【主論文の要旨・記入例】

学位報告 4

報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目　　自動車の協調制御システムのための

安全性向上手法

氏　　名　　石郷岡　祐

論 文 内 容 の 要 旨

低炭素化，交通事故低減，利便性向上を目的として自動車制御システムの高機能化が進展している．自動車制御システムは複数の電子制御ユニット（ECU：Electronic Control Unit）で構成され，接続する車載ネットワークを介して，ECU が協調制御することで，高度な制御機能を実現している．自動車の協調制御システムの故障は，人命に関わる重大な事故につながる可能性がある．従って，高い安全性が求められるが，自動車の協調制御システムでは安全性の保証が難しい課題がある．

協調制御システムでは，関連する ECU は原則的に同じ車載ネットワークに接続される．しかしながら，すべての ECU を同一の車載ネットワークに接続すると，通信量が車載ネットワークの容量を超過し，リアルタイム性を保証できなくなるため，特に関係の強い（通信メッセージを頻繁にやり取りする）ECU 群でサブシステムを設ける．このサブシステムはドメインと呼ばれ，エンジンやモータなどの車両駆動系のパワートレインドメイン，ワイパーやヘッドライト系のボディドメイン，操舵やブレーキ等の走行制御系のシャシードメインなどで構成される．ドメイン間の通信はゲートウェイ ECU が通信メッセージを転送することで実現する．

自動車制御システムにおける協調制御はドメイン内に限らず，ゲートウェイ ECU を介したドメイン間のハードリアルタイム分散処理が求められる．ハードリアルタイムとは決められたデッドライン以内に必ず実施しなければならない性質である．本論文では，ハードリアルタイムが求められる ECU を安全系 ECU，利便性・快適性向上を目的とした ECU を非安全系 ECU と呼び，協調制御は前者の安全系 ECU の分散処理で実現される．

ドメイン間のハードリアルタイム分散処理の例として，カメラや LiDAR の外部環境の認識デバイスを用いて車両走行状況を認識し，その結果に応じて運転手の代わりに自動で加速度や制動力を制御する運転支援システムや，すべての車両操作を運転手の代わりに実施する自動運転システムがある．このような協調制御の高度化に伴い，従来の自動車制御システムで用いられていた車載ネットワークの Controller

Area Network(CAN)では，通信量が不足してきたため，大容量通信の FlexRay に移行が進んでいる．しかしながら，異なるネットワークを介する分散処理では，デッドライン保証の予測が困難になる課題がある（第一の課題）．さらに，CAN を前提に開発された制御アプケーションやゲートウェイアプリケーションを時間駆動ネットワークの FlexRay に対応させるために再設計を要する課題がある（第二の課題）．

また，協調制御システムの一例である自動運転では，万が一，走行中に安全系 ECU が故障が発生しても，自動で安全な場所まで走行し続け，停止することが求められる．この故障後にも安全に動作し続ける機能をフェールオペレーショナル機能と呼ぶ．安全系の ECU が故障すると，車両制御の安全性が保てなくなるため，安全系の ECU で冗長構成を組むアプローチがとられる．これを達成するための従来方式として，ハードウェア冗長化方式がある．しかしながら，高性能マイコンを採用している自動運転 ECU を 2 組設けることは高コストとなる課題がある（第三の課題）．

さらに，協調制御システムでは，複数の安全系 ECU が 1 つのアクチュエータを共有し，調停しながら制御を行う場合がある．複雑な仕様となるため，ECU 連携時における設計不具合の有無を確認するための安全検証が求められる．設計段階で仕様の不具合を見つける方法として，制御ソフトウェア（コントローラ）と制御対象（プラント）をモデル化してシミュレーションで妥当性を確認するモデルベース開発(MBD)がある．特にマイコンの挙動も含めてテストする場合には Hardware-In-the-Loop-Simulation(HILS)が用いられる．しかしながら，HILS ではコントローラとプラントが特定の条件（タイミング，入力信号の順序）でのみ発生する不具合の検出は困難である．本研究では，このようなコントローラとプラントの相互作用による不具合をシステムレベルの不具合と呼ぶ．システムレベルの不具合を設計段階で検出するためには，複数の ECU が共有するアクチュエータを制御する際の組み合わせを特定の条件において検証可能とする技術が必要である（第四の課題）．さらに，不具合検証のためだけに，検証モデルを 1 から構築することは開発工数の観点から許容困難であるという課題がある（第五の課題）．

本研究では自動車の協調制御システム向けの安全性向上手法の構築を目指し，前節で述べた 5 つの課題を解決する研究を行った．

第一の研究では，イベント駆動ネットワークから時間駆動ネットワークへの移行を容易にするリアルタイムゲートウェイ方式を提案した．イベント駆動ネットワークから受信されるデータ量の予測が困難である．そのため，従来方式としてイベント駆動ネットワークから受信されるデータを時間駆動ネットワークに 1 対 1 で対応付ける方法が提案されているが，スロット効率が悪い懸念がある．そこで我々は，多対 1 の対応付けを実現することで，少ないスロットサイズでハードリアルタイム性を保証できるクラスタベース通信方式を提案した(第一の課題の解決)．そして，クラスタベース通信方式をミドルウェアに実装することで，イベント駆動ネットワーク向けに開発された開発済みのゲートウェイアプリケーションや制御アプリケーションをシームレスに時間駆動ネットワークに移行可能とした(第二の課題の解決)．シミュレーションによって通信方式を評価し，従来方式と比べて，約 49%の FlexRay スロットでハードリアルタイム性を保証可能なデータ通信を実現できる見込みを得た．またミドルウェアを処理時間とコードサイズに関して評価し，車載向けマイコンにおいて実装・動作可能であることを確認した．

第二の研究では，フェールオペレーショナル対応自動運転システム向けのレプリ

ケーション手法を提案した．従来方式として，自動運転 ECU と同じ機能を冗長化させるのではなく，冗長系を最低限の機能に絞った縮退機能で冗長化し，縮退状態で CPU が空いている ECU に割り当てる ECU マルチモード方式が提案されている．従来方式では，正常状態で縮退機能を実行しないため，CPU 負荷を低減できる．しかしながら，故障発生後に縮退機能に切り替えても，新たに実行を開始するために，有効な出力を発行できるまでに時間（ダウンタイム）を要する課題がある．そこで我々は，縮退機能を構成するアプリケーションの特性に応じた 3 つのレプリケーション手法を提案する．ダウンタイム要件を満たしつつ，CPU 負荷の低いレプリケーション手法を選択することで低コストに冗長系を構築可能とする（第三の課題の解決）．自動運転システムのプロトタイプを用いて提案手法を評価し，従来のホットスタンバイ方式と比べて，ダウンタイム要件を満たしつつ，正常状態で 41.6%，縮退状態で 14.0%の CPU 負荷を低減できた．これにより，より安価な CPU を選択可能となる見込みを得た．

第三の研究では，協調制御システム向けのモデルベース開発を活用した安全検証を提案した．従来方式に HILS があるが，HILS では制御ソフトウェアとプラントモデルが異なるハードウェアで動作するために各々を同期されたテストが難しい課題がある．そこで我々は，制御ソフトウェアとプラントモデルを統合することでシステム動作を模擬したモデルを構築し，記号実行を用いて安全検証を実施する検証プロセスを提案した（第四の課題の解決）．さらに，MBD で設計されたプラントモデルを再利用してシステムモデルを構築するために，検証計算量を削減するためのモデル簡易化フレームワークとモデル変換手法を提案した(第五の課題の解決)．自動車のブレーキ制御システムを用いて評価を実施し，第一のケーススタディによって，提案手法が 2 つの ECU による協調制御の不具合を検出可能であることを示した．さらに第二のケーススタディによって，提案したモデル簡易化フレームワークが約 35%の計算量を削減可能なこと，提案したモデル変換手法が生み出す変換誤差が認識できないほど小さいことを確認できた．

以上のように，本論文では自動車の協調制御システムの安全性を保証するための 5 つの課題を，3 つの研究で解決した．これにより，自動車の協調制御システムの安全性向上に貢献できた．