自動運転に対応した操舵系システムの安全設計*1

Safety Design of Steering Systems for Autonomous Driving

海原信之　N. KAIHARA　木村幸司　K. KIMURA　石原　敦　A. ISHIHARA　中村英夫　H. NAKAMURA

Fail-operational design is the key technology that ensures safety in case of autonomous driving system failure. In order to extract required issues for such fail-operational design, the steering system was developed as an example with reference to ISO 26262. In this activity, required issues and safety design case study for autonomous driving system have been obtained by applying ISO 26262, and the effectiveness of fail-operational design has been evaluated. This report summarizes the results relating to safety design for autonomous driving systems obtained through a project commissioned by the Ministry of Economy, Trade and Industry.

Key Words: autonomous driving, functional safety, ISO 26262, fail-operational, steering system

1．はじめに

現在，CASE（Connected, Autonomous, Shared & services, Electric）に関連する技術開発が加速しているなか，自動車の自動運転実現がもたらす効果の一つとして，交通事故の低減が挙げられる．これは，通常時の運転権限がシステム主体となり，従来人間が引き起こしていたヒューマンエラーなどによる事故の発生が抑制されると期待されているためである．しかし，このシステム（特に電気電子系）が故障した場合，自動運転の継続が困難になるため，新たな事故発生のリスクが懸念される．つまり，自動運転システム故障時に対し，機能を継続することで安全性を確実に担保できる安全設計技術（フェールオペレーショナル）の確立は，自動運転実現に向けた重要な課題である．

経済産業省では，この課題実現に向け，平成 26 年度から平成 27 年度の「次世代高度運転支援システム研究開発・実証プロジェクト」，および平成 28 年度から平成 30 年度までの「高度な自動走行システムの社会実装に向けた研究開発・実証事業」の一施策として，自動運転に対応したフェールオペレーショナルに関する研究を計画した．当社は，経済産業省からこのテーマを受託した一般財団法人日本自動車研究所（JARI）からの委託企業として，自動運転に対応した操舵系システムの安全設計に関する研究開発を行った．本事業は，自動車機能安全国際規格である ISO 26262：2011 を基に，安全設計／検証評価の課題を明確にしたうえで，その課題を実現するための「考え方・方法事例」を示し，「標準化・基準化の論議」や「個々の企業での開発」および「実証事業」におけるバックデータとして活用されることを目的としている．

本報は，経済産業省委託事業で得られた自動運転システムの安全設計に関する成果を述べたものである．

2．自動運転システムの課題と対策

本章では，自動運転の操舵系システムを例題に，ISO 26262：2011 に沿った開発から得られた代表的な安全設計や課題について述べる．まず，本テーマで実施した ISO 26262：2011 の Part. 3 から Part. 6 に関する開発フローを**図 1** に示す．

＊1　本報は，経済産業省受託事業の成果である，平成 26 年度および平成 27 年度の次世代高度運転支援システム研究開発・実証プロジェクト成果報告書，平成 28 年度のスマートモビリティシステム研究開発・実証事業成果報告書，平成 29 年度および平成 30 年度の高度な自動走行システムの社会実装に向けた研究開発・実証事業成果報告書を基に作成した．

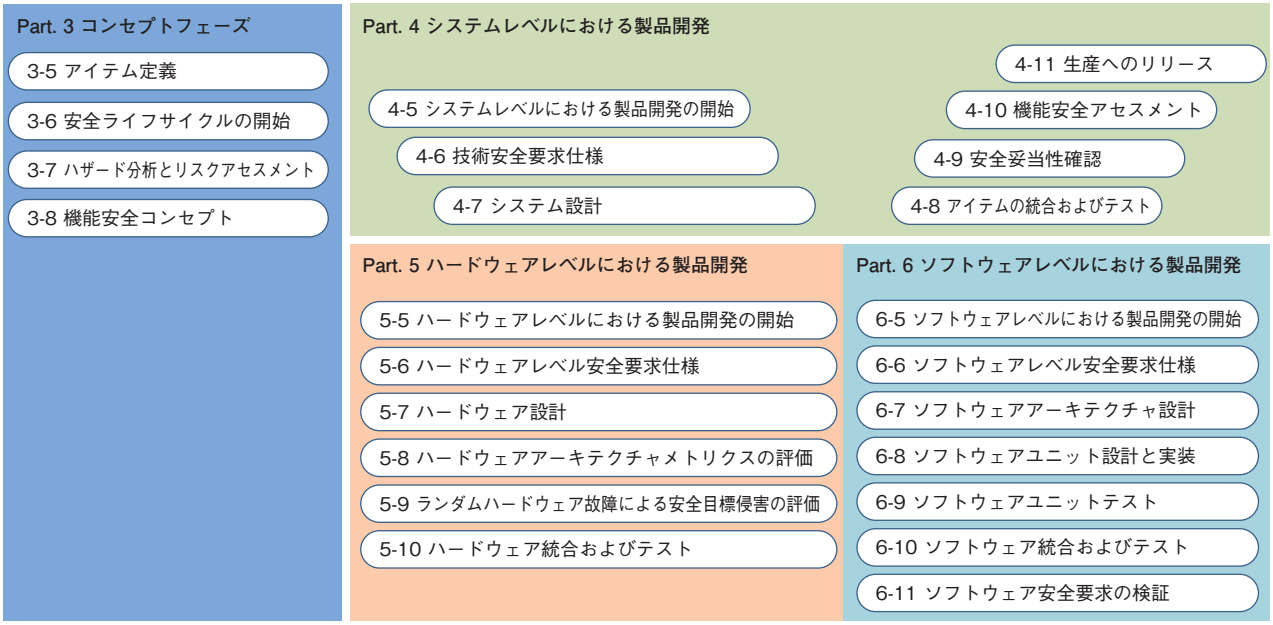


図1　ISO 26262:2011　開発フロー（Part. 3−Part. 6）
Development flow of ISO 26262:2011 (Part. 3-Part. 6)

2.1　フォールトトレラント時間間隔（Fault Tolerant Time Interval：FTTI）の考え方および設定

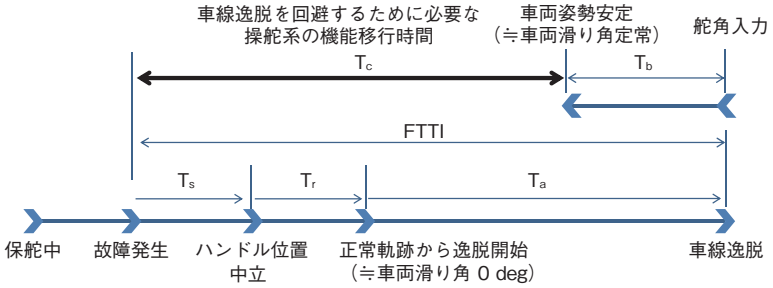
図1の Part. 3 において，自動運転車両の挙動から操舵系システムに求められる安全目標（Safety Goal：SG）を以下のように策定した．

・自動運転において車線逸脱に至る操舵失陥を防止する
・自動運転において車線逸脱に至る不必要な操舵を防止する

ここで示す操舵失陥とは，自動操舵を行うための機能が停止すること，また不必要な操舵とは，あるべき自動操舵に対し必要以上の操舵が行われることなどを表している．これら SG の実現に向け，故障が生じても操舵系機能を継続させるための機能安全要求（Functional Safety Requirement：FSR）および技術安全要求（Technical Safety Requirement：TSR）などを策定する必要がある．策定には，SG を定量的に表すこと，つまり，「自動運転車両に故障が発生したタイミングから車線逸脱までに至る時間（FTTI）」および「機能を継続させるための遵守すべき時間」の算出が重要である．本節では，この課題に対する実施事例として，操舵失陥を例に，その考え方および設定内容を示す．

まず，走行条件を「高速道路での旋回保舵中」とおいた．これは，故障発生による車線逸脱が高速道路で起きた場合，事故によるシビアリティ（危害の程度）が大きくなるという考えに基づいている．また，この時の車両の動きを，「保舵中に故障が発生し，セルフアライニングトルク（Self Aligning Torque：SAT）によりタイヤおよびステアリングが中立位置へ戻り，車両が直進運動に移行して車線逸脱する．」とおいた．これらを踏まえ，**図2**に，故障発生から車線逸脱に至るまでの時間と，そこから推測される車線逸脱を回避するために必要な操舵系の機能継続時間を示す．

図2の T_r は一般的な二輪モデルの車両運動方程式より算出し，T_a は**図3**で示す考え方を基に算出した．なお**図3**は，曲線半径 380m，設計車速 100km/h の高速道路旋回中を例としている．さらに，車線逸脱を回避するために必要な機能継続時間 T_c は，舵角入力から車両姿勢が安定するまでの時間 T_b を FTTI（T_r と T_a の和）から減じ値とした．**表1**に，道路構造令に準拠した高速道路および首都高速道路を想定した走行条件に対し，それぞれの時間を算出した結果を示す．これら各条件のなかで T_c が最も短くなる時間を本テーマにおける安全設計の目標値の一つとして設定した（曲線半径 88m の首都高速道路における T_c = 240ms）．また，算出における走行モデルは，定常円旋回を使用した．このように，操舵系のみならず，自動運転車両に搭載されるシステムの安全設計を行う際は，SG を事前に明確にすることで，SG とひも付いた詳細設計を行うことが可能となる．



T_s ：故障が発生し，SATにより，タイヤ／ハンドルが中央に戻されるまでの時間（机上計算ではゼロ秒と設定）
T_r ：SATにより，タイヤ／ハンドルが中央に戻されてから、車両重心が正常軌跡から逸脱し始めるまでの時間
T_a ：車両重心が正常軌跡から逸脱開始後、車両の一部が白線中央に接するまでの時間
T_b ：舵角を入力後，保舵の状態から，車両姿勢が安定するまでの時間（机上計算では0.5sと設定）

図2　車線逸脱に至るまでの状態
Status of deviation from traffic lane

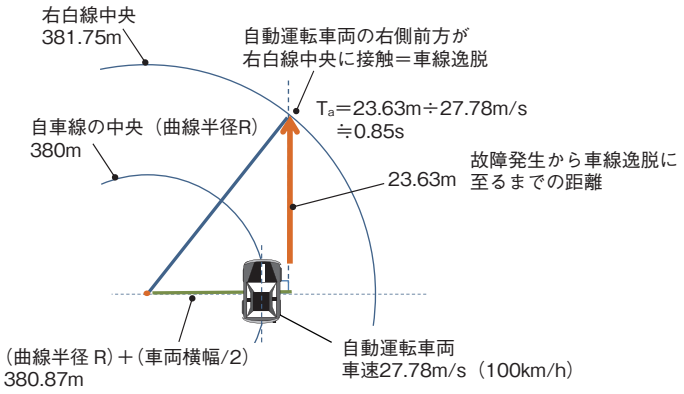


図3　車線逸脱に至るまでの動作
Movement of deviation from traffic lane

表1　車線逸脱に至るまでの時間
Time until deviation from traffic lane

道路条件				操舵角，deg	FTTI（$T_a + T_r$）		T_b，s	T_c，ms
場所	曲線半径，m	設計車速，km/h	幅員，m		T_a，s	T_r，s		
高速道路	380	100	3.50	16.8	0.85	0.14	0.50	490
	230	80	3.50	21.9	0.80	0.11	0.50	410
	88	50	3.25	40.6	0.67	0.07	0.50	240

2.2　演算機能故障時のフェールオペレーショナル

本テーマで策定した操舵系アーキテクチャを**図4**に示す．これは，安全目標（SG）を実現するための車両レベルでの機能安全要求（FSR）を基にしている．たとえば，「操舵角制御機能（主系）の故障を検知する機能を設けること」，「冗長系操舵角制御機能を設け機能を継続すること」などのFSRを，操舵系アーキテクチャの従来機能（Intended Functionality：IF）に対する安全機構（Safety Mechanism：SM）として実装することで，故障発生時のシステム継続を図っている．なお，FSRの内容説明は，本報では割愛する．

図4の操舵系アーキテクチャにおいて，自動運転に対応するための課題事例を以下に示す．前項で述べたとおり，自動運転のシステムに故障が生じた場合，安全性を担保するためには，車両が車線逸脱するまでの間に操舵系の機能を継続させる必要がある（本テーマの場合240ms以内：**表1**参照）．

たとえば，**図4**内の演算機能（メイン）が故障により機能停止した場合，演算機能（サブ）が演算機能（メイ

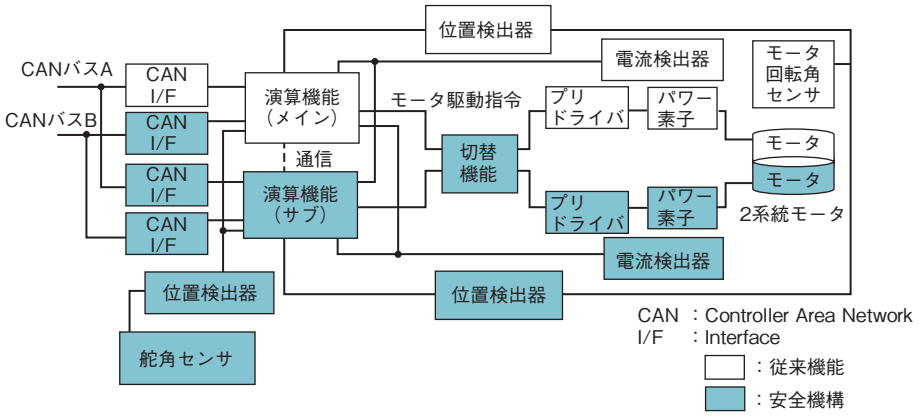


図4　操舵系アーキテクチャ
Steering system architecture

ン）の代わりに制御を行うことで，操舵系の機能が継続し車線逸脱を防ぐことが可能である．しかし，演算機能（サブ）が代わりに制御を行う場合，「車線逸脱後に切り替わる」・「切り替わった瞬間に車両挙動が急変し車線を逸脱」のようなSGの侵害を避けるための方策が必要となる．本テーマにおいて，このSG侵害を防ぐため，正常時における演算機能（サブ）の待機状態をホットスタンバイとした．**図5**に演算機能に実装したホットスタンバイの概念を示す．

図5に示すとおり，演算機能（サブ）は待機中においても，演算機能（メイン）と常に同じタイミングかつ同じ制御パラメータを用いて演算を行っている．つまり，演算機能のメインとサブが常に同じ制御状態であるため，メインからサブへの切り替えを安全かつ高速に行い，車両への影響を最小限に抑えることができる．演算機能の実設計においては，この考え方に基づき，故障検知から切り替え完了までを10ms以下で実現している．このような，演算機能に関するホットスタンバイの考え方は，自動運転システムの中でも，特に駆動モータ制御系や操舵系，および検知・認知・判断系といった，高速な切り替えが求められるシステムにおいては有効である．

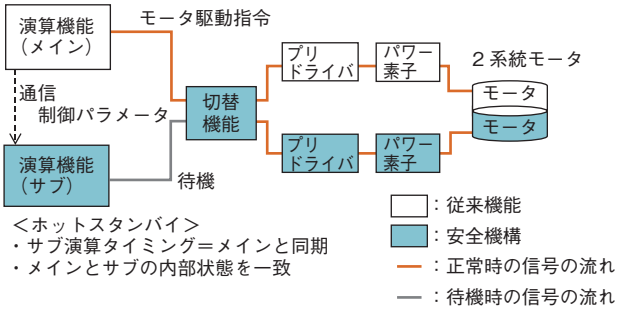


図5　演算機能におけるホットスタンバイの概念図
Concept of hot stand-by for operational function

3. 自動運転システムの課題検証

前章で述べた課題に対し，**図4**に示すような操舵系アーキテクチャを織り込んだ試作品（操舵系試作コントローラ）を作製し，台上やシミュレータおよび実車を用いそれぞれ検証を行った．本章は，ISO 26262-4：2011の8項「アイテム統合とテスト」を参考に実施した．**表2**に本テーマで構築したテスト環境一覧を示す．

3.1　操舵角制御システムベンチ（台上）での検証

ベンチでの検証の目的は，操舵系試作コントローラに織り込んだ安全機構（SM）の実装評価および性能評価である．**表2**で示す操舵角制御システムベンチを用い，操舵系試作コントローラ内の該当の機能へ模擬故障を注入し，故障検知および切り替え処置が設計通りに動作しているかどうかを評価した．評価に必要なテストケースは，ISO 26262-4：2011の8.4.1および8.4.3を参考に作成した．本報では，**2.2節**で述べた課題である，演算機能故障時のフェールオペレーショナルに関し，故障注入方法および確認結果を**図6**，**図7**に一例として示す．

表２　検証環境一覧
List of testing environments

評価環境	評価環境の特徴				
	自動操舵機能	路面負荷	周囲環境	車両運動	運転主権
操舵角制御 システムベンチ	コントローラ ＋モータ	負荷モータ	－	－	－
自動運転シミュレータ	コントローラ ＋モータ	負荷モータ　＋ シナリオ作成ツール	シナリオ 作成ツール	車両運動 シミュレーションツール	システム
実車評価	コントローラ ＋モータ	実路面負荷	実環境	実車	システム

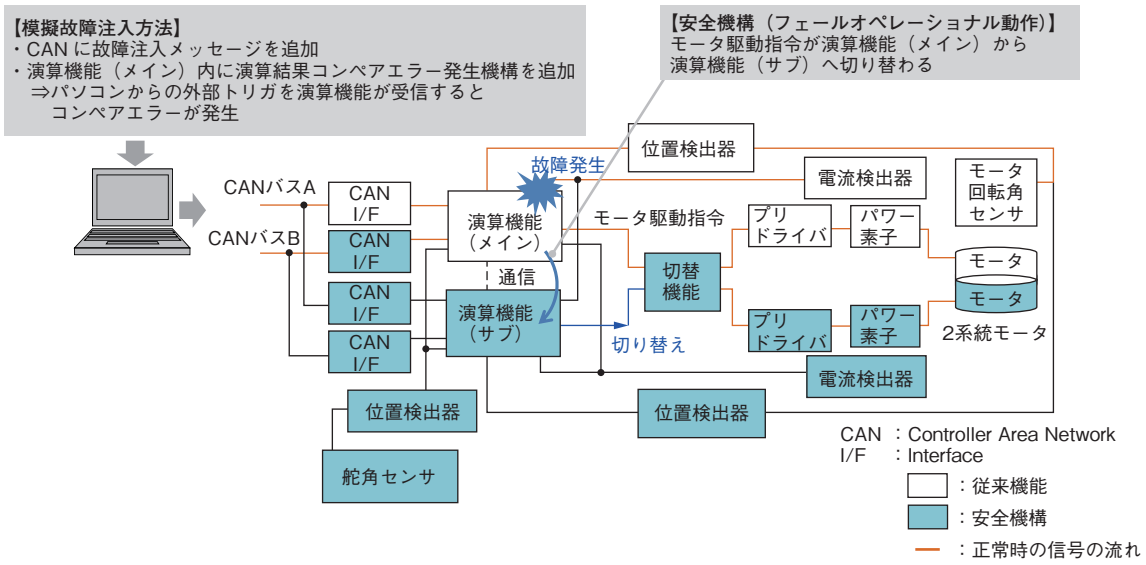


図６　演算機能への故障注入方法
Fault injection method to the operational function

図７より，演算機能（メイン）への模擬故障注入によって，車線逸脱を回避するために必要な機能継続時間 T_c (240ms) 以内に，故障を検知して演算機能（メイン）の出力が停止していること，およびモータへの出力（PWM 信号）が演算機能（サブ）に切り替わっていることが確認できる．これは，各安全要求を基に実装した SM が，意図通りに機能していることを表している．また，本テーマにおいては，演算機能のほか，実装した SM 全てに対してフェールオペレーショナルであることを確認したが，本報では割愛する．

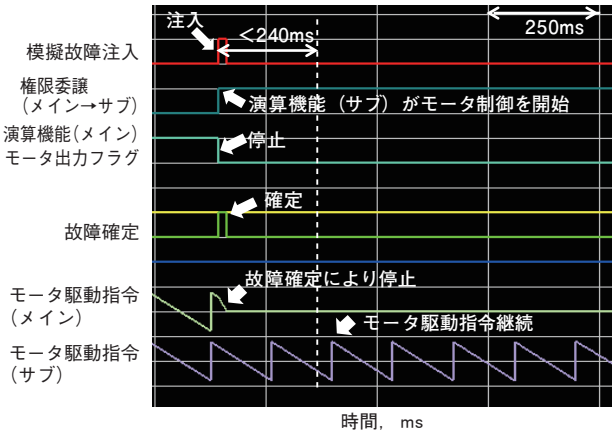


図７　フェールオペレーショナル確認結果
Fail-operational confirmation result

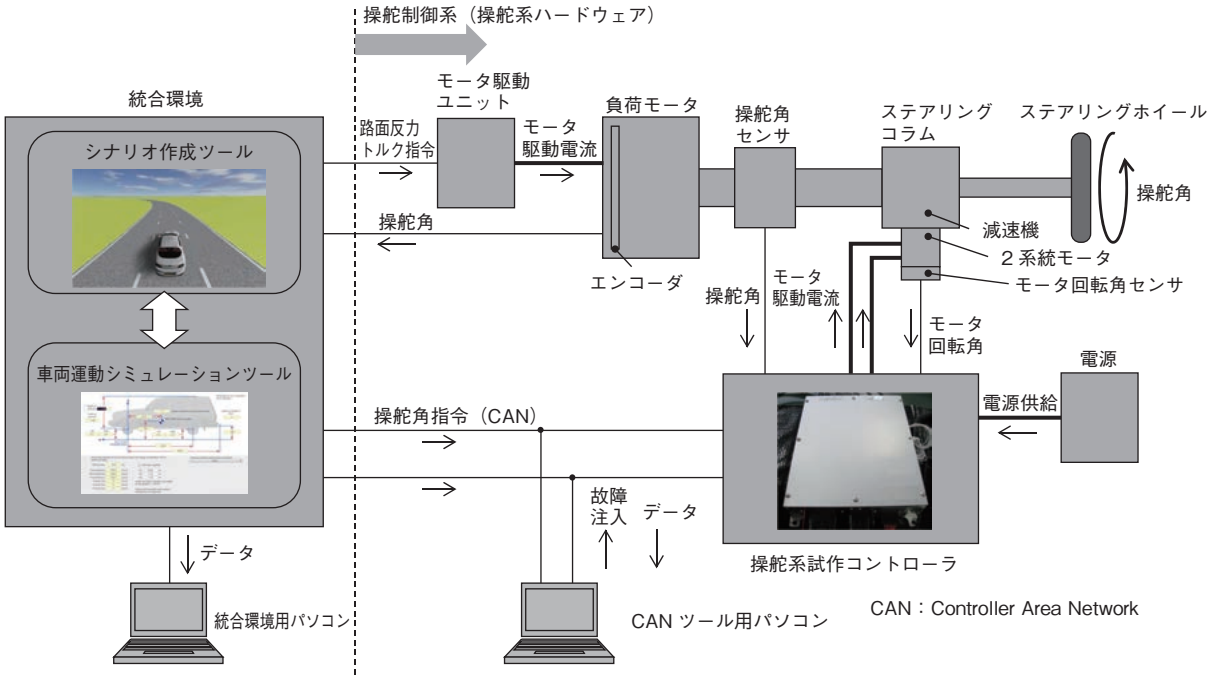


図８　自動運転シミュレータの構成図
Diagram of an autonomous simulator

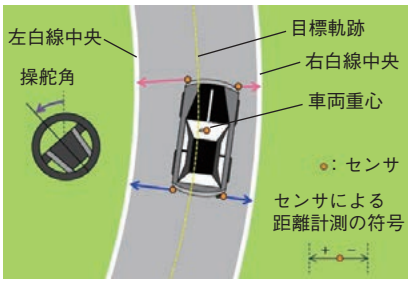


図９　計測センサ取り付け位置
Measurement sensor mounting positions

3.2　自動運転シミュレータでの検証

シミュレータでの検証目的は，**2.1 節**で机上算出した故障発生から車線逸脱までに至る時間（FTTI）の確度確認，およびフェールオペレーショナルを実現するための安全機構（SM）による自動運転車両挙動への影響評価である．これらの詳細は，次項 **3.2.1** および **3.2.2** にて述べる．まず，**図８**に自動運転シミュレータの構成図を示す．

図８より，シナリオ作成ツールは走行シーンの作成および車両挙動の描写を行い，車両運動シミュレーションツールは，与えられた車両制御値と車両諸元，路面状況から車両運動を計算する．統合環境は前述の両ツールの連携，統合環境外部（操舵系ハードウェア）との通信を行い，自動運転の走行を模擬している．

つぎに，自動運転車両の車線逸脱を計測するためのセンシング方法を示す．シナリオ作成ツール内の車両に，前方左・前方右・後方左・後方右・車両重心の計 5 か所にセンサを取り付け，自車線の車線境界線（以下，「白線中央」という）および目標軌跡までの最短距離を計測できる構成とした（**図９**，**10** 参照）．車両右側に取り付けたセンサは，右白線中央までの距離をセンシングし，車両左側に取り付けたセンサは，左白線中央までの距離をセンシングする．センサは対象物（白線中央もしくは目標軌跡）が車両前方に対し，左側にある場合は＋（正）の値，右側にある場合は－（負）の値を出力する．また，操舵角は反時計回りを＋（正）とする．

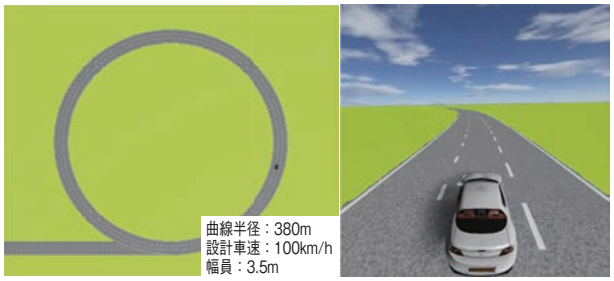


図10　車両挙動確認画面
Vehicle behavior confirmation screen

3.2.1　FTTI の確度検証

本項では，自動運転シミュレータを用い，**2.1 節**で机上算出した故障発生から車線逸脱までに至る時間（FTTI）の確度を確認した結果を述べる．操舵失陥発生時の FTTI は，**2.1 節**で示したとおり，旋回保舵中の模擬故障注入から，車両が白線中央を逸脱するまでの時間を示す．シミュレータによる操舵失陥の発生は，外部から運転停止指令を操舵系コントローラへ送信する構成とした．運転停止指令を受信した操舵系コントローラは，モータへの駆動電流を停止するため，モータトルクの発生が無くなり，その結果，走行中の操舵失陥状態が発生する．この操舵失陥発生方法を用いて，**表3**に示す走行条件に対し机上算出した FTTI の確からしさを確認した．ここでは，**表1**の高速道路での条件に加え，同一モデルで検証可能な一般道路の左折を模擬した条件についても，参考評価として実施した．

2.1 節での机上算出値と，本節のシミュレータ確認結果との比較を**表4**に示す．さらに，その結果の一部を同一プロットしたグラフを**図11** に示す．

表4より，机上算出値とシミュレーション結果を比較すると，FTTI への寄与が高い T_a（自動運転車両が正常な軌跡から逸脱を開始し車体が白線中央と重なるまでの時間：**図2**参照）は，高速道路を想定した走行条件で類似の特性を示していることが確認できる．これは，T_a が直進走行を仮定した車両の静的な挙動を表しており，簡易的な車両運動方程式での算出が可能である．また，一般道に比べて，曲線半径が大きい高速道路では，円曲線部走行中，保舵状態での操舵角が小さく，SAT により操舵角が中立付近まで戻る時間が短いことも，T_a に相関が現れた一因である．

一方，**図11** に示す，曲線半径 15m の一般道を想定した自動運転シミュレータでの結果は，操舵角が中立付近に戻る前に自動運転車両が自車線を逸脱している．従って，低速時のような操舵失陥前の操舵角が大きい条件

表3　自動運転の走行条件（FTTI 検証）
Autonomous driving conditions (FTTI confirmation)

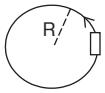
道路条件				参考	走行モデル
場所	曲線半径，m	設計車速，km/h	幅員，m		
高速道路	380	100	3.50	道路構造令	
	230	80	3.50	道路構造令	
	88	50	3.25	首都高参宮橋	
一般道	15	20	3.50	道路構造令	

表4　FTTI 比較結果
FTTI comparison results

道路条件				操舵角，°	FTTI 算出結果			
場所	曲線半径，m	設計車速，km/h	幅員，m		環境	FTTI，s	T_a，s	T_r，s
高速道路	380	100	3.50	16.80	机上	0.99	0.85	0.14
					シミュレータ	1.08	0.85	0.23
	230	80	3.50	21.90	机上	0.91	0.80	0.11
					シミュレータ	1.06	0.85	0.21
	88	50	3.25	40.60	机上	0.74	0.67	0.07
					シミュレータ	1.03	0.74	0.29
一般道	15	20	3.50	185.40	机上	0.59	0.56	0.03
					シミュレータ	1.23	0.99	0.24

机上：机上算出結果
シミュレータ：自動運転シミュレータ結果

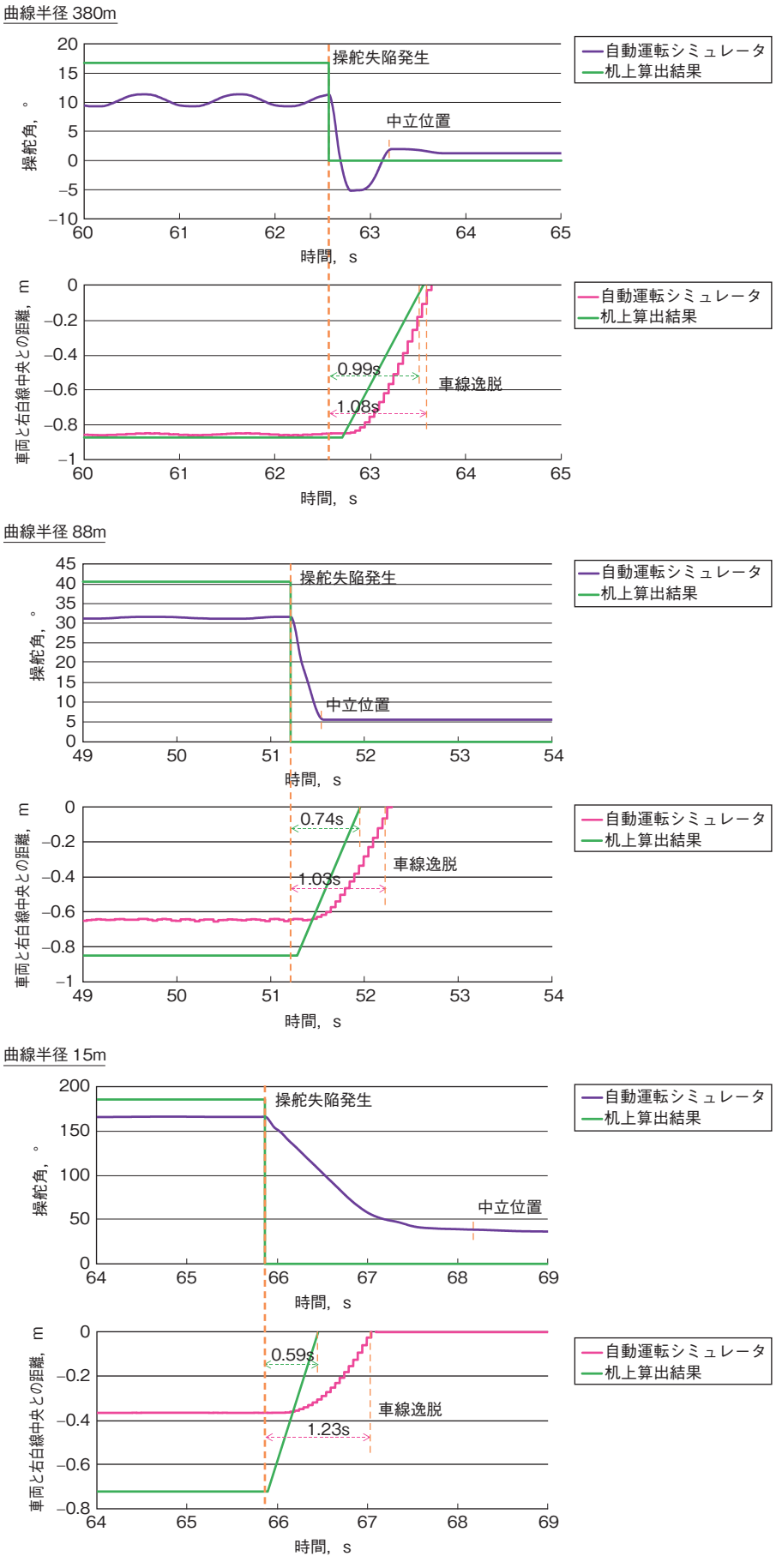


図11　FTTI 比較図（抜粋）
FTTI comparison diagram (excerpt)

においては，机上算出条件でゼロ秒と置いた区間（保舵状態からセルフアライニングトルク（SAT）により操舵角が中立位置に移行する時間）を加味する必要がある．また，車速が低く，操舵角が大きくなるにつれ，机上算出結果と自動運転シミュレータ結果の FTTI の差が大きくなることがわかる．

以上の結果から，高速道路を想定した条件では，簡易式を用いた机上算出でも FTTI が参考値となりうるが，一般道を想定した低速域へ走行条件を広げる場合は，シミュレータを活用した確認も必要となる．

3.2.2　フェールオペレーショナルによる自動運転車両挙動への影響確認

本項では，自動運転シミュレータを活用し，模擬故障の注入によるフェールオペレーショナル動作から，自動運転車両の姿勢が安定するまでの間の，安全目標（SG）の侵害（車線逸脱）有無の検証結果を述べる．検証を行う走行シーンは，**3.2.1 項**の**表 3** と同様の条件を選定し，各シーンでの旋回中に模擬故障を注入した．その確認結果の一部を**図 12** に示す．模擬故障は，演算機能（メイン）への注入とし，そのほかの注入結果については割愛する．

図 12 より，演算機能故障によるフェールオペレーショナル時の車両挙動は，模擬故障注入前後での走行軌跡（車両の各四隅と白線中央との最短距離）の変動がなく車線逸脱には至っていないことが確認できる．これは，**3.1 節**での操舵角制御システムベンチによる検証結果同様，演算機能（メイン）から演算機能（サブ）への機能移行は 10ms 以下で完了するため，車両挙動には影響していないと考えられる．

このように，シミュレータを活用することで，自動運転の走行シーンを容易に模擬でき，あわせて故障が発生した際のフェールオペレーショナルおよび自動運転車両の挙動などを，リスクが高くシビアな条件においても再現性良く確認できる．今後，自動運転の開発がさらに加速していく中で，本章で示したような課題検証の事例は，有益なものになっていくと考える．

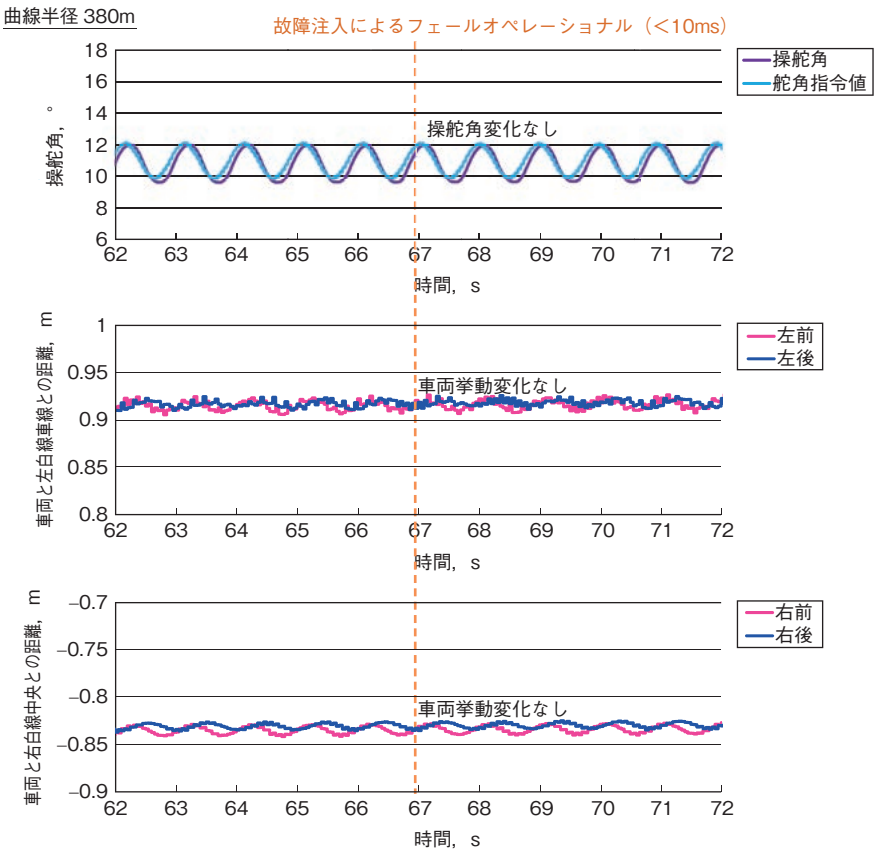


図 12　フェールオペレーショナルによる車両挙動確認結果
Results of confirming vehicle behavior through fail-operational

3.3　実車での検証

実車での検証は，ISO 26262 V 字モデルの最終確認という位置付けで実施した．これは，各節で述べた机上算出結果や自動運転シミュレータ検証結果との比較を行うことで，それぞれの検証方法の有効性を確認することを目的としている．

実車に搭載した自動運転システムは，リアルタイム OS（Operating System）をベースとしたオープンソースの自動運転制御ソフトウェアを活用し，自車位置を把握するための周辺環境認識機器に LiDAR（Light Detection and Ranging）を搭載した．さらに操舵系システムは，フェールオペレーショナルを実装した操舵系試作コントローラおよびモータを含むコラムタイプ電動パワーステアリングを搭載した．**図13** に，検証に用いた自動運転車両を示す．

自動運転車両と白線中央との距離計測は，3 次元地図を用いて，**図9** と同様のセンシングを行い，また走行条件を**表3**の一般道と同様にすることで，シミュレーション結果との比較条件を合わせた．**図14** に，演算機能（メイン）に模擬故障を注入した際の実車挙動確認結果を示し，**図15** に，故障発生から車線逸脱までに至る時間（FTTI）に対する机上算出値・自動運転シミュレータ値・実車計測値の比較結果を示す．

図14 では，演算機能（メイン）故障によるフェールオペレーショナル時の車両挙動は，模擬故障注入前後での走行軌跡に変動がなく車線逸脱には至っていない．これは，**3.2.2 項**の自動運転シミュレータでの検証結果とほぼ一致しており，演算機能（メイン）から演算機能（サブ）への機能移行が，実車でも同様に 10ms 以下で行われており，車両挙動に影響を及ぼしていない．

図15 の (a) は操舵角指令値と操舵角，(b) は車両の前方右と右白線中央の距離，(c) は車両の重心と目標軌跡との距離の比較結果である．なお，操舵失陥が発生した時刻がゼロ秒となるようグラフの時間軸（x 軸）を合わせている．

図15(b) において，操舵失陥発生から車線逸脱までの時間 FTTI は，実車評価と自動運転シミュレータの結果が近い値を示している．しかし，操舵失陥前のゼロ秒以前のデータを見ると，車両の前方右と右白線中央の距離が評価環境によりそれぞれ異なる．これは，円曲線部走行中の車両滑り角が異なっているためであり，精度向上を行う場合は，自動運転シミュレータ側のパラメータの合わせこみを行う必要がある．

図13　自動運転車両
Actual vehicle for autonomous driving

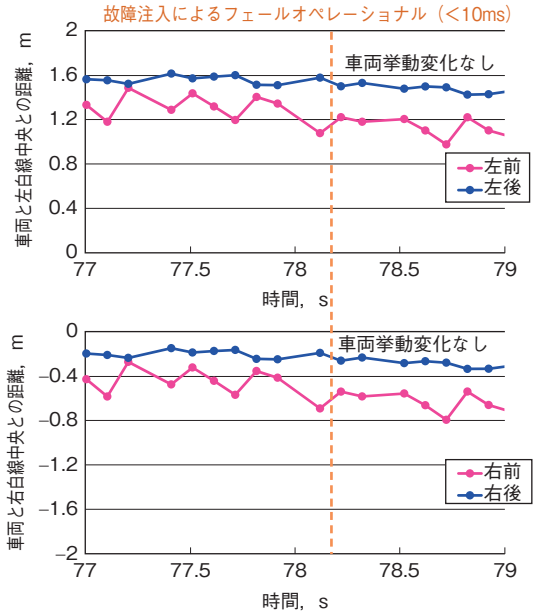
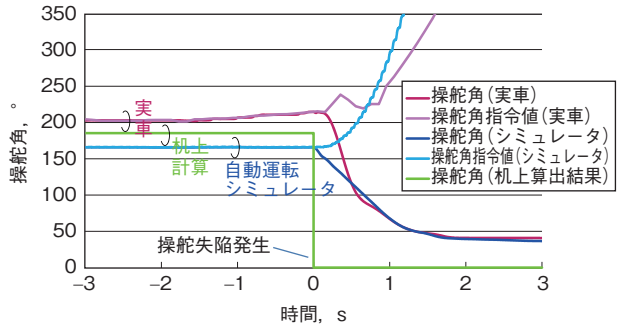
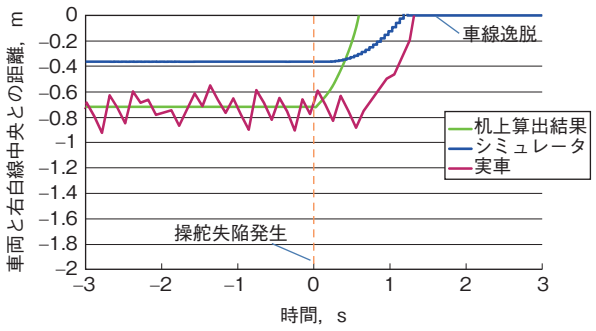


図14　フェールオペレーショナルによる車両挙動確認結果（実車評価）
Results of confirming vehicle behavior through fail-operational (Actual vehicle evaluation)

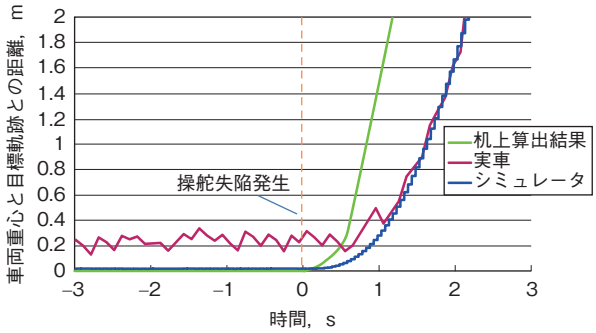
また，**図15**(c) は，**図15**(b) に対し，車両滑り角の影響を除いた場合の車両挙動を表している．**図15**(c) より，実車では，操舵失陥前の車両重心と目標軌跡との距離が一致しておらず，改善の余地があるものの，操舵失陥発生後の車両挙動は，自動運転シミュレータでの車両挙動と同じ特性を示している．つまり，車両の軌跡は，シミュレータと実車において，同様の特性を得ることが可能である．従って，シミュレータと実車を活用する際は，検証する用途に合わせて使い分けることが望ましい．机上算出結果とシミュレーション結果との比較は，**3.2 節**を参照してほしい．



(a) 操舵角指令値と操舵角



(b) 車両の前方右と右白線中央との距離



(c) 車両重心と目標軌跡との距離

図15　評価環境による差異（FTTI結果）
Difference due to evaluation environments (FTTI results)

4. おわりに

本報では，経済産業省からの受託事業に関する成果事例について述べた．**第2章**では，操舵系システムを例題に，ISO 26262：2011 から抽出された自動運転システムに関する安全設計や課題の中から，安全機構（SM）を検討するために必要な要求である故障発生から車線逸脱までに至る時間（FTTI）の考え方，および机上算出値について述べた．さらに，演算機能故障時における安全な切り替え方法（ホットスタンバイ）について一事例を示した．また，**第3章**では，自動運転システムに対する課題に対し，台上・自動運転シミュレータ・実車，それぞれ検証環境を構築し，安全設計確認および各検証方法の有効性を確認することができた．

これら成果は，経済産業省を通じ一般公開されており，今後自動運転の技術開発に着手する個々の企業および実証事業に対し，有益なバックデータとなれば幸いである．

5. 謝辞

本研究成果は，平成 26 年度および平成 27 年度の「次世代高度運転支援システム研究開発・実証プロジェクト」，平成 28 年度の「スマートモビリティシステム研究開発・実証事業」，平成 29 年度および平成 30 年度の「高度な自動走行システムの社会実装に向けた研究開発・実証事業」で得られたものである．研究実施にあたり，多大なるご協力を賜った一般財団法人　日本自動車研究所に対し，感謝の意を表する．

筆　者


海原信之*
N. KAIHARA


木村幸司*
K. KIMURA


石原　敦**
A. ISHIHARA


中村英夫***
H. NAKAMURA

*　研究開発本部　FFR 部
**　研究開発本部　システム創生研究部
***　一般財団法人　日本自動車研究所　ITS 研究部