様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成２５年　６月　５日現在

機関番号：１３９０１
研究種目：若手研究(B)
研究期間：2011　～　2012
課題番号：23700035
研究課題名（和文）
組込みマルチプロセッサシステムの高信頼性を実現するデュアルＯＳアーキテクチャ
研究課題名（英文）
Dual OS architecture for reliable multiprocessor embedded system.
研究代表者
本田　晋也（SHINYA HONDA）
名古屋大学・情報科学研究科・准教授
研究者番号：20402406

研究成果の概要（和文）：
本研究では、マルチコアシステムでリアルタイム OS(RTOS)と汎用 OS を同時実行可能な**組込みマルチプロセッサシステムの高信頼性を実現するデュアルＯＳアーキテクチャ**である SafeG-MP を開発した。本環境を用いることで、情報処理とリアルタイム処理の混在する組込みシステムに必要な要件を満たすと共に、近年組込みシステムで採用の進むマルチコアシステムの利用が可能である。SafeG-MP は、RTOS のリアルタイム性を保証しつつ、各コアの使用率を最大化するように設計を行った。そのために、各コアの OS スケジューリングを非同期に行い、 RTOS の処理があるコアでは、RTOS の処理を優先実行する。しかしながら、こうしたスケジューリング方式を採用することで、汎用 OS で性能低下を生じる。性能低下問題は、同期処理の遅延(LHP 問題)と負荷の各コアへの不均一な割り当て(不均等負荷問題)に大別できる。本研究では、双方の性能低下問題を抑止するための手法に関しても提案・実装を行い、評価を行った。実機での評価を行った結果、SafeG-MP により RTOS と汎用 OS が安全に同時実行可能 であり、汎用 OS について提案手法の導入により性能低下抑止を確認できた。

研究成果の概要（英文）：
SafeG-MP is a virtualization environment that allows a real-time operating system (RTOS) to run concurrently with a general-purpose operating (GPOS) on a multi-core embedded system. SafeG-MP schedules the workload of each core between both OSs independently. When both Oss are ready to run on a certain core, the RTOS is executed with higher priority. Unfortunately, such scheduling algorithm has performance issues on the GPOS: an increased synchronization delay, and a load imbalance among cores. We propose a technique to address both issues. We implemented and evaluated it on a physical platform, confirming its effectiveness at mitigating the GPOS performance loss.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	3,200,000	960,000	4,160,000

研究分野：情報額
科研費の分科・細目：ソフトウェア
キーワード：オペレーティングシステム

１．研究開始当初の背景
近年、組込みシステムは、高機能化と複雑化が進んでおり、制御系の機能と情報系の機能の両方が要求されるシステムが増えている。例えば、カーナビゲーションシステムでは、一台のコンピュータ上で、ナビゲーション等の情報系の機能に加えて、ブレーキやエンジン等と連携する制御系の機能も実行する必要がある。制御系の機能は情報系の機能と比較して、高い信頼性やリアルタイム性が要求される。 複雑な情報系の機能を効率良く実現するためには機能が豊富な UNIX 等の汎用 OS が、制御系のリアルタイム性を実現するためにはリアルタイム OS が必要となる。

近年、汎用コンピュータと同様に、組込みシステムの分野においても、マルチプロセッサの利用が進んでいる。そこで、マルチプロセッサを用いて、情報系(汎用 OS)と制御系(リアルタイム OS)をそれぞれ異なるプロセッサで実行する方法が考えられる。しかしながら、この方法は、次の問題がある。

1.制御系が情報系から保護されていない
情報系 OS は高機能であり規模が大きく機能追加が継続的に行われるため、制御系 OS と比較して信頼性が低く、不具合が発生する確立が大きい。このことは、Windows や Linux のセキュリティパッチが毎月リリースされていることからも明らかである。

制御系 OS と情報系 OS はそれぞれのプロセッサにおいて、同じ特権レベルで動作するため、情報系 OS に不具合が発生した場合、その問題が制御系に波及してしまう。

2.リアルタイム性とスループットの両立が困難
1 の問題を解決する方法として、申請者がこれまで開発したシングルプロセッサ向けのハイブリッド OS 技術を用いて、制御系を情報系から保護する方法がある。しかしながら、既存手法では、制御系の処理が発生すると、情報系の処理を中断して実行する。そのため、情報系がプロセッサ間の排他処理を実施している間に中断が発生すると、情報系の処理全体を止めてしまい、情報系のスループットを下げてしまう。

3.OS 間の通信の問題
制御系と情報系は合わせて一つのシステムを実現するため、両者の間では情報のやり取りが必要となる。しかしながら、既存手法では、OS 間の通信を実現する方法が提供されていない。

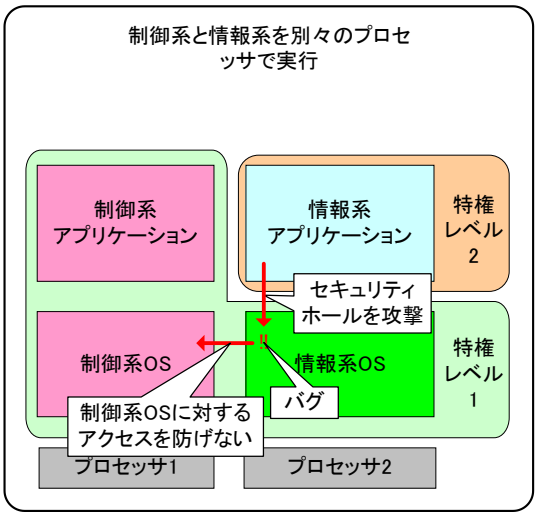

図 1： 提案手法適用前

２．研究の目的
本研究では、前章で提示した 3 つの問題を、以下のように解決する。

A)ハイブリッド OS 技術のマルチプロセッサ対応
申請者がこれまで開発したシングルプロセッサ向けのハイブリッド OS 技術をマルチプロセッサに拡張することにより、情報系を制御系より低い特権レベル動作させ、制御系を保護する。また、各プロセッサで制御系と情報系を同時に動作させることにより、システムのスループットの向上と、情報系の監視が実現できる。

B)OS スケジューリング手法
制御系のリアルタイム性と情報系のスループットを向上させるための OS スケジューリング方法と機構を実現する。具体的には、制御系のリアルタイム性を確保するためには、制御系の割込みや処理が発生した場合に負荷が低いプロセッサで制御系 OS を実行する方法や、情報系 OS がプロセッサ間の排他制御を行っている間はその処理を中断して制御系を実行すると情報系 OS 全体スループットが下がるため、可能な限りそのプロセッサでは制御系 OS を実行しない方法等がある。

C)OS 間通信
両 OS 上で動作するアプリケーションに対して、それぞれの OS の既存の API と近い形の

OS 間通信を定めて提供する。通信方法は、キューイングを行わない状態変数とキューイングするメッセージキューの 2 種類をサポートする。また、メッセージに優先度を持たせて、リアルタイム通信を可能とする。

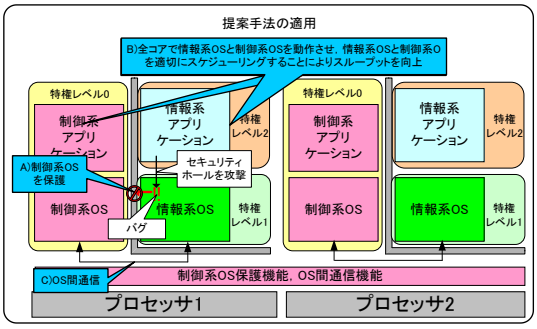

図 2：提案手法適用後

３．研究の方法

本研究は、以下の 3 つのサブテーマから構成される。

- ハイブリッド OS 技術のマルチプロセッサ対応
- OS スケジューリング手法
- OS 間通信

平成 23 年度と 24 年度の 2 年間で、機構の開発、実装、ならびに、事例評価を行った。事例の例題としては、情報系 OS として Linux ベースの Android を、制御系 OS として ITRON 系の OS を動作させ、情報系 OS で Web ブラウザやマルチメディア処理を実行し、制御系 OS で機器制御を行う例題を用いた。

（平成 23 年度）

平成 23 年度前期では、ハイブリッド OS 技術のマルチプロセッサ対応と OS 間通信の機構研究を行った。そして、平成 23 年度後期でそれぞれの実装と評価を行った。そして、申請者がこれまでに開発したシングルプロセッサ向けのハイブリッド OS をベースに実装する。

実装・評価と同時に OS スケジューリング手法について機構研究を行う。特に情報系のスループットを向上させるためのスケジューリング手法について重点を置いて研究を行った。

具体的には、制御系を実行する場合、情報系のスループットを極力下げないプロセッサを選択して動作させるようにした。例えば、情報系の処理がプロセッサ間の排他制御区間を実行している間は、可能な限りそのプロセッサでは制御系の処理を実行しない。

（平成 24 年度）

平成 24 年度は、平成 23 年度後期の評価をフィードバックして、ハイブリッド OS 技術のマルチプロセッサ対応、OS 間通信の二次実装を行った。また、OS スケジューリングに関しては、検討した機構を実装し評価した。

また、事例を用いた評価を実施した。評価においては、制御系のリアルタイム性の確保と情報系のスループットの実現に重点を置いて評価を行った。

４．研究成果

ハイブリッド OS 技術のマルチプロセッサ対応に関しては，最大 4 コア上で，RTOS と Linux を動作させるシステムを実現した。オーバヘッドも十分小さく、ほぼ理論値通りに押さえることができた。

OS スケジューリング手法に関しては，汎用 OS で発生する、同期期処理の遅延(LHP 問題)と負荷の各コアへの不均一な割り当て(不均等負荷問題)に対して、それぞれ軽減する手法を提案し、実装と評価を行った。本成果に関しては、現在論文としてまとめ学会誌に投稿中である。

OS 間通信に関しては、OS 間で安全な通信を実現するための通信仕様を定め、実装と性能評価を実施した。

なお，ハイブリッド OS 技術のマルチプロセッサ対応と OS 間通信に関しては，開発した成果はオープンソースとして、TOPPERS プロジェクトから公開した。
（http://www.toppers.jp/safeg.html）
OS スケジューリング手法に関しても、今後オープンソースとして公開する予定である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

D. Sangorrin, S. Honda, H. Takada, "Integrated Scheduling for a Reliable Dual-OS Monitor", 情報処理学会論文誌, (ACS 23), Vol.5, No.2, pp.99-110, 2012.（査読有）

D. Sangorrin, S. Honda, H. Takada, "Reliable and Efficient Dual-OS Communications for Real-Time Embedded Virtualization", コンピュータソフトウェア, Vol.29,No.4, pp. 182-198, Nov 2012.（査読有）

〔学会発表〕（計２件）
太田貴也，Daniel Sangorrin，本田晋也，高田広章， 組込みマルチコア向け仮想化環境における性能低下抑止手法，情報処理学会第 123 回 OS・第 27 回 EMB 合同研究発表会，東京，2012 年 12 月 5 日.

Daniel Sangorrin, Shinya Honda and Hiroaki Takada, ″Reliable Device Sharing Mechanisms for Dual-OS Embedded Trusted Computing″, Proceedings 5th International Conference on Trust and Trustworthy Computing, pp. 74-91, Vienna, Austria, Jun 14 2012.

〔その他〕
研究成果である組込みシステム向け仮想化 SystemBuilder の公開ページ
http://www.toppers.jp/safeg.html

６．研究組織
(1)研究代表者
本田 晋也（HONDA SHINYA）
研究者番号：20402406

(2)研究分担者　なし

(3)連携研究者　なし