論 文 内 容 の 要 旨

氏 名 （ 櫻井 康平 ）	
論文題名	An Autonomous Decentralized Architecture with Agreement Protocols for Safety-Critical Embedded Distributed Control Systems （自律分散アーキテクチャおよび合意プロトコルによる 高信頼組込み分散制御システムに関する研究）

論文内容の要旨

本研究の対象である組込み制御システムは，現在，家電，自動車，鉄道などの工業製品に広く使われている．組込み制御システムには，情報システムと比較して，高いリアルタイム性が要求されるとともに，コストや利用可能なハードウェアリソースに強い制約がある．本研究では，組込み制御システムの中でも，量産規模が大きいため，特にこれらの制約が厳しい自動車の制御システムを対象とする．

近年，自動車では電子制御化が急速に進展しており，より高度で複雑な制御システムが開発されている．これらのシステムの中で，複数の制御装置（以下ノードと記す）が通信ネットワークを介して協調動作することで，「走る，曲がる，止まる」を電子的に制御するX-by-Wire（XはDrive，Steer，Brakeなど）と呼ばれる走行制御システムは，次世代の自動運転に向け，自動車の走行性能や安全性を高める制御システムとして今後の普及が期待されている．

X-by-Wireシステムには高い信頼性が要求される一方で，航空機や鉄道などと異なり，信頼性を確保するための追加コストに厳しい制約がある．したがって，本システムを普及させるためには，高信頼性と経済性を両立させる技術の開発が必要である．以上のような背景を踏まえ，本研究は，自動車のX-by-Wireシステムを題材とし，高信頼かつ低コストな組込み分散制御システムを提案することを目的とする．

まず，本研究では，自律分散システムの考えを取り入れた新たな制御システムアーキテクチャを提案した．本アーキテクチャでは，各々のノードが自分の制御に必要な情報をネットワークから取り込み，あるノードに障害が発生した場合でも，残存する正常なノードが自律的にバックアップ制御を行うことでシステムの機能を維持する．これにより，障害ノードの存在を許容するシステムを構築できるため，故障時にも正常動作を継続するように個々のノードを冗長化する必要がなくなり，システムコストを低減することが可能となる．さらに，個々のノードについても冗長化に頼らずに高信頼性を確保するハードウェアアーキテクチャを示した．

自律分散アーキテクチャでは，各々のノードが異なった制御モードに移行することを防止するために，システム内ノードに関する状態情報をノード間で常に一致させるための合意プロトコルが必要である．これを実現するために，本研究では，メンバシッププロトコルを提案した．本プロトコルでは，各ノードが個別に評価したシステム内の全ノードに関する状態情報を，他ノードと相互に交換し，これを多数決することでノード状態を判定する．提案プロトコルは，先行研究とは異なり，多重故障や，プロトコル仕様としては正しいもののデータの内容にエラーが含まれるByzantine故障を許容できること，および，上記のプロトコル処理をパイプライン的に実行することでノード状態判定のリアルタイム性を高めたことが特長である．また，上記の故障条件において，本メンバシッププロトコルが正当性，完全性，一貫性等のプロパティを満たすことを証明した．

本プロトコルをTDMA（タイムトリガ）方式の自動車制御用通信プロトコル上にミドルウェアとして実装し，自律分散Brake-by-Wireシステムのプロトタイプを構築した．機能評価により，自律分散アーキテクチャを実際の自動車制御システムに適用可能なことを実証した．一方で，性能評価により，メンバシップミドルウェアの演算処理負荷を実用上はさらに低減する必要があることを指摘した．

この課題を解決するために本研究ではさらに，軽量なメンバシッププロトコルを提案した．この軽量プロトコルは，多数決対象ノード数を減らすことなどにより，演算処理負荷と通信データ量を低減することができる．実測により，はじめに提案したメンバシッププロトコルに比べ，多数決演算の処理負荷を8ノードの場合，約60%低減できることを示した．一方で前記プロパティの証明により，軽量メンバシッププロトコルは耐障害性が低下することを明らかにし，耐障害性を向上させる追加プロトコルを提案した．

最後に，本研究では，タイムトリガ通信を用いた高信頼分散制御システムの一連の開発，すなわち，設計からテスト，検証までを支援するための汎用的な形式モデルを提案した．再利用性の高いモジュール構成のモデルとすることで，開発工数を低減できるとともに，形式手法の専門家でないシステム開発者が活用することも容易となる．本研究では，SAL（Symbolic Analysis Laboratory）言語を用いてプロトタイプモデルを開発した．検証のユースケースとして，提案したメンバシッププロトコルのモデル検査を実施し，本プロトコルが前記プロパティを満足することを検証した．

様式7

論文審査の結果の要旨及び担当者

氏　名　（　櫻井　康平　）		
	（職）	氏　名
論文審査担当者	主査　教　授	土屋　達弘
	副査　教　授	今井　正治
	副査　教　授	増澤　利光
	副査　准教授	橋本　昌宜

論文審査の結果の要旨

本論文は、組込み制御システム、特に、自動車制御システムにおける、現実的なコスト制約下での信頼性の向上に関する研究の成果をまとめたものであり、以下の主要な結果を得ている。

１．自律分散システムの考えを取り入れた制御システムアーキテクチャの提案

次世代の自動車制御に必要な分散制御において高信頼性を現実的なコストの下で実現するために、自律分散システムの考えを取り入れた制御システムアーキテクチャを提案した。このアーキテクチャでは、各々のノードが自分の制御に必要な情報をネットワークから取り込み、ノードに障害が発生した場合でも、残存する正常なノードが自律的にバックアップ制御を行うことでシステムの機能を維持する。これにより、システムは障害ノードの存在を許容できるため、個々のノードを冗長化する必要がなくなり、システムコストを低減することが可能となる。さらに、個々のノードについても高信頼性を確保するハードウェアアーキテクチャを示した。

２．メンバシップ合意プロトコルの提案と実装

自律分散アーキテクチャでは、各々のノードが異なった制御モードに移行することを防止するために、システム内ノードに関する状態情報をノード間で常に一致させるためのプロトコルが必要である。これを実現するために、メンバシップ合意プロトコルを提案した。本プロトコルでは、各ノードが個別に評価したシステム内の全ノードに関する状態情報を、他ノードと相互に交換し、これを多数決することでノード状態を判定する。提案プロトコルは、先行研究とは異なり、多重故障や、データの内容にエラーが含まれるByzantine故障を許容できること、および、上記のプロトコル処理をパイプライン的に実行することでノード状態判定のリアルタイム性を高めたことが特長である。本プロトコルをTDMA（タイムトリガ）方式の自動車制御用通信プロトコル上にミドルウェアとして実装し、自律分散Brake-by-Wireシステムのプロトタイプを構築した。更に、演算処理負荷と通信データ量を低減することができる、軽量なメンバシップ合意プロトコルを提案した。

３．形式モデルの提案とそれを用いたプロトコル検証

タイムトリガ通信を用いた高信頼分散制御システムの一連の開発、すなわち、設計からテスト、検証までを支援するための汎用的な形式モデルを提案した。再利用性の高いモジュール構成のモデルとすることで、開発工数を低減できるとともに、形式手法の専門家でないシステム開発者が活用することも容易となる。本論文では、SAL言語を用いてプロトタイプモデルを開発した。検証のユースケースとして、提案したメンバシップ合意プロトコルのモデル検査を実施し、本プロトコルが必要なプロパティを満足することを検証した。

以上のように、本論文における組込み制御システムに関する研究は、分散制御を必要とする状況において高信頼性を現実的に実現できる点を実証しており、非常に有用である。これにより、自動車制御等の重要な応用分野の発展に貢献するものと期待できる。従って、博士（情報科学）の学位論文として価値のあるものと認める。