

氏 名	さい とう まさ ひこ 齊 藤 雅 彦
学位(専攻分野)	博 士 (情 報 学)
学 位 記 番 号	情 博 第 178 号
学位授与の日付	平 成 17 年 9 月 26 日
学位授与の要件	学 位 規 則 第 4 条 第 1 項 該 当
研究科・専攻	情 報 学 研 究 科 通 信 情 報 シ ス テ ム 専 攻
学 位 論 文 題 目	ユビキタス情報制御システムにおける高信頼リアルタイム分散制御 アーキテクチャの研究
論文調査委員	(主 査) 教 授 富 田 眞 治 教 授 奥 乃 博 教 授 湯 淺 太 一

論 文 内 容 の 要 旨

プラント制御システムにおいて、生産管理部門から製造現場に至るまでの「きめ細かな情報共有」が求められる。このような情報共有を行うため、本論文では、HTML/XML といった情報系ネットワーク技術でインタフェースを統一する「製造現場ユビキタス通信基盤」を提案した。さらに、本プラットフォームを実現するための基本技術として、以下に示す分散制御技術、組込み計算機技術について研究したものである。

本論文の内容は以下の通りである。

第1章 序論

本研究の背景、目的、および、本論文の構成について述べている。

第2章 製造現場ユビキタス通信基盤

主な研究ターゲットである「製造現場ユビキタス通信基盤」の詳細を考察している。製造現場ユビキタス通信基盤において、多数の設備機器が協調して動作する超分散プラント制御システムを構築することができるが、セキュリティに代表される課題も加速的に大きくなる。本論文では、主としてプラント制御システムのセキュリティについて考察し、コントローラを権限管理主体とするセキュリティフレームワークを提案した。同時に、セキュリティフレームワーク構築の過程で、セキュリティ、Schema 機能など、コントローラ（設備端末）に対する負荷が大きくなっていることを明確化した。

第3章 プラント制御における高信頼分散制御システム技術

プラント制御システムにおいても、PC/小型サーバの利用がかつてないほど進んでおり、個々の計算機単体での信頼性は従来に比べて低下しているといえる。本論文では、このような環境における高信頼分散制御システムアーキテクチャを提案している。

プラント制御システムにおいては、製造現場情報を収集した生産管理部門がスケジュール管理、トレーサビリティ等のアプリケーションを実行する。本論文では、これらの特徴を生かし、故障発生時に改めて必要なデータを収集し、システム管理ソフトウェア、アプリケーションを再構築する高信頼化方式“Lazy Fault Tolerance”を提案している。Lazy Fault Tolerance は通常時に行う処理をできる限り省略しているため、通常時のオーバーヘッドを極めて小さな値とすることが可能である。

第4章 プラント制御ネットワークのリアルタイム同期機構

プラント制御システムの将来像では、個々のコントローラにおける応答性・リアルタイム性だけでなく、ネットワークを含んだリアルタイム性を保証していく必要がある。本論文では、ネットワークを介したリアルタイム性保証の対象の一つとして、複数の計算機間で待合せを行うバリア同期に着目し、これに対して時間制約を保証するための機構「リアルタイムバリア同期」を提案している。リアルタイムバリア同期は、計算機間でのグローバルなスケジューリングを行う交渉フェーズと、交渉フェーズによって決定された時間制約にしたがって各々の計算機でタスクを起動するスケジューリングフェーズと

に分割して実行され、計算機間での同期処理に対して時間制約を保証する。

第5章 リアルタイム制御機能と情報系ネットワーク技術との共存方式

本論文では、既存制御機能に加え、情報系ネットワーク技術を導入した「ユビキタスコントローラ」の概念を提示し、それに基づく二つの組込み計算機技術を開発している。第一に、情報系ネットワーク技術に優れた汎用 OS と制御機能に適したリアルタイム OS とを単一プロセッサ上で共存させる組込み計算機システムを開発した。組込み計算機システム特有の条件である応答性・リアルタイム性保証を行うため、異なる OS 間での優先順位体系の差違を吸収し、より高い重要性を有するタスクを実行している OS を動作させる「優先順位統一モデル」を提案している。

次に、HTML/XML に代表される情報系ネットワーク技術と、Rate Monotonic スケジューリングで実行されるリアルタイム制御機能とをよりいっそう連携させ、「Web でモノを制御する」コンセプトの確立を目指した。本論文では、HTML/XML タグで優先順位・時間制約を指定し、処理サイクルの時間の流れに合わせて解釈・実行することにより、情報系ネットワーク技術を含めたリアルタイム性を保証する方式を提案している。

第6章 コントローラにおける並列処理支援技術

コントローラに搭載される機能が増大するにしたがって重要となる並列処理支援技術について考察している。コントローラで動作するアプリケーションは、通常、プラント制御システムのユーザが構築するものであるため、並列処理環境においては、特に、使い勝手やユーザのプログラミング作法に対する堅牢性が重要となる。

使い勝手向上という観点から、マルチスレッド実行環境のための並列処理インタフェースを開発した。この中で、複数のスレッドをまとめて操作する「スレッドグループ」という概念を提案している。

次に、堅牢性という観点から、マルチスレッド実行環境において、スレッドのスタック領域を保護し、かつ、仮想空間を最大限に使用する「動的スタック拡張方式」を開発した。動的スタック拡張方式は仮想空間を複数のユーザページに分割し、これを単位として、スレッドのスタック領域に仮想空間を動的に割り当てる方式である。これにより、ユーザがスタック領域の大きさを指定したり、気にかけたりする必要はなく、仮想空間を最大限に使用することができる。

第7章 結論

本論文で得られた主要な結論について要約し、今後のプラント制御システムに必要な組込み計算機システムの課題を提示している。

論文審査の結果の要旨

プラント制御システムでは、HTML/XML といった情報系ネットワーク技術で情報共有を行う「製造現場ユビキタス通信基盤」の構築が必要となっている。本論文では、プラント制御システムの将来像を考察し、製造現場ユビキタス通信基盤のアーキテクチャとその要素技術についての検討を行った。その内容と得られた成果は以下の通りである。

1. 製造現場におけるセキュリティフレームワークの提案

プラント制御システムにおいて、設備機器を直接監視制御するコントローラが権限管理主体となるセキュリティフレームワークを提案した。セキュリティフレームワークを実現するため、eTRON を利用したセキュア対応コントローラを試作した。同時に、Schema 機能など、コントローラに対する負荷が大きくなってきていることを示した。

2. プラント制御における高信頼分散制御システム技術の提案と評価

プラント制御システムの特徴を生かし、故障発生時に改めて必要なデータを収集し、システム管理ソフトウェア、アプリケーションを再構築する高信頼化方式“Lazy Fault Tolerance”を開発した。Lazy Fault Tolerance では、通常時に行う処理をできる限り省略しているため、通常時オーバヘッドを3%以下とすることができる。

3. プラント制御ネットワークのリアルタイム同期機構の提案と評価

計算機間での待合せに対して時間制約を保証するための機構「リアルタイムバリア同期」を提案した。計算機間でのグローバルなスケジューリングを行う交渉フェーズと、交渉フェーズによって決定された時間制約にしたがって各々の計算機でタスクを起動するスケジューリングフェーズとに分割して、リアルタイムバリア同期を実現した。

4. リアルタイム制御機能と情報系ネットワーク技術との共存方式の実現と評価

既存制御機能に加え、情報系ネットワーク技術を導入した「ユビキタスコントローラ」の概念を提示した。第一の方法として、汎用 OS とリアルタイム OS とを単一プロセッサ上で共存させるハイブリッド OS 実行環境を提案し、 10μ 秒以下のオーバーヘッドで二つの OS を共存させる環境を構築した。次に、制御機能と情報系ネットワーク技術のより密接な連携を目的とし、HTML/XML タグで指定した優先順位を Rate Monotonic スケジューリングに統合する方法を示し、数%程度のオーバーヘッドで実装できることを示した。

5. コントローラにおける並列処理支援技術の提案と評価

コントローラに並列処理の考え方を導入するにあたって、複数のスレッドをまとめて操作する「スレッドグループ」という概念を導入した。同時に、堅牢性を向上させるため、スレッドのスタック領域を相互に保護する「動的スタック拡張方式」を開発し、これらが5%程度以下のオーバーヘッドで実現できることを示した。

以上、本論文は、プラント制御システムの将来像を実現するための提案と、試作・評価を行ったものであり、学術上、実際に寄与するところが少なくない。よって、本論文は、博士（情報学）の学位論文として価値あるものと認める。また、平成17年8月8日実施した論文内容とそれに関連した試問の結果、合格と認めた。