平成22年度 情報工学コース卒業研究報告要旨

高田 研究室	氏　　名	太 田　貴 也
卒業研究題目	組込み向け高信頼デュアルOSモニタのマルチコアアーキテクチャへの適用	

近年，単一ハードウェア上でリアルタイムOSと汎用OSを同時に実行する組込みシステムが見られるようになった．これには，多機能な汎用OSの恩恵を受けつつ，従来から利用されてきたリアルタイムOSがもつ信頼性やリアルタイム性といった性質を合わせ持ったシステム構築を行いたいという要求が根底にある．複数のOSを同時に実行する技術として，ハイブリッドOS方式や仮想マシン方式がある．しかし，ハイブリッドOS方式ではリアルタイムOSを汎用OSから保護することができず，仮想マシン方式では実行時間オーバヘッドが大きいためリアルタイム性の保証が難しい．こうした問題を解決するために，セキュリティ支援ハードウェアを利用し，リアルタイムOSを保護しつつ，システム全体のリアルタイム性を保証する方式が提案された．この方式ではSafeGと呼ばれる小さなソフトウェアモジュールによって，シングルコア上で2つのOSが切り替えられる．

また組込みシステムでは，マルチコアアーキテクチャの導入が進んでいる．マルチコアアーキテクチャ上で複数のOSを同時実行するために，従来からとられてきた方法として，各コアで個別のOSを実行する方式がある．しかし，この方式ではOS間で同一コアを共有できず，マルチコアアーキテクチャを用いた負荷分散による性能向上を見込めない．またOS間で使用するリソースが保護できず，あるOSから他OSの使用するハードウェアやメモリ領域に対するアクセスを防ぐことができない．これに対してSafeGを用いた方式では，OS間の保護が可能であり，構築したシステムで組込みシステムに不可欠なリアルタイム性を保証できる．

そこで本研究ではSafeGをマルチコアアーキテクチャ用に拡張し，組込みシステムに適したデュアルOS環境を提案，実装した．SafeGをマルチコアアーキテクチャに適用するにあたり，コアごとに異なるSafeGを用意する方法と，単一のSafeGイメージを複数コアから共有する方法が考えられた．前者はコア数に比例したSafeGのためのメモリ領域が必要であり，OSに対しても多くの改変が必要である．後者はSafeGが各コアごとに異なる処理をするための改変が必要で，そのための実行時間オーバヘッドおよびメモリ領域増加の可能性がある．本研究では，システム全体への改変が少ない後者の方法を選択した．これを実現するためのSafeGへの拡張として，OS切り替えに必要なレジスタ情報の退避領域をコア数分追加した．また，SafeGの起動処理，割込みハンドリングおよびOS切り替えの実行パスに，ロードすべき退避領域を判定する変更を加えた．このSafeGを用いたマルチコアアーキテクチャ上のデュアルOS環境の実現にあたり，OSの配置や，OSのスケジューリングを考慮し3種類の実装方式を提案した．提案した実装方式について比較および検討を行った上で優れた1つの実装方式を選択し，実装を行った．

評価実験として，マルチコアアーキテクチャ向けのOSであるFMPカーネルを，2つ同時に実行した．まずSafeGのプログラムサイズおよび実行時間オーバヘッドを計測した．この結果，SafeGをマルチコアアーキテクチャに適用することで生じる，実行時間オーバヘッドの増加は約0.2μsに，データ領域の増加は約1KBに抑えられたことを確認できた．また，同時実行されるFMPカーネルのスピンロック取得時間および，プロセッサ間割込みを使用したAPIの実行時間を計測し，SafeGをマルチコアアーキテクチャに適用するにあたって，より効率的なシステムを構築するために解決すべき課題を提示した．