなくなる．なお，トルクが発生しないインホイールモータはグラフによって異なる．このインホイールモータ故障に対する走行軌跡を図 3.4 に示す．図 3.4 の(a)横変位，(b)スリップ角，(c)ステアリング指令値，(d)ヨーレートを示す図では，VSCS は安全性を保つことができることを確認した.

前左インホイールモータのトルクが発生しない際に，操縦安定性を確保するための独立トルク制御，前輪操舵角とトルクを統合した制御（VSCS）を用いる場合，および，これらの制御を用いない場合の結果を図 3.5 に示す．このシミュレーションでは，走行スタート後から 5 秒経過した際に前左(FL)の IWM へのトルクが全く発生しなくなる．トルク制御単独は VSCS より横変位が大きい．この結果より，VSCS はトルク制御より優れていることが確認された．ただし，トルク制御を用いると横変位が約 5 cm 発生しているが，安全性は確保できていると考えられる.

次のシミュレーションではステアリング指令の遅れが生じることを想定している．車両は車速 60km/h で走行し，シミュレーション開始後 3 秒の時点からインホイールモータへのトルクが発生しなくなる．図 3.6 の(a)横変位，(b)スリップ角，(c)ステアリング指令値，(d)ヨーレートを示す図では，インホイールモータのトルクが発生しない時にステアリング指令の入力の遅れが 0.2 秒以下であると，操縦安定性が十分に保たれる．しかし，ステアリング指令の入力の遅れが 0.3 秒以上になると，操縦安定性が大幅に不安定になることがわかった.

3.3　安全制約と被害の大きさの特定

3.2 節で示したシミュレーション結果に基づいて安全制約を特定する．例えば，表 2.2 の「1e)　1，2，または，3 台のモータが駆動力を出さない」という不安全な動作に関しては「駆動あるいは制動トルク制御の実行が意図しているより 0.2 秒以上遅れてはならない」という安全制約を特定することができる.

ISO26262 は，車載の安全関連 E/E(Electronic/Electric)システムの開発・運用のためのガイドラインである．E/E システムとは自動車の電気・電子システムである．ISO26262 では，特定の状況下で必ず発生する故障であるシステマティック故障，および，ハードウェアの劣化によりランダムに生じるランダムハードウェア故障によるリスクを回避

するための要求事項を規定する． 表 3.2 はシビアリティのクラスを示す．シビアリティは，ドライバまたは他の交通関係者が受ける傷害の大きさの見積もりである．本研究では被害の大きさのレベルを次に示す軽度および重度の 2 個で定義する．軽度な不安全な制御アクションは VSCS で対応が可能なものであり，重度は VSCS で対応が不可能なものである．表 3.3 は失陥モードのリストを表す．

Table 3.2 Classes of severity and countermeasures

クラス	記述	対策
S0	傷害なし	なし
S1	軽度および中継度の傷害	VSCS
S2 **S1+S1**	重度および生命を脅かす傷害（生存の可能性がある）	安全に停止する
S3 **S2+S1** **S2+S2**	生命を脅かす傷害（生存がはっきりしない），致命的な傷害	安全に停止する

Table 3.3 Fault mode

		失陥モータのモード
FL RL	FR RR	*)1 台
FL,RL,RR FL,FR,RL	FR,RL,RR FL,FR,RR	*)3 台
FL,RL	FR,RR	*)左側，右側（側部）
FL,RR	FR,RL	対角
FL,FR	RL,RR	前輪，後輪

FL : Front left (前左)；FR : Front right (前右)；RL : Rear left (後左)；RR : Rear right (後右)

3.2 節で示したシミュレーション結果に基づいて安全制約と被害の大きさのレベルを特定する．図 3.5 の結果で VSCS を用いると，約 5cm の横変位が発生しているが，安全

性は保たれていると考えられる．そのため，「1e)　1，2，または，3 台のモータが駆動力を出さない」の不安全な制御アクションは軽度であると定める．

例えば，「1e)　1，2，または，3 台のモータが駆動力を出さない」および「2c)　前輪操舵角制御の実行が意図しているより遅れる，または，早すぎる」という組み合わせの不安全な制御アクションのシミュレーションを行った結果，VSCS のみでは安全性を確保できないため，被害の大きさのレベルを重度と特定する．安全制約は「前輪操舵角の指令より 0.2 ms 以上遅れてはならないまたは早すぎていけない」と設定する．一方，単体の不安全な制御アクションであれば，被害の大きさは軽度である．表 3.2 は ISO26262 に基づく被害の大きさのレベルを示す．組み合わせのクラス，および，それらに対する対策は本研究で定めたものである．

以下に表 2.2 で特定した不安全な制御アクションの安全制約と被害の大きさレベルを記述する．

1a)　アクセルコマンドはアクセルペダルを踏んだ時のみ出力される(S2)
1b)　摩擦ブレーキ圧力指令値が与えられる(S2)
1c)　ブレーキ制動ができる(S2)
1d)　コントローラから制御対象 MEV に指令値が届かなければならない(S3)
1e)　駆動あるいは制動トルク制御の実行が意図より 0.2 s 以上遅れてはならない(S1)
1f)　駆動トルクが指令値より 2 倍以上超えては行けない(S2)
1g)　必要に応じて流れる(S2)
1h)　駆動あるいは制動トルク制御の実行が意図より 0.2 s 以上遅れてはならない(S2)
1i)　アクセルコマンドはアクセルペダルを踏んでいる時だけに出る(S2)
1j)　ブレーキコマンドはブレーキペダルを踏んでいる時だけに出る(S2)
1k)　モータの指令が同時に与えられなければならない(S2)
1m)　トルク指令を受信した後に，トルクが発生する(S1)
1n)　駆動あるいは制動トルク制御が停止指令を出した後のみに停止する(S2)
2a)　ドライバがステアリング指令を与える限り，ステアリングが効く(S3)
2b)　発生する前輪操舵角が指令値との差が 4 割以下にならなければならない(S2)
2c)　前輪操舵角の指令より 0.2 ms 以上遅れてはならない，または，早すぎてはいけない(S1)
2e)　ステアリングの入力の後に，前輪操舵角が発生する(S1)
2f)　前輪操舵角制御が停止指令を出した後のみに停止する(S2)

3a)　VSCS が駆動/制動トルクおよび前輪操舵角を統合する制御を実施する(S2)
3b)　駆動/制動トルクの配分が適切に実施する(S2)
3c)　統合した操縦安定化制御の実行が意図 0.2 s 以上遅れてはならない(S2)
3d)　統合した操縦安定化制御が停止指令を出した後のみに車両が停止する．(S2)

シミュレーションを行った結果，軽度な不安全な制御アクションは主にコンポーネントの故障に関連し，特にインホイールモータのトルクが発生しないことである．一方，重度の不安全な制御アクションは相互作用における不安全な制御アクションであり，具体的には信号送信の遅れなどが挙げられる．また，軽度の不安全な制御アクションの組み合わせによって重度の不安定な制御アクションが生じることも確認した．

第 4 章
耐故障制御システムアーキテクチャの検討

4.1 概要

この章では MBSE に基づき，MEV の操縦安定性に対する耐故障制御システム(Fault-tolerant Control)のアーキテクチャの検討を行う．従来の耐故障制御はコンポーネントの故障・失陥に対応するために使われている．しかし，MEV のシステムは様々コンポーネントから構成されているため，コンポーネントのみではなくシステム全体を考慮し，安全性を確保する耐故障制御を検討する必要がある．

まず，開発対象である耐故障制御システムのシステムレベルでのユースケースから外部システムとの相互関係性を明確にし，耐故障制御システムの境界，および，コンテキストを定義する．耐故障制御システムと関連するシステムの振る舞いを詳細に分析するため，ユースケース図で明確にしたシステムの各ユースケースをシーケンス図により分析し，システムの機能要求を整理する．その結果得られた情報をもとに機能アーキテクチャを導出する．

4.2 機能要求の明確化

耐故障制御システムのモデルの全体的なパッケージ構造を定義する．図 4.1 は耐故障制御システム編成のパッケージ図を表す．パッケージは，他のモデル要素をグループ化するためのモデル要素である．パッケージ図は，パッケージ間の関係を表現するための図である．エンジニアリング解析パッケージ (Engineering Analysis package)は，性能解析に用いる制約ブロック，またはほかの解析に関するモデルを含んでいる．「安全ビューポイント」（Safety Viewpoint），「性能ビューポイント」（Performance Viewpoint）を用い，耐故障制御システムに対して複数のステークホルダーが関心を持つ視点を表す．耐故障制御システムの「安全ビューポイント」は安全に焦点を当てた側面を強調しているため，要求，振る舞い，ユースケースおよびテストは評価されている要素を，「性能ビューポイント」は，特に性能要求とテストを，それぞれ含んでいる[12].

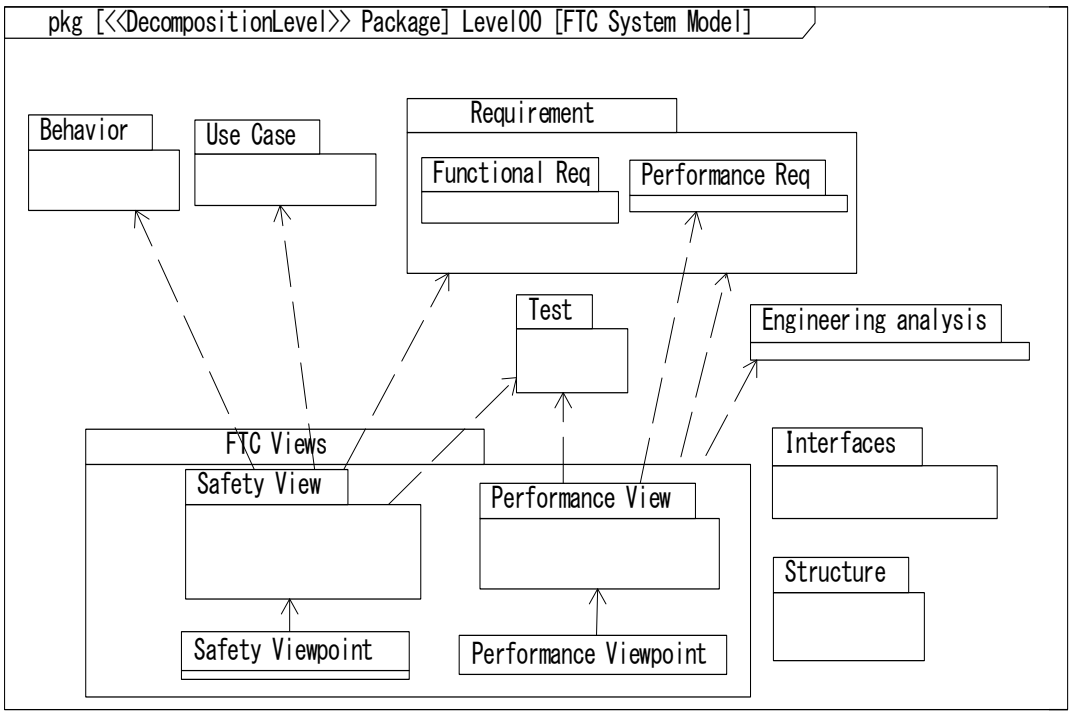


Fig. 4.1 Package diagram of fault-tolerant control system model

図 4.2 は故障許容の要求図を示す．故障許容の要求は，「Fault tolerance components」と「Fault tolerance interfaces」の 2 個の要求の集合として表されている．また，これら 2 個の要求は，それぞれ 3 個ずつの要求の集合として表されている．MEV のコンポーネントで故障が発生した際に，MEV を安全な状態に維持するという要求に関し，アクチュエータ・バッテリー・センサーというコンポーネントを故障時であっても安全な状態に維持するということが要求される．一方，コンポーネント間のインタフェースの故障に関しても，アクチュエータ・バッテリー・センサーに関するインタフェースを安全な状態に維持するということを要求している． MEV に故障が発生した際に，安全性を確保することを検討すると，対象の MEV のドライバは耐故障制御システムから安全な運転支援を受け取る外部システムと考えられる．以下に，MEV に故障が発生することを想定した場合に，耐故障制御システムが実際に働いた場合のユースケースを示す．

1. 走行中，インホイールモータやセンサー等の重大な故障が発生しても，正常時と同等の性能をドライバが享受できる．
2. 故障時に，横風，または，障害物に MEV の走行を阻害されても安定に走行できる．
3. 故障時に，低摩擦の路面があってもスリップせずに安定に走行できる．

図 4.3 は耐故障制御システムのドメインを示す. 外部システムとして「ドライバ」,「車両」,「環境」を定義し，さらに，路面，天気，障害物をアクターとして定義する．

先に挙げた耐故障制御システムのユースケースとドメインの定義を用いて，トップレベルのユースケースを導出して，耐故障制御システムの設計範囲，および，外部システムとの関係性を明確にする．図 4.4 は耐故障制御システムのユースケース図を示す．図 4.4 のように，耐故障制御システムは車両，および，ドライバに対し，MEV の重大な故障を許容する「Tolerate faults」という機能を提供する．「Tolerate faults」は，4 個の機能を含んでいる．これら 5 個の機能のほかに，2 個の機能がある．それぞれの説明は表 4.1 に述べられる．

ドライバ，および，車両は外部システムとして，耐故障制御コントローラと関わっている．本研究では，コンポーネント故障の検知「Detect component's faults」，モータ故の許容「Tolerate motor fault」，および，前輪操舵角の故障の許容「Tolerate front steering angle fault」のみに着目する．

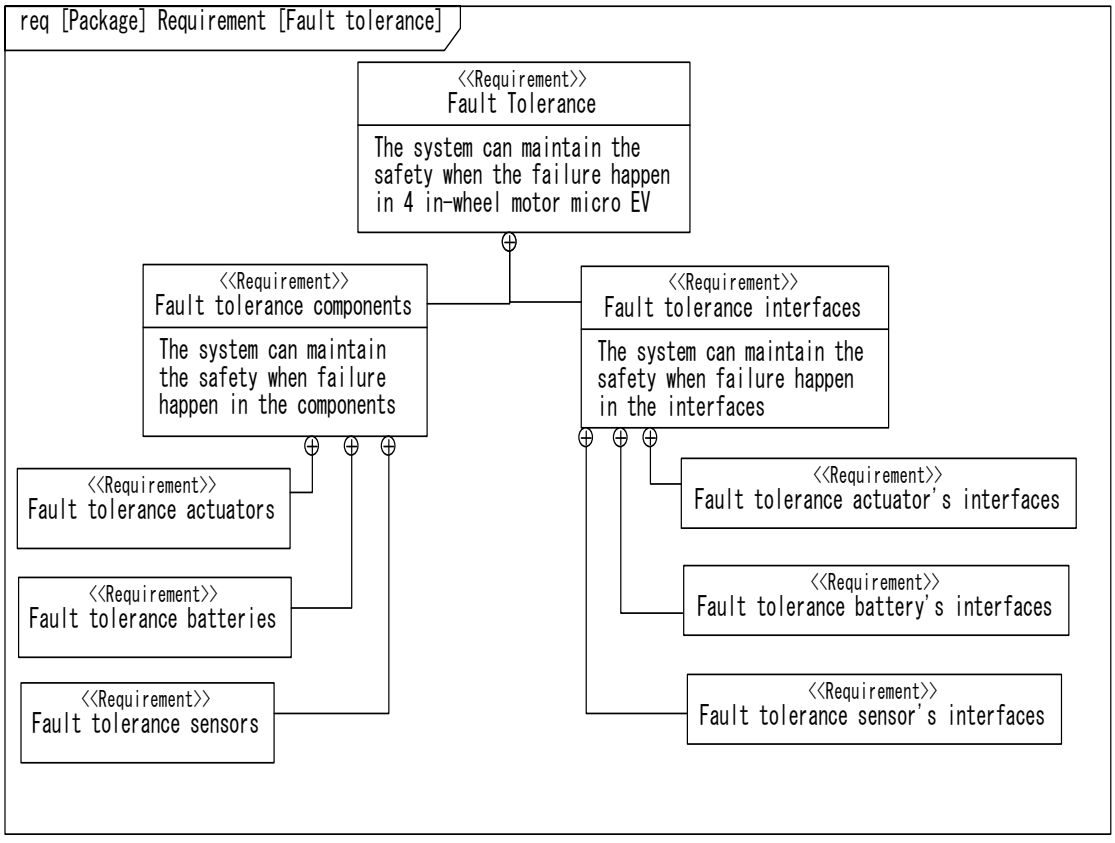


Fig. 4.2 Requirement diagram for the fault tolerance

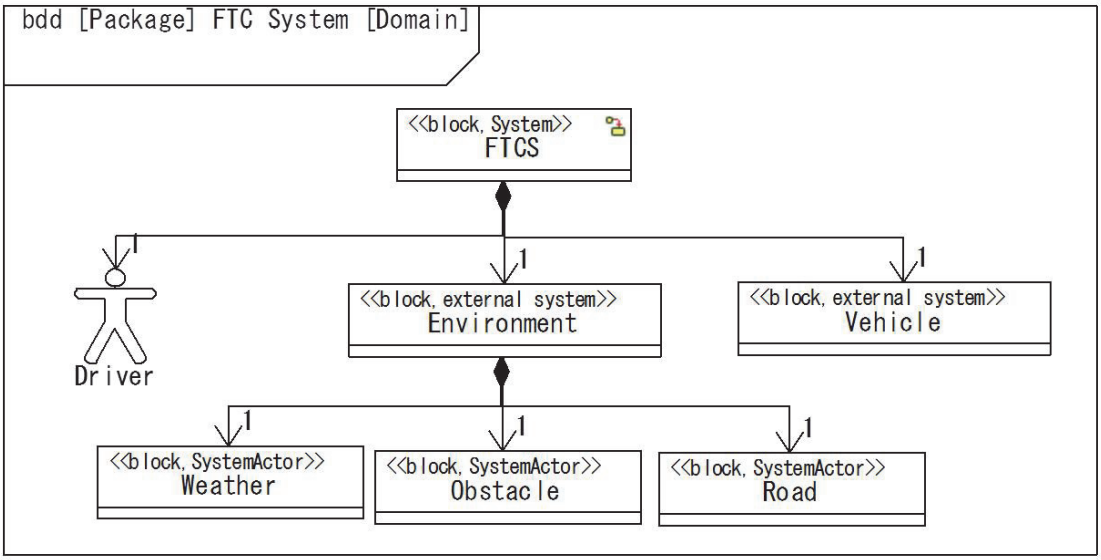


Fig. 4.3 Domain of fault-tolerant control system model

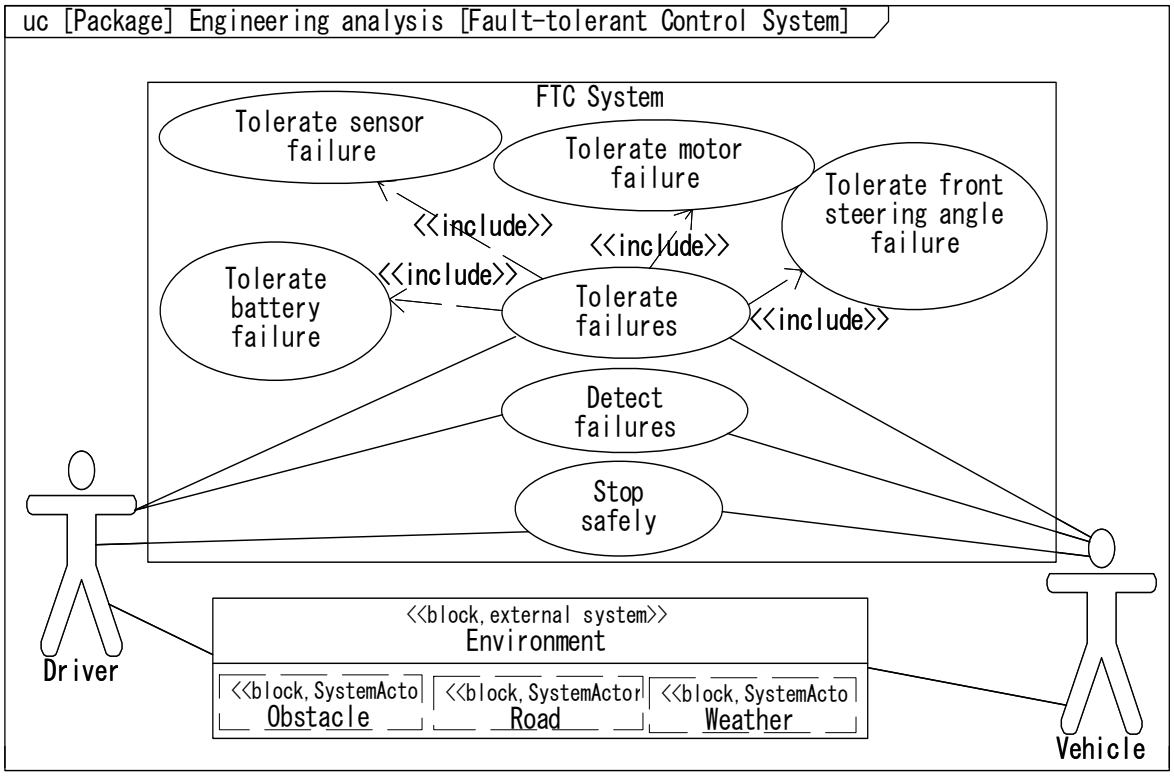


Fig. 4.4 Use case of fault-tolerant control system

Table 4.1 Use Case Explanation

ユースケース名	概要
Tolerate faults	故障を許容する
Detect faults	大事なコンポーネントの故障を検知する
Tolerate battery fault	バッテリの故障にも関わらず，正常に走行する
Tolerate motor fault	モータの故障にも関わらず，正常に走行する
Tolerate front steering angle fault	前輪操舵角の故障にも関わらず，正常に走行する
Tolerate sensor fault	センサーの故障にも関わらず，正常に走行する
Stop safely	重度の故障があると，安全に止まる

故障の許容「Tolerate faults」，は主なユースケースであり，この中にバッテリ故障の許容，モータ故障の許容，前輪操舵角故障の許容，センサー故障の許容が含まれている．「Detect faults」とは大事なコンポーネントの故障を検知するといことである．「Tolerate battery fault」とはバッテリの故障にも関わらず，正常に走行するといことである．「Tolerate motor fault」とはモータの故障にも関わらず，正常に走行するといことである．「Tolerate front steering angle fault」とは前輪操舵角の故障にも関わらず，正常に走行するといことである．「Tolerate sensor fault」とはセンサーの故障にも関わらず，正常に走行するといことである．「Stop safely」とは重度の故障があると，安全に止まるといことである．

以上の 4 つ許容の機能が大事であり，故障があることにも関わらず，車両の動作が正常に継続する必要がある．例えば，「Tolerate motor fault」は MEV に原動機の 4 つのインホイールモータがあり，1，2，あるいは 3 台が故障すると，車両の走行がまだ継続する可能性がある．しかし，この異常の状態で対応するコントローラが必要である．

「Stop safely」，安全の停止は大事な対策であり，他の許容の機能が不可能であれば，安全に停止しなければならない．重度な故障を検知すると，適切な減速度を計算する．可能であれば，徐々に減速し，急に止まることではない．なぜなら，急に止まると周辺の車両に衝突する可能性が高い．

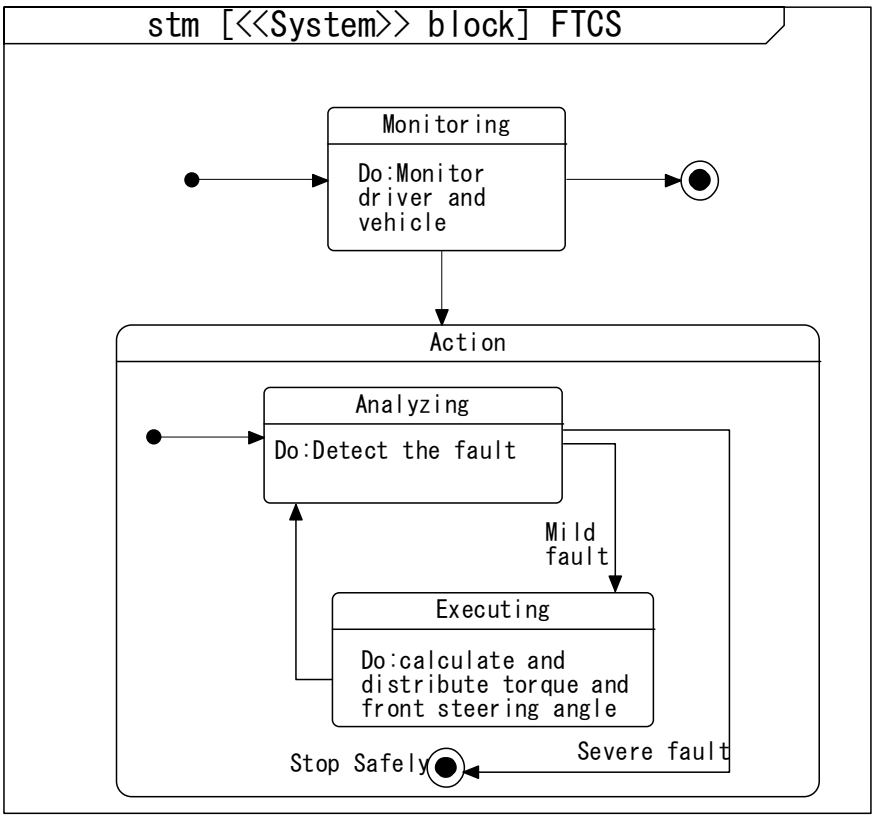


Fig. 4.5 State machine diagram for fault-tolerant control system

図 4.5 は耐故障制御システムのステートマシン図を示す．ステートマシン図は，対象の状態や状態間の遷移を表現する図である．耐故障制御システムの主な状態は 3 個あり，それぞれ監視「Monitoring」，解析「Analysis」，実行「Executing」である．解析の状態から実行，または，完全に停止するという状態に遷移する．不安全な制御アクションとなる危険性が高い「Severe fault」，重度な故障が発生すると，安全な停止に移行し，故障許容ができると実行モードになる．

この安全な停止の機能がシミュレーションで確認した．実施されたシミュレーションは以下の条件で実施した．

- 横風が発生しない．
- 車両速度は一定とし， 16.67 m/s とする．
- ドライバのステアリング指令はシミュレーション時間内で何度か遅れる．
- シミュレーション開始後 3 秒の時点から，前左のインホイールモータへのトルクが発生しなくなる．

VSCS はドライバのステアリング指令の遅れが 0.1 秒~ 0.3 秒の際に，操縦安定性を確保できた．しかし，横風が発生する際に，操縦が不安定になることが予想される．その

ため，事故を防ぐためには，横風が発生した際に車両を安全に停止する必要がある．この不安全な制御アクションを検知したのち，突然停止するのではなく，徐々に減速し停止することが安全性を確保するために重要である．そこで，安全に車両を停止するためのパラメータを検討するために，シミュレーションを以下の条件で行う．

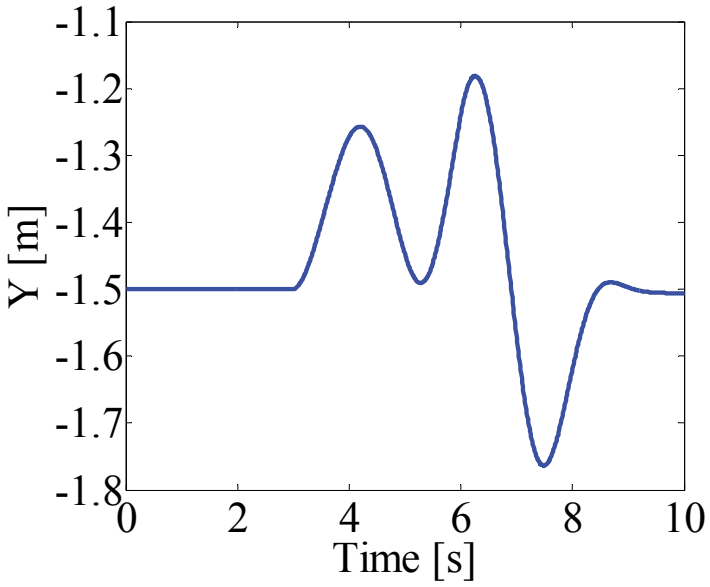
- 20 m/s の横風が発生する．
- ドライバのステアリング指令において，3 秒から 0.3 秒の遅れが生じる．
- シミュレーション開始後 3 秒の時点から，前左のインホイールモータへのトルクが発生しなくなる．
- 車両速度は一定とし, 16.67 m/s とする. 3 秒から減速し, 減速度は約 2.4 m/s^2.
- VSCS を用いない．

図 4.15 はこれらの条件下で行ったシミュレーションの結果を示す．この結果より，このシミュレーション下での車両の横変位は，最大で約 30 cm となることがわかった．走行が始まってから 8 秒，モータの失陥が発生した後 5 秒経過後に，車両が停止する．この結果により，約 30 cm に横変位があるが，まだドライバが許容できると考えられる．そのため，重度な故障があり，および VSCS の対応ができない際に，安全に停止する機能が必要である．重度な故障を検知すると，適切な減速度を計算する．可能であれば，徐々に減速し，急に止まることではないことに設定する必要がある．なぜなら，急に止まると周辺の車両に衝突する可能性が高い．

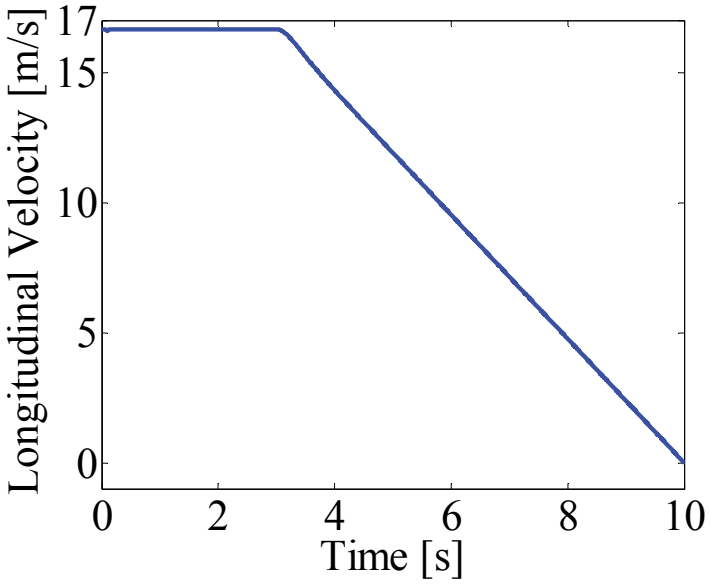
ドライバ，および，周辺車両に対し故障に関する情報をインジケータで伝える．たとえば，ドライバに対しては，ダッシュボードにある画面で故障の情報を伝える．周辺車両に対しては，テールランプを点滅させることで故障の情報を掲示する．

この次はインタフェースの明確必要がある．耐故障制御システムは外部のシステムとどのように相互作用があることを確認する．および，耐故障制御システムの中にも何の要素が構成すればいいかを検討する．

最後に，耐故障制御システムのアーキテクチャに検討する際に，この明確にした機能要求およびインタフェースを用いる．アーキテクチャでは導出した機能要求およびインタフェースがどこの部分に割り当てられるかを調査する．

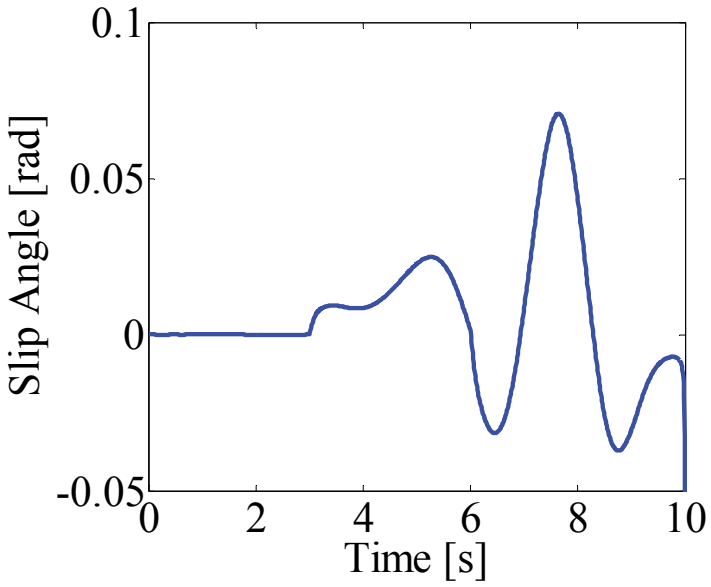


(a) Trajectory

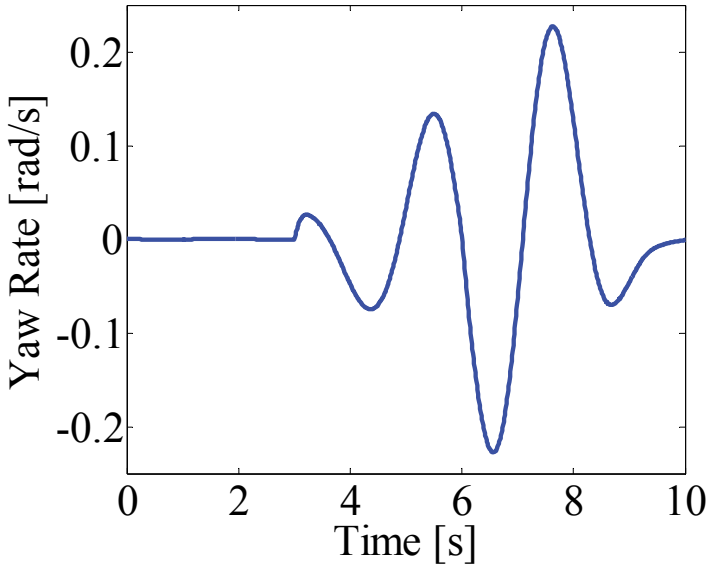


(b) Longitudinal velocity

Fig. 4.6 Simulation result in lateral wind test using MEV model



(c) Slip Angle



(d) Yaw rate

Fig. 4.6 Simulation result in lateral wind test using MEV model

4.3　インタフェースの明確化

機能要求を導出したのち，インタフェースを明確にする必要がある．耐故障制御システムは外部のシステムとどのような相互作用をもつのかを確認する．さらに，耐故障制御システムを構成する要素を検討する．

図 4.7 は FTCS を操作することを表す「Operate FTCS」のシーケンス図を示している．耐故障制御システムのトップレベルにおけるユースケースである「耐故障制御」から，「コンポーネント故障を検知する」,「モータ故障を許容する」,「前輪操舵角の故障を許容する」に着目した際の基本機能を検討するため，メッセージ交換を通した耐故障制御システムと外部システム間の相互作用を表す．FTCS を操作することを表す「Operate FTCS」のユースケースは数多くあるため，すべてをシーケンス図に実現すると，図が複雑になり解析が難しくなる．そのため，シーケンス図上で各ユースケースを参照する形で記述する．そして，着目するユースケースを参照先のシーケンス図で表現する．シーケンス図で振る舞いを表すユースケースはコンポーネント故障の検知「Detect component's faults」，モータ故障の許容「Tolerate motor fault」，前輪操舵角の故障の許容「Tolerate front steering angle fault」，および，安全な停止「Stop safely」のみに着目する．

図 4.7 と図 4.8 のシーケンス図では，耐故障制御システムと外部システムを表現するライフライン，つまり耐故障制御システム「FTCS」，ドライバ「driver」， 車両「vehicle」，障害物「Obstacle」，道路「Road」，天気「Weather」のライフライン間の相互作用を示す．

最後に，耐故障制御システムのアーキテクチャを検討する際に，導出した機能要求，および，インタフェースがシステムのどの構成要素に割り当てられるかを調査する．

図 4.8 は耐故障制御システムが故障を検知することを表す「detect faults」のシーケンス図を示す．ドライバは障害物の存在を認識し，車両は道路，および，天気の外乱を検出する．それぞれ,「Receive obstacle's disturbance」,「Receive road's disturbance」,「Receive weather's disturbance」というメッセージで相互作用を表している．「Monitor driver input」,「Monitor vehicle state」というメッセージは，それぞれ耐故障制御システムがドライバ，および，車両を監視していることを示している．そして，「Analyze the state」は，耐故障制御システムが監視した結果に基づいて，ドライバと車両の状態を解析することを表している．

図 4.9 はモータの故障を許容することを表す「tolerate motor fault」のシーケンス図を示す．モータの故障を検知すると，耐故障制御システムは自らモータの駆動トルクと前輪操舵角の制御を再構成する．そして，再構成された制御モードを車両に送信する．そ

れぞれ「Reconfigure torque and front steering angle control」,「Command chosen control mode」というメッセージで表されている.

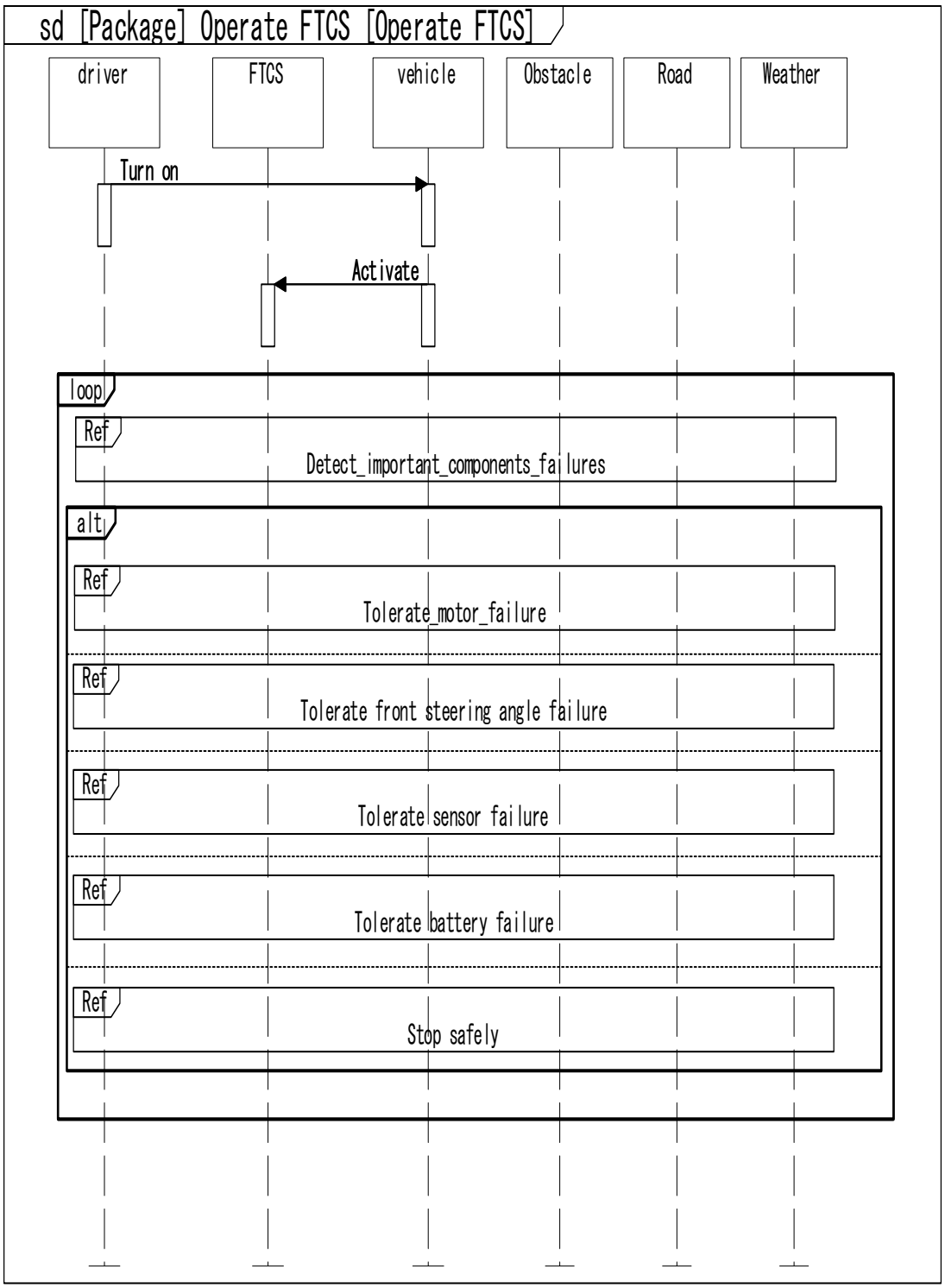


Fig. 4.7 Sequence diagram of fault-tolerant control system in top-level use case

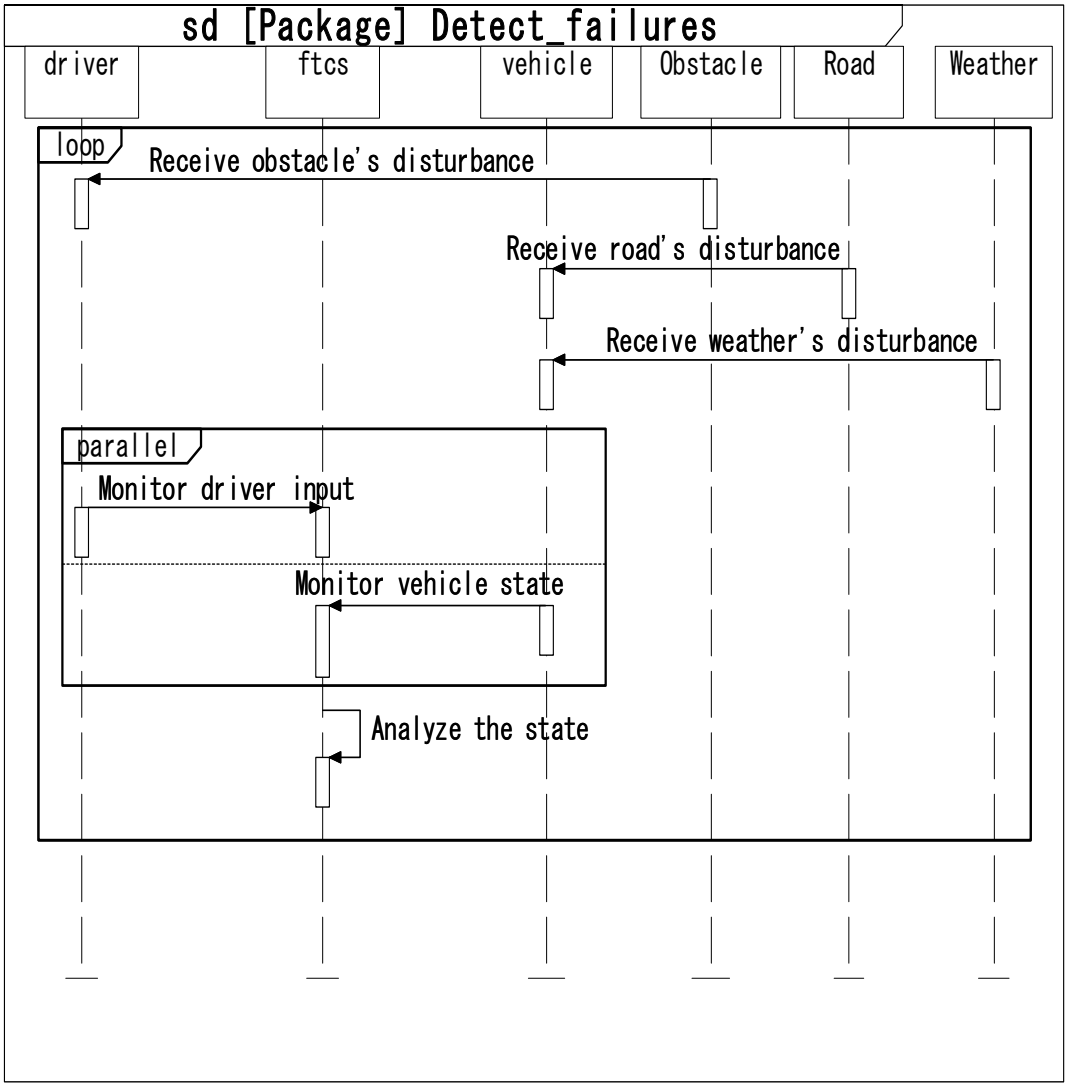


Fig. 4.8 Sequence diagram for the detect faults interaction

図 4.10 は耐故障制御システムを構成するコンポーネントを示す．インジケータ「Indicator」，制御アロケータ「control allocator」，状態オブザーバー「state observer」，VSCS (Vehicle Stability Control System)「車両安定化制御システム」，および，再構築コントローラ「Restructuring Controller」から耐故障制御システムが構成される．

故障の検知「detect faults」のシーケンス図（図 4.8）より，それぞれのメッセージアクションを詳細化する．まず，ドライバの入力を監視する「Monitor driver input」のシーケンス図を示す（図 4.11）．状態オブザーバー「State observer」は，3 種類のドライバ入力を計測する．3 種類のドライバ入力とは，アクセルの計測「Measure accelerator」，ブレーキの計測「Measure brake」，および，ステアリングの計測「Measure steering」である．そして，その結果から速度と前輪操舵角を計算する（Calculate desired speed and direction）．

図 4.12 は車両の状態を監視する「monitor vehicle state」のシーケンス図を示す．状態オブザーバーは，車両から主に 6 個のデータを取得することを表している．これらはトルク「Measure torque」，前輪操舵角「Measure front steering angle」，ヨーレート「Measure yaw rate」，スリップ角「Measure slip angle」，速度「Measure velocity」，および，パワー「Measure power」である．

図 4.13 は状態を解析する「analyze the state」のシーケンス図を示す．状態オブザーバーは，ドライバと車両の計測結果を比較（Compare measurement result from driver and vehicle）して，制御アロケータ（Control allocator）は比較の結果を受け入れ（Receive comparing result），比較の結果をもとに故障の有無を検知する（Detect fault）．故障を検知すると，故障の被害の大きさを決めて，故障の情報をインジケータ（Indicator）に送る．インジケータ（Indicator）はドライバに故障に関する情報を表示する（Show fault info）．

図 4.14 はトルクと前輪操舵角制御を再構成する「reconfigure motor torque and front steering angle control」のシーケンス図を示す．制御アロケータは故障の被害の大きさにより故障モードに対応する制御モードを選ぶ（Select recovering control）．故障の被害の大きさが軽度であれば VSCS を利用する（Control vehicle stability）．その後，VSCS は必要なトルクと前輪操舵角の値を計算する（Calculate motor torque and front steering angle）．計算が完了すると，インホイールモータにトルクの指令（Generate torque），前輪操舵に前輪操舵角の指令（Generate front steering angle）を送る．故障が重度であると，再構築コントローラ（Restructuring Controller）に安全な停止を開始させるための「Start stop safely」のメッセージを送る．次に，再構築コントローラ

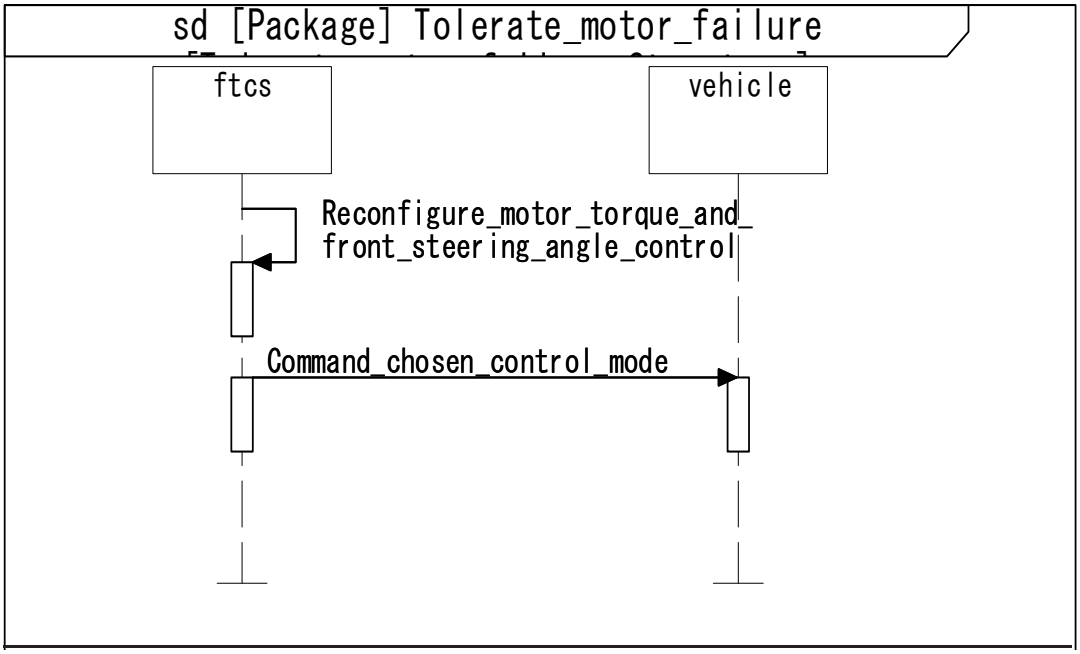


Fig.4.9 Sequence diagram for the tolerate motor fault

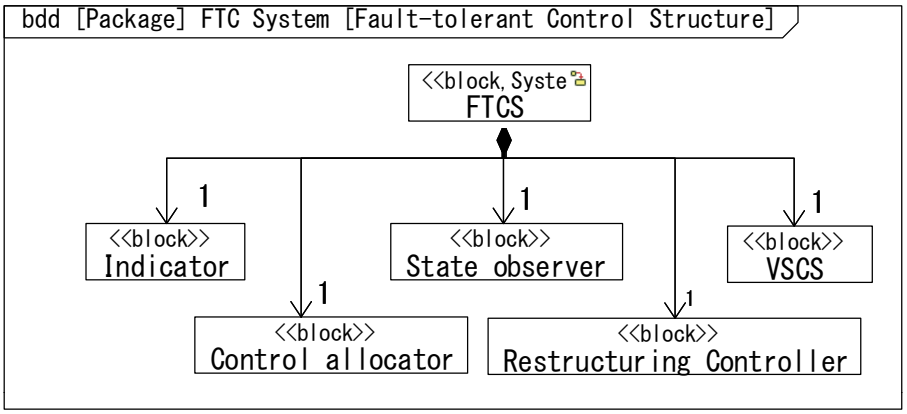


Fig.4.10 Fault-tolerant control system structure

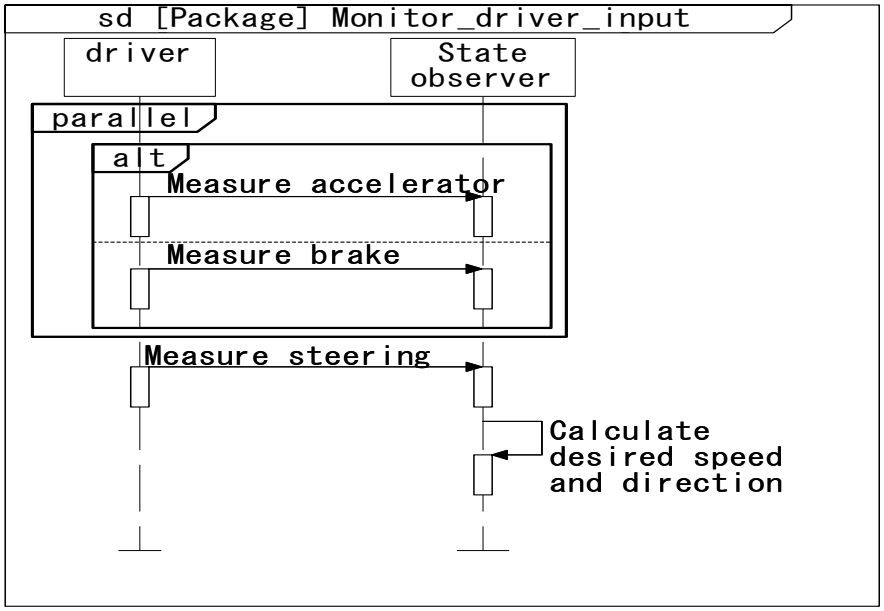


Fig.4.11 Sequence diagram for the monitor driver input

ジを送る．次に，再構築コントローラ（Restructuring Controller）は減速のためのトルクを計算する（Calculate deceleration torque）．そして，減速のためのトルク指令を前輪操舵に送る（Decrease torque）．図 4.15 に示すブロック定義図を用いて，FTCS と外部関連システム，ドライバ，車両，路面，障害物，天気とのインタフェースを明らかにした．太い実線はインタフェースの使用（usage），細い実線はインタフェースの実行（realization）を示す．図 4.16 に示すブロック定義図を用いて，FTCS のコンポーネント間のインタフェースを明らかにした．

これらのシーケンス図を用いることで，システムの構成要素，および，外部要素からのメッセージアクションの順序が明らかになる．また，各シーケンス図を検討することにより，メッセージアクションのインタフェースを明確にした．次の節では明確にした機能要求とインタフェースに基づいて，耐故障制御システムのアーキテクチャの検討について述べる．

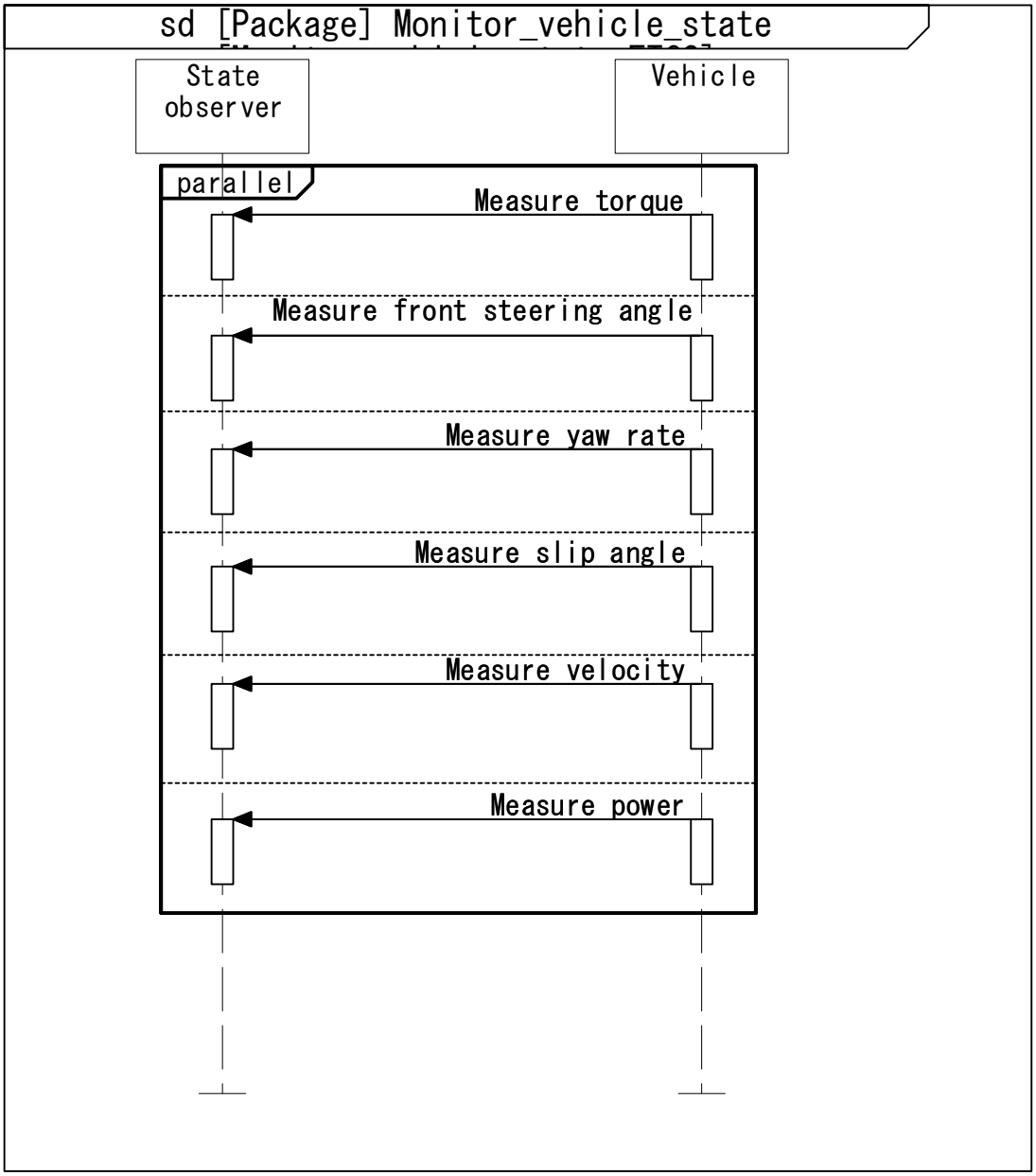


Fig. 4.12 Sequence diagram for the monitor vehicle state

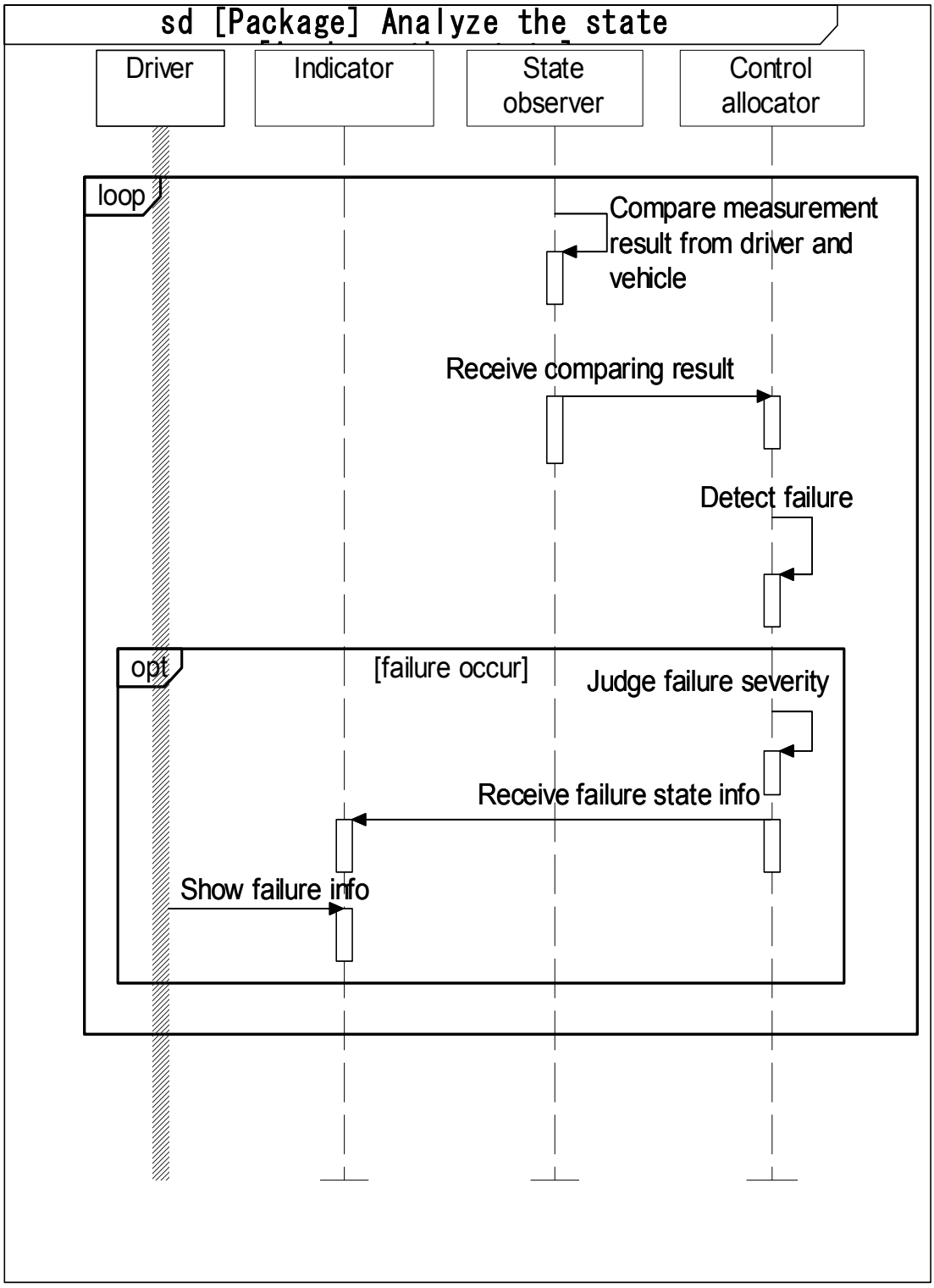


Fig. 4.13 Sequence diagram for the analyze the state

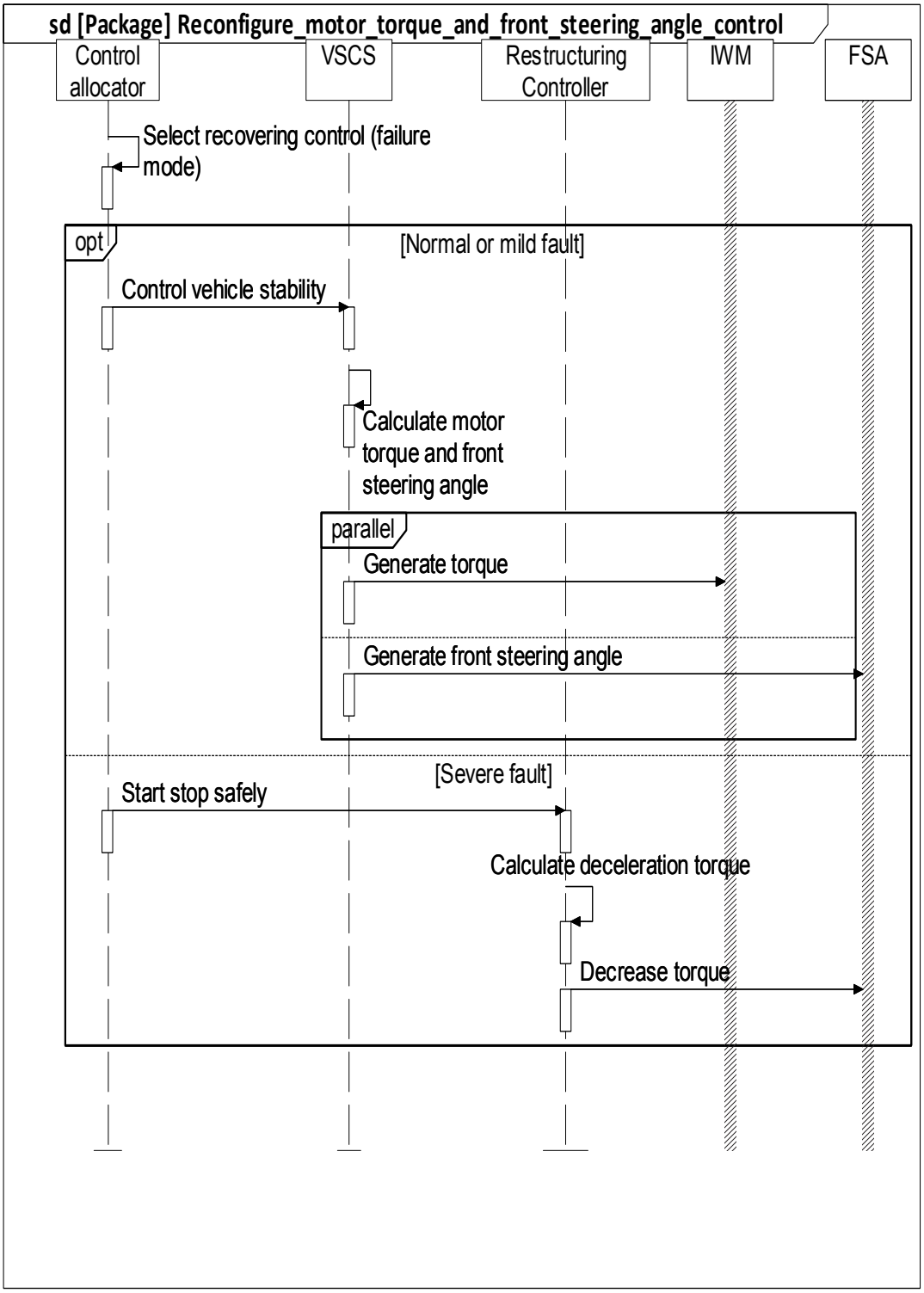


Fig. 4.14 Sequence diagram for the reconfigure motor torque and front steering angle control
(IWM = In-wheel motor; FSA = Front steering angle)

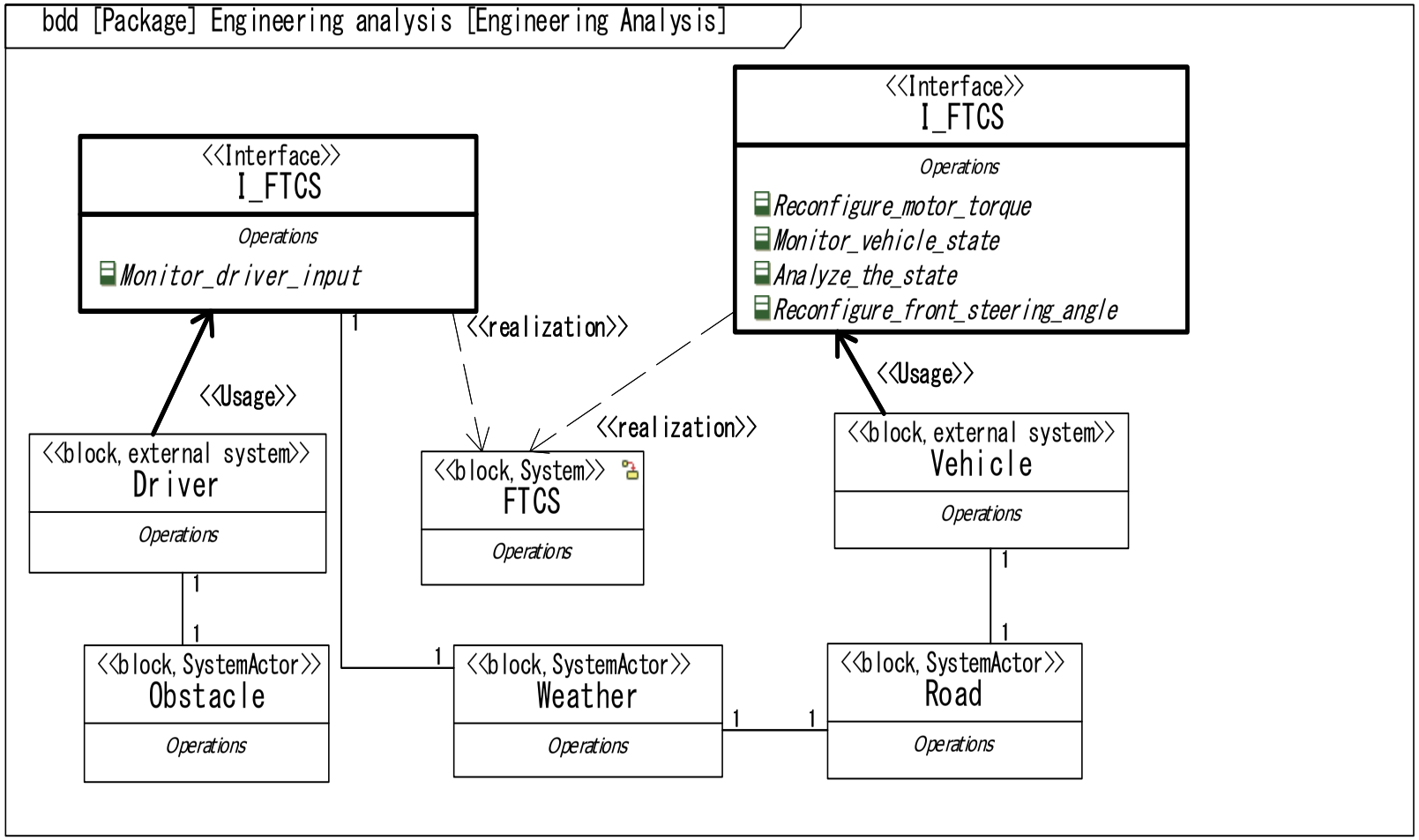


Fig. 4.15 Integration of the fault-tolerant control system with the external system using interfaces at context level

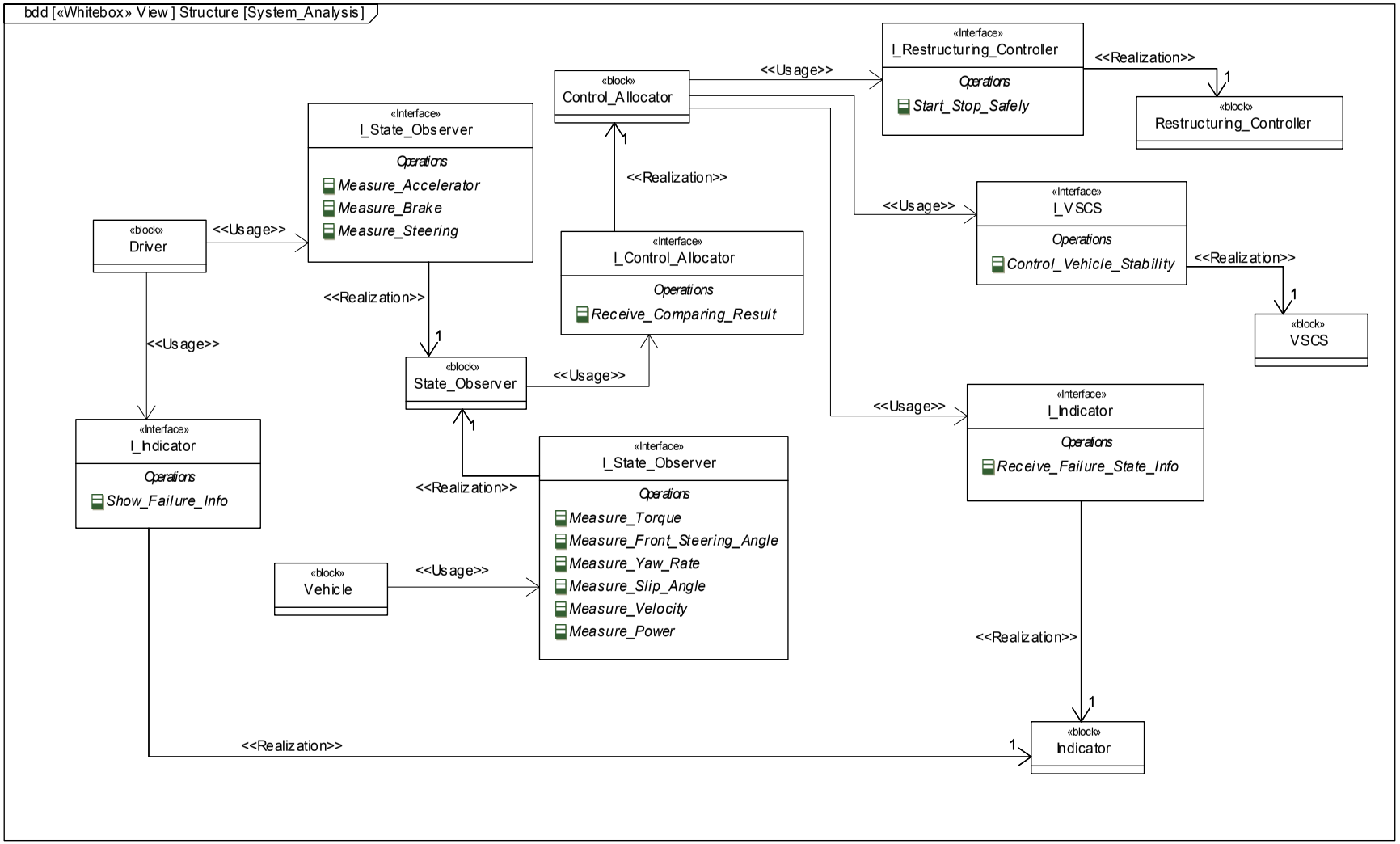


Fig. 4.16 Block definition diagram for FTCS

4.4　アーキテクチャの検討

図 4.17 は MEV のための耐故障制御システムのアクティビティ図である．3 章に述べた被害の大きさに対応する耐故障制御システムが必要である．故障がない時，および，軽度の故障がある時には VSCS で対応が可能である．一方，重度の故障は再構築コントローラ「Restructuring Controller」を用いて対応する．4.2 節に示した機能要求の一つに安全な停止「Stop Safely」が含まれており，再構築コントローラがこの機能を実現する．ステートオブザーバは車両の状態，および，ドライバの入力を計測し，両方の値を比較する．そして，比較の結果を制御アロケータに送る．

制御アロケータはこの結果をもとに故障の被害の大きさを判断する．故障の被害の大きさが軽度であれば，VSCS を用いて車両の操縦安定化制御を始める．VSCS はこの指令を受け入れ，前輪操舵角，および，トルクの制御を実施する．まず，それぞれの制御に必要な故障をしていないモータのトルク，および，前輪操舵角の値を計算する．その後，VSCS が操縦を安定化するために計算したトルク，および，前輪操舵角の値を指令として送信する．

重度の故障を検知すると，制御コントローラは安全に車両を停止すべく制御を開始する．まず，安全に停止するために必要な減速の割合を計算する．計算が終わると，その値に従いトルクの出力を減らす指令を送信する．一方で，ドライバ，および，周辺車両に対し故障に関する情報をインジケータで伝える．たとえば，ドライバに対しては，ダッシュボードにある画面で故障の情報を伝える．周辺車両に対しては，テールランプを点滅させることで故障の情報を掲示する．

先のアクティビティ図では，FTCS の部分が故障の許容「Fault-tolerant」にどのように相互作用するかを説明した．システムの部分は，アクティビティ図におけるアクティビティ区画によって表される．図 4.18 は FTCS の内部ブロック図を示す．この図により，部分がこの機能性を達成するためにどのように相互接続されるかを示し，コンポーネント間のインタフェースを規定するために用いられる．アクティビティ図で表された振る舞いのビューに対して，これはシステムの構造的なビューである．

図 4.19 は耐故障制御システムと MEV の制御構造図を示している．緑色の枠で囲まれた部分は耐故障制御システムを表しており，それには 5 つのコンポーネントが含まれて

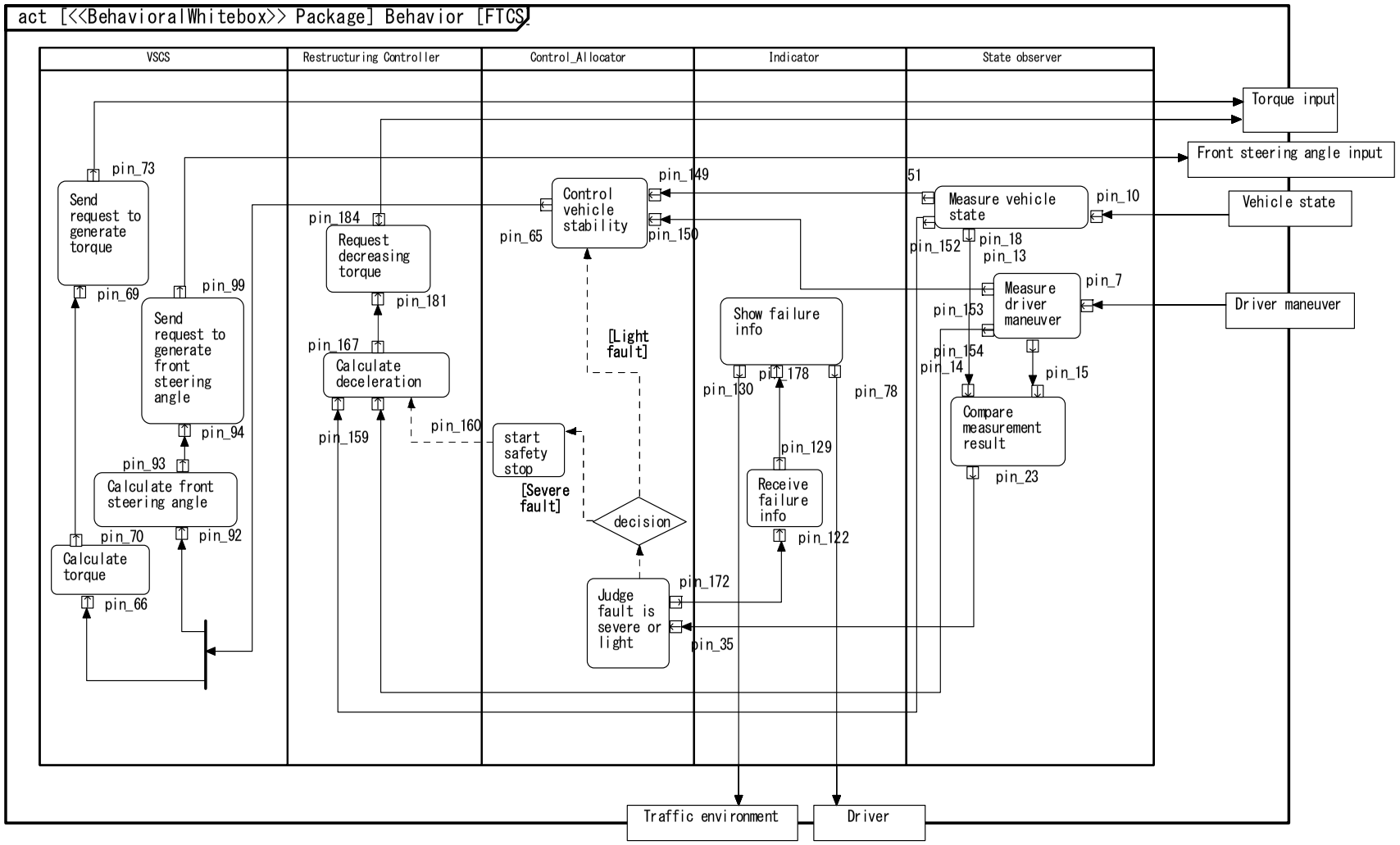


Fig. 4.17 Activity diagram for FTCS

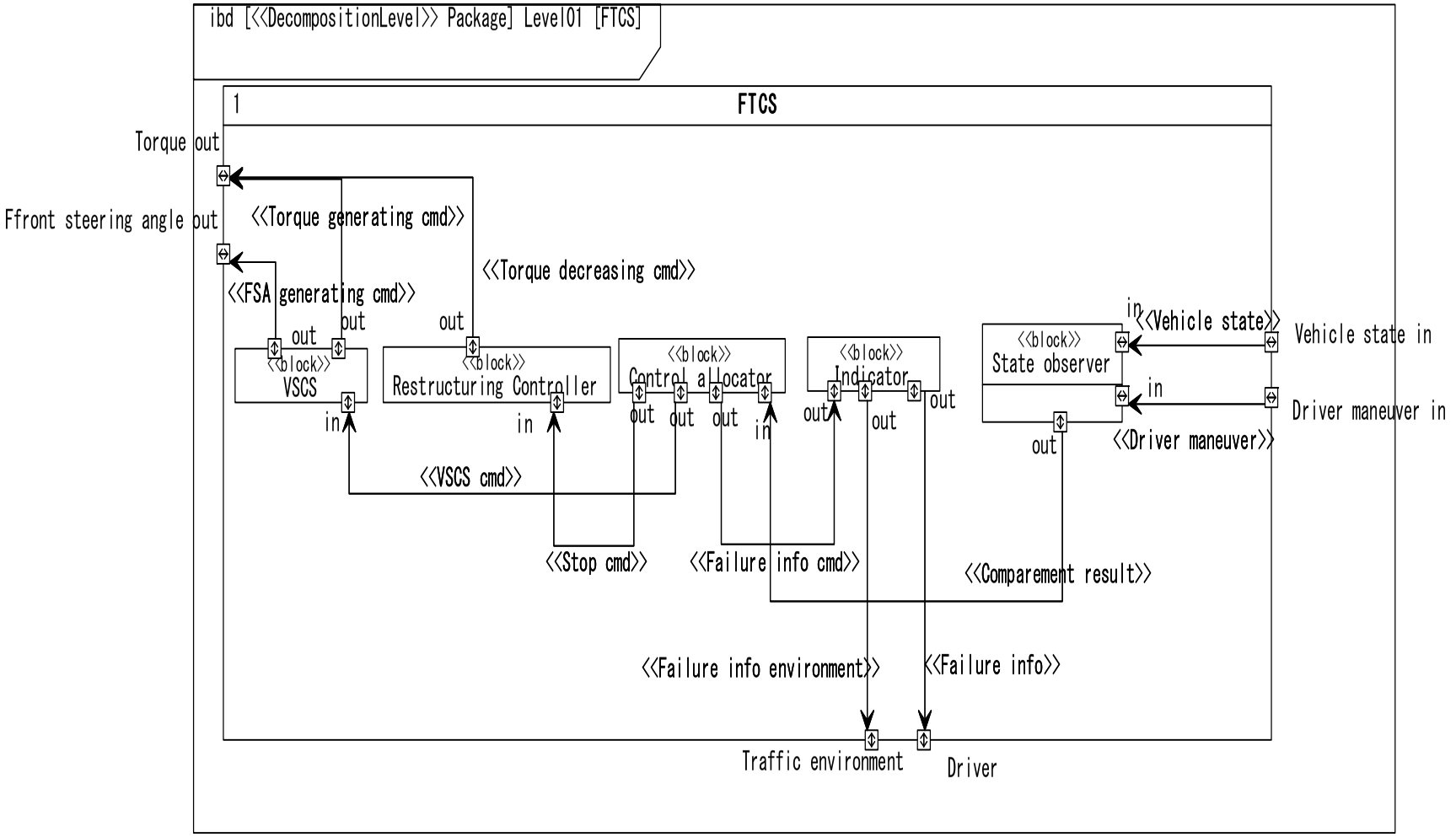


Fig. 4.18 Internal block diagram for FTCS

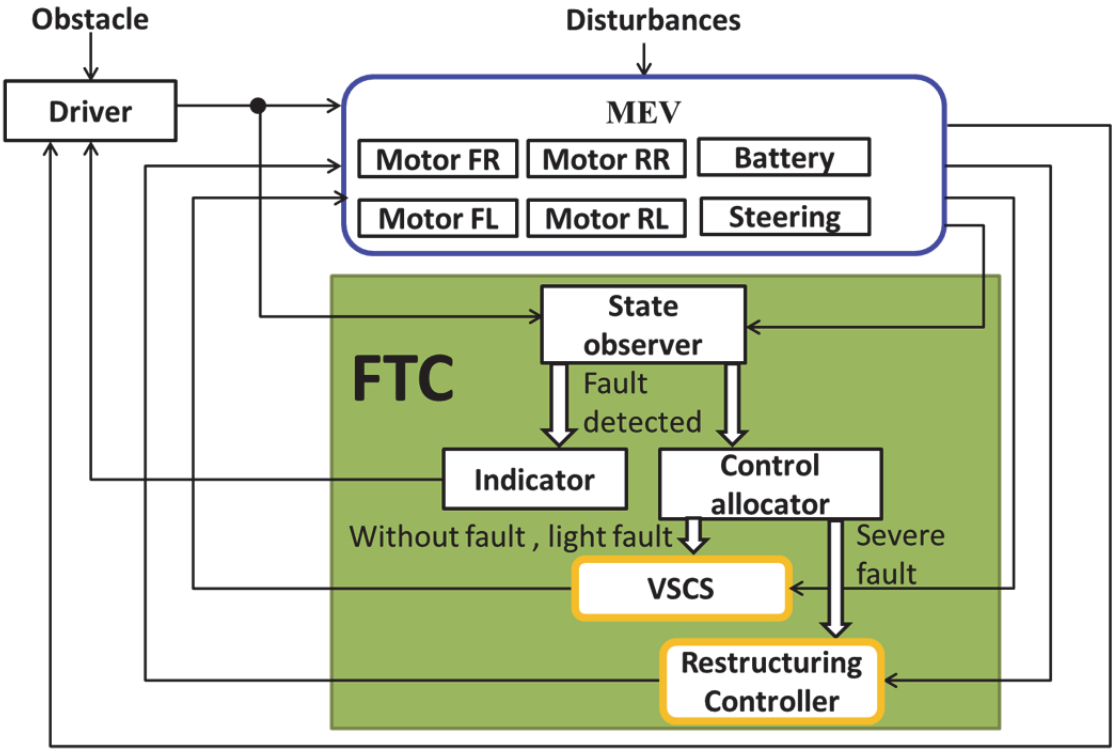


Fig. 4.19 Diagram of control structure of MEV with fault-tolerant control system

いる．故障の被害の大きさにより VSCS と「Restructuring Controller」のどちらのコントローラを動作させるかは，制御アロケータが決定する．

軽度の故障がある時のみでなく，故障が全くない場合にも，VSCS が使用され，再構築コントローラは動作しない．VSCS，および，再構築コントローラは制御アロケータ，および，車両からのデータを受信し，車両の安全性を確保するための動作をする．

現状では重度の故障を想定する際に安全な停止という機能を検討しているが，今後の課題として，重度の故障が発生した場合でも車両の走行を継続できることが期待される．そのためには，新しいコントローラを設計する必要がある．

第 5 章 結論

5.1 結論

本論文では，MEV の交通環境における安全性の確保を目指し，操縦安定化制御システム（VSCS）に関する安全解析を行い，その対策の検討を行った．特に，コンポーネントの故障のみに着目するのではなく，システムの相互作用に着目した安全解析を行い, 不安全な制御アクションを特定した. さらに, 不安全な制御アクションを抑制, あるいは，除去する仕組みを明確にした.

STAMP/STPA のみを用いるのでは，アクションやメッセージなどの順序およびタイミングに関する不安全な制御アクションを網羅できない可能性がある．そのため，アクションの順序，および，タイミングを表すシーケンス図を用いて相互作用を検討した. 検討した相互作用にガイドワードを適用し, 不安全な制御アクションを特定した. そして, 従来の STAMP/STPA でコントロールループ上にガイドワードを適用することで特定した不安全な制御アクションに繋がる潜在的原因を容易に見出すことができた.

特定した不安全な制御アクションを，除去あるいは抑制するために，Dymola 上のシミュレーションを用いて安全制約および被害の大きさのレベルを特定したところ，VSCS が対応できない不安全な制御アクションを確認した．本研究では被害の大きさのレベルを次に示す軽度および重度の 2 つで定義し，不安全な制御アクションでも VSCS によって対応が可能な軽度と, VSCS では対応不可能な不安全な制御アクションを重度とした．シミュレーションを行った結果，軽度の不安全な制御アクションは主にコンポーネントの故障に関連することがわかった．一方，重度の不安全な制御アクションは相互作用における不安全な制御アクションであり, 軽度の不安全な制御アクションの組み合わせによって重度の不安定な制御アクションが生じることを確認した.

さらに，特定した安全制約，および，被害の大きさのレベルに基づいて，MEV の操縦安定性に対する耐故障制御システムの検討を行った．必要な制御システムアーキテクチャの機能要求およびインタフェースを明確にし，MBSE に基づき，耐故障制御システムのアーキテクチャを検討した．また，重度の不安全な制御アクションの場合には，安全停止という機能で対応できることをシミュレーションで確認した．そして，耐故障制御システムは不安全な制御アクションの被害の大きさを特定し，対応するコ

ントローラを選ぶ必要があることを明確にするとともに，VSCS と耐故障制御システムとの関係性を明確にした．

5.2 今後の展望

今後は, MEV の操縦安定性に対する耐故障制御システムのモデルベース設計をさらに推進する必要がある．重度の故障が発生した場合でも車両の走行を継続できることが期待されるため，耐故障制御システムについて，さらに検討する必要がある．また，安全解析に関しては，システムの状態遷移に着目した安全解析手法 SMHA(State Machine hazard Analysis)や SAHSTD(Safety Analysis Method based on Hierarchical State Transition Diagram)を用いた場合との比較ができていない．これらの方法を適用した結果を，本研究で得られた結果と比べることにより，それぞれの安全解析手法の長所を分析し，より高い安全性を実現できる手法を開発できるものと考えられる．

参考文献

参考文献

(1) 超小型モビリティ導入に向けたガイドライン，国土交通省投資局・自動車局

(2) Itoh，Y.，Sakai，K.，Makino，Y.，In-Wheel Motor System，NTN Technical Review，No.79(2011)

(3) ユンソンギル，イルハムドリフィディアント，他，“インホイールモータを搭載した超小型電気自動車のためのシステム同定と H_∞ 制御系設計”，自動車技術会春季学術講演会 2013 年， No.48-13

(4) ユンソンギル，イルハムドリフィディアント，森 崇，西村秀和， “超小型電気自動車の操縦安定化制御システム設計”，第 **13** 回「運動と振動の制御」シンポジウム

(5) Zong，J.，Liu，C.，Zheng，H.，Liu，J.， Fault Tolerant Control Against Actuator Failures of 4WID/4WIS Electric Vehicles， SAE Technical Paper 2013-01-0405，2013

(6) 河上清源，田辺秀敏，神蔵貴久，永廣健太郎，清水浩，吉田博一，"インホイールモータを用いた全輪駆動車におけるモータ失陥時の操縦安定性に関する評価"，日本機械学會論文集. C 編，No.05-0804， (2006) ， pp.2123

(7) Fredrik Asplund, “Safety-Guided Design through System-Theoretic Process Analysis, Benefits and Difficulties”, Technical Report, 2012

(8) Journal of Hazardous Materials, Hazard and operability (HAZOP) analysis. A literature review. Dunjó, Jordi, et al. 1-3, 2009 : Elsevier B.V., 2010, Vol. 173. ISSN: 0304-3894

(9) Nancy G. Leveson， Engineering a Safer World: Systems Thinking Applied to Safety，MIT Press， 2012

(10) Clifton A. Ericson，“Hazard analysis techniques for system safety”，Wiley-Interscience，2005

(11) Geo_rey Biggs， Takeshi Sakamoto， Tetsuo Kotoku， A profile and tool for modelling safety information with design information in SysML， Journal of Software and Systems Modeling manuscript， 2014

(12) 金周慧，松原豊，高田広章，”階層型状態遷移図に着目した安全分析手法”，9th Workshop on Critical Software System，2011

(13) Yichen Fan， Qi Gong， Yuanzhen Zhu， Jianguo Zhang， Safety Analysis for Complex System Based on the Finite State Machine Theory， IEEE， 2011

(14) HyeonJeong Kim， W. Eric Wong， Vidroha Debroy， DooHwan Bae， Bridging the Gap Between Fault Trees and UML State Machine Diagrams for Safety Analysis， Asia

Pacific Software Engineering Conference, 2010

(15) 廣田幸嗣, 足立修一, 小笠原悟司, 出口欣高, 電気自動車制御システム, 東京電気大学出版局, 2009

(16) ユンソンギル, インホイールモータ搭載超小型電気自動車に対する操縦安定化制御システムのモデルベース設計, 慶應義塾大学大学院システムデザイン・マネジメント研究科, 修士論文, 2013

(17) Yutaka Hirano, Development of New Concept Vehicles Using Modelica and Expectation to Modelica from Automotive Industries, Proceedings of the 9th International Modelica Conference (2012), pp.579–588

(18) ユンソンギル, 西村秀和, 村上普太郎, "超小型 4 輪インホイールモータ電気自動車に対する前輪操舵角と駆動/制動トルクを統合した操縦安定化制御システム設計", 自動車技術会春季学術講演会 2014 年

(19) Sanford Friedenthal, Alan Moore, Rick Steiner, A Practical Guide to SysML, The MorganKauffmanOMG Press, 2008

(20) 安部正人, "自動車の運動と制御", 東京電機大学出版局, 2012

(21) 平野豊, "エネルギー消費と動的性能の両立を目指した新モビリティ用車両制御", 日本機械学会とことんわかる自動車のモデリングと制御 2012, pp1-10

(22) 平野豊, "エネルギー消費と動的性能の両立を目指した新モビリティ用車両制御—自動車制御とモデリング：ベンチマーク問題 3—", 自動車技術会学術講演会前刷集, No.146-11, 2011

(23) Kevin Forsberg, Hal Mooz, Howard Cotterman, "Visualizing Project Management, Third Edition", John Wiley & Sons, Inc., 2005

(24) ISO 26262

(25) http://sec.ipa.go.jp/users/seminar/seminar_tokyo_20140121-2.pdf

(26) Liu, J., Zong, C., and Ma, Y., "4WID/4WIS Electric Vehicle Modeling and Simulation of SpecialConditions," SAE Technical Paper 2011-01-2158, 2011

(27) Zong, C., Liu, J., and Zhang, Z., "Stability Integrated Control Algorithm for 4WID4WIS4WIB EV Based in Model Predictive Control," presented at VTI 2012, China, July 16-19, 2012

(28) Sakai, S., Sado, H., and Hori, Y., "Dynamic Driving/Braking Force Distribution in Electric Vehicles with Independently Driven Four Wheels," Electrical Engineering in Japan, Vol.138, No.1, pp.79-89, 2002

(29) Dumont, P.E., Aitouche, A., Merzouki, R. and Bayart, M., "Fault Tolerant Control on an Electric Vehicle," presented at IEEE International Conference on Industrial Technology,

ICIT 2006. pp.2450-2455, Dec. 2006

(30) Wang, R. and Wang J., “Fault-Tolerant Control With Active Fault Diagnosis for Four-Wheel Independently Driven Electric Ground Vehicles,” IEEE Transactions on Vehicular Technology, Vol.60, No.9, pp.4276-4287, Nov. 2011

(31) 坂井信一郎，佐渡秀夫，堀洋一，“4 輪独立駆動電気自動車における動的な制駆動力配分法”，電気学会論文誌 D，120.6 , pp.761-768, 2000

(32) Systems Engineering Handbook, “A Guide for System Life Cycle Process And Activities”, Ver.3.2, International Council on Systems Engineering, 2010

(33) D. Rizal, S. Tani, K. Nishiyama and K. Suzuki,”Dynamic Simulator for Evaluation of Safety Objects in Batch Process”, European Symposium on Computer Aided Process Engineering, 2005

(34) J. A. McDermid1, M. Nicholson, D. J. Pumfrey and P. Fenelon, “Experience with the application of HAZOP to computer-based systems”, Computer Assurance , 1995

(35) Storey, Neil. Safety-Critical Computer Systems. Harlow : Addison Wesley Longman, 1996

謝辞

本研究を行うにあたり，本論文の主査であり，指導教員としてご指導いただきました西村秀和教授に心より深く感謝致します．未熟者の私に対して熱心に勉強面や生活面などあらゆる面で指導して頂きました．本研究をここまで進めることができたのは西村先生のご指導のおかげです．深く御礼申し上げます．本当にありがとうございました．

副査を担当して頂いた，五百木誠准教授には，本論文をまとめるにあたって貴重なご助言を頂きました．ご指導いただき誠にありがとうございました．

ユンソンギルさん，木下聡子さん，三島邦子さんには，多大な助言とサポートを賜りました．サポートしてくれたことはいくら礼をしてもしきれません．本当にありがとうございました．