

## 論文審査の結果の要旨および担当者

報告番号	※ 甲 第	号
------	-------	---

氏 名 石郷岡 祐

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

論文審査担当者

主 査 名古屋大学教授 高田 広章

委 員 名古屋大学教授 結縁 祥治

委 員 名古屋大学准教授 本田 晋也

## 論文審査の結果の要旨

石郷岡祐君提出の論文「自動車の協調制御システムのための安全性向上手法」は、複数の電子制御ユニット（ECU）が車載ネットワークで接続されている自動車の協調制御システムの安全性を向上させる技術に関する一連の研究をまとめたもので、6章で構成される。

第1章は序論であり、近年、自動車の協調制御システムの高機能化が進んでいることを述べ、その安全性の課題として、イベント駆動ネットワークと時間駆動ネットワークが混在していること、フェールオペレーショナルの実現にハードウェアの冗長構成を利用することが困難であること、複数のECUが1つのアクチュエータを共有する場合の安全検証手法が必要であることについて説明している。また、本論文の構成と概要について述べている。

第2章では、自動車の協調制御システムに対する安全性向上手法について述べている。まず、本論文で対象としているシステムにおける安全性について定義し、安全性向上手法であるフェールオペレーショナル処理と安全検証手法について説明している。また、自動車の協調制御システムにおけるハードリアルタイム分散処理の特徴として、イベント駆動ネットワークと時間駆動ネットワークが混在していることを説明している。

第3章では、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化するリアルタイムゲートウェイについて述べている。提案しているリアルタイムゲートウェイは、イベント駆動ネットワークから送られるデータを時間駆動ネットワークのスロットに多対1に割り付けることで、小さいスロットサイズでハードリアルタイム性を保証するクラスベース通信方式を提案している。また、イベント駆動ネットワーク向けに開発された既存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するミドルウェアを実現している。提案手法は、想定されるデータセットにおいて、従来手法と比べて約49%のスロットサイズで、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ことを示している。

第4章では、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について述べている。従来のホットスタンバイ方式ではハードウェアコストが高くなり、コールドスタンバイ方式では故障発生時に縮退機能に切り換えて有効な出力を発行できるまでの時間（ダウンタイム）が長いという課題に対して、縮退機能を構成するアプリケーションの特性に応じて3つのレプリケーションを使い分ける手法を提案している。提案手法を自動運転システムのプロトタイプに適用し、ダウンタイム要件を満たしつつ、ホットスタンバイ方式と比べて、正常状態で41.6%、縮退状態で14.0%のCPU負荷を低減できることを示している。

第5章では、協調制御システム向けのモデルベース開発（MBD）を活用した安全検証について述べている。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

## 論文審査の結果の要旨

動作するために時間的に同期したテストが難しいという課題に対して、提案手法では、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、記号実行を用いた安全検証を実施する検証プロセスを提案している。また、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ことで検証計算量を削減する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ている。ケーススタディによる評価により、提案手法を用いて協調制御の不具合を検出可能であること、モデル簡易化フレームワークにより約 35% の計算量を削減できること、モデル変換手法の変換誤差が小さいことを示している。

第 6 章は結論であり、本論文の成果をまとめるとともに、今後の課題について論じている。

以上のように、本論文は、自動車の協調制御システムの安全性を向上させる各種手法に関する研究に取り組み、いずれにおいても有効な成果を挙げている。提案した技術や発見した知見は、いずれも、学術的な新規性に加えて実用性も高いものであり、情報学の学術上・技術上の寄与が大きい。よって、本論文提出者、石郷岡祐君は、博士（情報学）の学位を受けるに十分な資格があるものと判定した。