学位報告 4

報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目	組込みリアルタイムシステムにおけるメモリ保護機能対応プラットフォームおよび確率的応答時間解析
氏　　名	石川 拓也

論 文 内 容 の 要 旨

大規模・複雑化が進む組込みリアルタイムシステムの開発において，開発コストの低減や開発期間の短縮が求められている．ソフトウェアの開発に関して，開発効率向上のために，リアルタイムオペレーティングシステム（OS）や，組込みシステム向けのソフトウェアコンポーネント技術が提案されている．既存のコンポーネント技術は，アプリケーションソフトウェアの開発を支援するものが多いが，ミドルウェアやデバイスドライバなどのソフトウェアプラットフォームを開発できるものもある．ソフトウェアプラットフォームをコンポーネントベース開発することにより，システムのハードウェア構成やアプリケーションの要求に応じて，ソフトウェアプラットフォームの構成を容易に変更できる．また，近年では，安全性が求められるシステムのアプリケーション開発に適用するためのリアルタイム OS やコンポーネント技術が提案されている．

一方で，組込みリアルタイムシステムでは，システム内のタスクが，個々のデッドラインを満たすかどうかを検証することが重要である．従来のリアルタイムシステムにおけるスケジューラビリティ解析では，タスクの応答時間を解析する際に，タスクの最大実行時間など，一意的な値が用いられることが多い．しかし，これらの手法で仮定されている，実行時間が最大となるような状況は通常発生することはなく，これらの手法によって解析された結果はあまりに悲観的であるため，そのシステムに求められる性能を過大に見積もってしまい，開発コストの増加や開発期間の増加を起こしてしまう可能性がある．

本研究では，組込みリアルタイムシステムにおける開発効率の向上や開発コストの削減を目的として，大きく分けて，2 つの研究課題について取り組む．まず 1 つ目に，リアルタイム OS やソフトウェアコンポーネント技術などのアプリケーション開発支援技術についての課題に取り組む．この研究では，組込みシステム向けのコンポーネント技術である TECS を対象とし，TECS によりソフトウェアプラットフォームをコ

ンポーネントベース開発することの有用性を示し，さらに，メモリ保護を考慮した組込みシステム向けのコンポーネント技術，HR-TECS を提案する．また，HR-TECS を実現するために，メモリ保護機能を持ったリアルタイム OS，TOPPERS/HRP2 カーネル（HRP2 カーネル）を提案する．そして 2 つ目に，リアルタイムシステムにおける応答時間解析技術について，悲観的な解析結果を改善し，リアルタイムシステムの開発コストや開発期間の増加を抑えるための課題に取り組む．この研究では，周期タスクで構成されるシステムを対象とし，タスクの応答時間分布を解析する手法を提案する．

既存のコンポーネント技術は，アプリケーションソフトウェアの開発を支援するものが多いが，ミドルウェアやデバイスドライバなどのソフトウェアプラットフォームを開発できるものもあると述べた．本研究で対象とした組込みシステム向けのコンポーネント技術 TECS では，実行時間やメモリ使用量のオーバヘッドが小さく，デバイスドライバのようなソフトウェアの細部までコンポーネント化できるとされているが，実際に TECS によりプラットフォームを開発し，その有用性を評価することはされていない．

そこで本研究では，組込みシステムにおけるソフトウェアプラットフォーム開発において TECS を適用することの有効性を示した．そのために，組込みシステム教材として用いられている LEGO 社製 MindstormsNXT におけるソフトウェアプラットフォームを，TECS コンポーネント技術により開発した事例について述べ，TECS が，ソフトウェアプラットフォームの開発に有用であることを併せて示した．そして，プラットフォームをコンポーネント化することにより，容易にプラットフォームの構成を変更でき，無駄なメモリ使用量や実行時間を削減できることを評価により示した．

一方で，近年，高い安全性が求められる組込み制御システムの開発では，安全に関する国際規格に準拠することが求められている．これらの国際規格に準拠してソフトウェアを開発する場合，その設計やテストに対して厳格な検証が求められており，ソフトウェアの開発コストが高くなり，開発期間も増大する．ソフトウェアの開発コストを低減し，開発期間を短縮するためには，パーティショニング機構を用いて，高い安全性が求められるソフトウェア部分をできる限り局所化し，厳格な検証が必要な部分を少なくすることが有効である．そのため，安全性が求められる組込みソフトウェアの開発効率を向上するために，パーティショニング機構を提供するリアルタイム OS が提案されている．

パーティショニング機構の重要な機能の 1 つとして，メモリ保護機能がある．メモリ保護を実現するためには，メモリ管理ユニット（MMU）やメモリ保護ユニット（MPU）といった，専用ハードウェアが用いられることが多い．しかしながら，厳しいリソース制約やハードリアルタイム性が要求される組込みリアルタイムシステムでは，MMU は適さない．一方，MPU は，メモリ保護機能の実現を支援するが，MMU と異なり TLB のようなキャッシュを必要とせず，MPU の設定を切り替えるための時間は固定であるため，リアルタイム性の保証がしやすい．ハードリアルタイムシステムでは，メモリ保護のために MPU を用いる場合があるが，現在文献等で公表がされており，MPU をサポートするリアルタイム OS では，MPU の隠蔽が不十分であり，アプリケーション開発の生産性が低いという問題がある．

そこで本研究では，MPU を用いたメモリ保護機能を提供するリアルタイム OS，HRP2 カーネルを提案した．HRP2 カーネルでは，静的コンフィギュレーションにより，メモリ配置を静的に行う．そして，MPU を用いたメモリ保護を実現するとともに，メモリ保護に必要な情報を静的に生成し，RAM 使用量のオーバヘッドを抑えることを可能とした．本研究では，SH2A と ARM Cortex-M3

の MPU を用いて，HRP2 カーネルを実現する方法を示した．そして，HRP2 カーネルの実用性を確かめるために，メモリ保護機能を持つことによって生じる実行時間やメモリ使用量のオーバヘッドを，メモリ保護機能を持たないリアルタイム OS と比較評価し，実行時間の予測が可能であること，RAM 使用量のオーバヘッドが小さいことを示した．

また，組込みシステム向けのコンポーネント技術において，メモリ保護を考慮したソフトウェアのコンポーネントベース開発が可能な技術が提案されている．メモリ保護を考慮したコンポーネント技術は，メモリ保護機能を提供するリアルタイム OS をベースとして用い，コンポーネントに対するアクセス権やコンポーネントのパーティションへの割当てを静的に指定することで，リアルタイム OS のみを用いる場合と比較して，高い抽象度でのソフトウェア開発を可能としている．また，異なるパーティションに属するコンポーネント間の通信処理についても隠蔽することができるため，パーティションへの配置を意識することなくコンポーネントを開発でき，ソフトウェアコンポーネントの再利用性を維持できる．しかしながら，既存のコンポーネント技術で，組込みシステムに適した実装や評価がなされており，かつ，ソフトウェアプラットフォームを開発することが考慮されているものはない．

そこで本研究では，メモリ保護を考慮した組込みシステム向けのコンポーネント技術，HR-TECS を提案した．HR-TECS では，TECS コンポーネント技術を拡張することで，メモリ保護を考慮したコンポーネントベース開発を可能とし，また，HRP2 カーネルの機能を利用することで，メモリ保護機能を実現した．そのために，HR-TECS のコンポーネント記述から，HRP2 カーネルの設定ファイルを自動生成する．コンポーネント間の通信について，通信処理本体をコンポーネント記述から自動生成することで，個々のコンポーネントにおける通信 API の記述は，配置されるパーティションに依存せず，共通の API で開発することができる．また，HR-TECS は，非特権モードで動作するアプリケーションだけでなく，特権モードで動作するミドルウェアやデバイスドライバなどのプラットフォームの開発にも利用できる．そして，評価実験により，実行時間のオーバヘッドが小さく，かつ，予測が可能であること，メモリ使用量のオーバヘッドが小さいことを示した．

一方で，リアルタイムシステムにおける応答解析において，悲観的な解析結果を改善するために，タスクの実行時間を確率変数として扱い，リアルタイムシステムの応答時間を確率的に解析する手法が提案されている．この手法では，タスクの実行時間のみを確率変数として扱い，タスクの応答時間分布を数学的に解析する手法を提案している．ここで，確率変数を用いて解析を行う場合，解析手法が複雑になり，解析時間が長くなってしまうことが問題とされる．そのため，複雑さを軽減し，短時間で解析可能な手法として，応答時間分布を悲観的に近似する手法が提案されている．しかしながら，これまでに提案されている解析手法では，周期タスクの初期位相が確率変数である場合が考慮されておらず，初期位相が定数であるタスクセットしか解析することができない．

そこで本研究では，初期位相分布を考慮した，周期タスクの応答時間分布を解析する手法を提案した．タスクの初期位相を確率変数として扱う場合，各タスクの初期位相が取りうる値の任意の組合せに対して，応答時間分布を解析する必要があり， 解析時間が長くなると考えられる．そこで，本論文で提案する手法では，タスクの実行時間分布と初期位相分布を悲観的に離散化し，さらに，応答時間分布の終端部分に着目して数学的に解析することで，応答時間分布の解析時間を短縮した．モンテカルロシミュレーション結果との比較評価により，提案手法では，応答時間分布を悲観的に近似でき，かつ，高速に解析できることを示した．