

| | |
|------|-------------|
| 報告番号 | 甲 第 11465 号 |
|------|-------------|

主 論 文 の 要 旨

論文題目 車両に潜在する冗長性を活用した
耐故障制御系設計に関する研究

氏 名 伊藤 章

論 文 内 容 の 要 旨

本研究は、Steer-by-Wire とインホイールモータ方式の Drive-by-Wire を搭載した次世代仕様車両の操舵、駆動系のアクチュエータおよびセンサ故障に対する耐故障制御系設計に関するものである。急速に進む車載システムの電子制御化に伴い必要性の高まる安全設計に対し、車両重量やコストの増加など、電子制御化の利点を損なう従来の冗長化手法から脱却した新たな手法を提案することで、より高度な電子制御技術の普及に貢献することをねらいとする。

1970 年代にエンジン制御を起点に進んだ車載システムの電子制御化は、燃費や性能を極限まで追求するあまり、現在ではドライバ意図にまで制御が介入する X-by-Wire へと発展している。X-by-Wire とは、航空機の Fly-by-Wire に代表されるように、「ドライバの意思を電気信号に変換し、その電気信号に基づき電子制御ユニットがアクチュエータを駆動する」技術である。電気信号で意思を伝達するため機械的伝達機構が廃止でき、燃費向上、予防安全技術の実現、衝突安全性向上や搭載位置・デザインの自由度向上といった多くの利点がある。そのため、既に製品化されている Drive-by-Wire に加え、Steer-by-Wire、Shift-by-Wire、Brake-by-Wire など、あらゆる機構の X-by-Wire 化が検討され、製品化を目指している。しかし、多くの利点を有する反面、ドライバ操作とアクチュエータ動作の間に機械的結合が存在しないことに加え、ドライバ意図にも制御が介入することから、制御系を構成するコンポーネントのいずれかに故障が発生すると、暴走、セルフステア、逆走などの危険に至る恐れがあり、安全設計が極めて重要になる。Fly-by-Wire で先行する航空機の安全設計手法を自動車に適用すればよいと思われるが、自動車は航空機と比べコストや搭載スペースの制約が厳しいこと、故障発生から危険回避するまでの時間的余裕がないこと、厳格な運行管理がされていないことなどが理由で容易ではない。そのため、自動

車の安全設計は乗り物の中で最も難しいといわれており、既に十分な性能が確認されている X-by-Wire システムも存在するが、安全性が十分に検証できていないため製品化に至っていない。すなわち、製品化する上では「安全性の確保」が最重要課題であり、安全設計が確立しない限り、我々は X-by-Wire 技術の恩恵を享受できないといっても過言ではない。

しかしながら、従来安全設計に対する明確な基準やプロセスがなく、車両メーカー、部品サプライヤ毎に独自の手法で安全設計を行うのが一般的であった。そのため、長年慣れ親しんできたハードウェアを中心とした機械式システムの設計プロセスが踏襲されることが多く、正常時の機能を実現するためのハードウェアを作り込んだ後、故障の木解析 (FTA) や故障モードと影響解析 (FMEA) などで各故障モードの致命度を分析し、危険と判断された故障モードに対し、故障検出、フェイルセーフ/フェイルソフトや保護装置の追加による影響度の軽減、材質強化や冗長化による発生頻度の低減などで安全性を確保するという手順で行われていた。その結果、既に作り込みが完了している正常時の機能や他のシステムに影響を及ぼさないようなコンポーネント単位の安全設計に帰着し、コンポーネント間に重複した冗長性が散在することで、車両重量やコストの増加を招いた。安全設計により X-by-Wire の利点が失われるといった問題の顕在化により、従来手法の延長線上では高度化する電子制御システムの安全性確保は困難であり、安全基準、プロセスを各社が独自に策定し、運用する方法ではもはや限界であることが広く認識されはじめたことを背景に、2011年に国際標準化機構 (ISO) が自動車向け機能安全規格 ISO26262 を発行した。客観的に安全性評価ができるという利点から、口火を切った欧州の車両メーカーに続き、国内の車両メーカーも 2014年以降に生産が始まる新規の電子システムから規格対応する方針を提示し、部品サプライヤに対しても規格対応を求める動きが活発化している。そのため部品サプライヤは、コンポーネント単位で安全設計を行い、ボトムアップ式に車両の安全性を主張してきた従来手法を改め、規格が要求するハザード分析とリスクアセスメント結果より決定した安全目標から設計要件を導出し、ソフトウェア、ハードウェア設計を行うトップダウン式手法への変革を求められており、製品設計初期段階から性能のみならず、安全性も考慮した設計手法を模索し始めた。

本研究は、上記課題に焦点を当て、コンポーネント単位で構成部品を冗長化し安全性を確保する従来手法から脱却するため、車両全体を俯瞰し、性能や利便性の向上を目的に導入されたシステムや人間 (ドライバ) と電子制御の間に潜在する冗長性を活用するというアプローチで耐故障制御系設計に取り組んだ。その結果、新たにバックアップ目的の部品を追加することなく、安全性を確保した耐故障制御系を得た。さらに設計面では、従来の後付け的な安全設計を見直し、ISO26262 が提唱する制御系設計初期段階から性能と安全性の両要件を考慮した手法を与えた。

本論文の構成は、以下の通りである。

第1章では、本研究の背景、目的を述べる。

第2章では、将来の小型電動車両向け操舵・駆動方式として期待される、Steer-by-Wire

とインホイールモータを搭載し、前輪操舵に加え左右後輪の制駆動力が独立制御可能な車両を耐故障制御系の設計対象とし、車両の等価3輪モデルとSteer-by-Wireの回転2次系モデルを紹介する。さらに、本論文で取り扱う操舵、駆動系のアクチュエータとセンサに関連する故障を定義し、故障発生時の車両挙動について分析する。

第3章では、第2章で定義した車両の操舵系故障を対象とし、従来のステアリングホイールとラック軸を機械的に結合する、バックアップモータに切り替える、前輪操舵に加え後輪操舵を併用するといった専用のバックアップ装置を必要とする操舵系に閉じた機能補償とは異なり、左右輪の制駆動力差による旋回モーメント発生という駆動系の潜在能力に着目し、系の枠を超え、操舵系故障を駆動系で補償する耐故障制御系とその設計法を提案する。具体的には、故障発生から危険に至るまでの時間が数十msと非常に短い操舵系故障に対処するため、故障検出を伴わずにフェイルソフトを実行するアプローチとし、外乱オブザーバの考え方を活用する。すなわち、故障に伴う操舵性能不足を規範モデルと実車両挙動との偏差として捉え、偏差に応じて常時左右制駆動力による補償を行う制御系を構築する。さらに、提案した耐故障制御系により、故障発生後の退避操作が安全に達成されることをシミュレーションで確認する。

第4章では、第3章の内容に対して新たに駆動系故障を考慮し、操舵、駆動系両者の故障に対応可能な耐故障制御系を構築し、より実用的な手法へと発展させる。従来駆動系故障に対しては、インホイールモータなど駆動手段を限定することなく、前後または4輪独立駆動などの独立駆動系構造に着目した方法が提案されている。たとえば、前後輪独立駆動構造をもつ駆動系を構成し、片方の故障による駆動力喪失分を他方の正常な駆動系で補償する方法や、4輪独立制御可能な駆動系を構成し、故障により喪失した駆動力を、車両や路面の状況に応じて残りの車輪に再配分することで車両挙動を安定化させる方法などが挙げられる。操舵系同様、駆動系内で閉じた機能補償であり、コンポーネント毎の冗長化を助長させるアプローチであるといえる。これに対し、本研究では片輪駆動とSteer-by-Wireによる旋回モーメントの打ち消しという操舵・駆動系間の潜在能力に着目して駆動系故障に対処し、操舵・駆動系が相互補完しあう耐故障制御系とその設計法を提案する。各制御器の設計では、外乱オブザーバ、ゲインスケジューリング H_{∞} 制御手法を適用し、その有効性をシミュレーションで検証する。

第5章では、センサ故障に焦点を当てる。アクチュエータ故障では、操舵・駆動系間に潜在する冗長性に着目したが、センサ故障では、人間（ドライバ）・電子制御間に潜在する冗長性に着目したアプローチを適用している点が異なる。自動車の運転に必要な「認知」、「判断」、「操作」のサイクルには、人間と電子制御による2つのサイクルが存在している。運転に最低限必要な基本機能が確保されていれば、人間によるサイクルのみで自動車の運転は可能であるが、電子制御によるサイクルが加わることで、ドライバの操作負担軽減やドライバでは不可能な緻密な制御を行い予防安全、環境性能などの付加機能を達成している。ここでセンサは「認知」の役割を担うが、同時に人間も視覚、聴覚、三半規管などを

使って車両挙動，周辺状況を「認知」している．この人間と電子制御の間に潜在する冗長性を考慮すると，センサ故障発生後も人間による「認知」は可能であるため，センサ故障により電子制御によるサイクルが人間によるサイクルに悪影響を与えない限り，人間主体の運転は継続可能であるといえる．本研究では，Steer-by-Wire の操舵制御において，上述した基本機能と付加機能を明示的に区別した制御系を構築し，基本機能に関与するセンサには，冗長化，多数決選択といった従来型の安全設計手法を踏襲して耐センサ故障性を確保し，付加機能に関与するセンサには，故障時に基本機能に悪影響を及ぼさないことを要件とした対策，すなわち制御器の出力抑制，制御ループ切断などを施すことで全てのセンサの冗長化を回避する耐故障制御系とその設計法を提案する．制御系設計には，第3，4章と同じ設計・解析手法を適用し，その有効性をシミュレーションで検証する．

第6章では，本研究のまとめを行うとともに，今後の展望について述べる．