様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１９　日現在

機関番号：　１３９０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６３３００６２

研究課題名（和文）高信頼組込みリアルタイムシステム向けパーティショニング機構の実現

研究課題名（英文）The partitioning mechanism and RTOS for high reliability system

研究代表者
本田　晋也（Shinya, Honda）

名古屋大学・情報学研究科・准教授

研究者番号：２０４０２４０６

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：近年、車載システムなどの高い信頼性が求められる組込みシステムの高機能化や機能統合により、単一の組込みコンピュータ内に安全度水準が異なる複数のアプリケーションを実行するため、メモリ保護や時間保護といったパーティショニング機構を用いてシステムを構築する必要がある。
本研究では、高信頼性システム向けの時間パーティショニング機構の提案とその機構を持つリアルタイムOSであるパーティショニングOSを実現した。研究成果はオープンソースとして一般に公開している。

研究成果の概要（英文）：To integration of different safety integrity level software in the single embedded computer, a partitioning mechanism such as memory and time protection is required for high reliability system.
In this work, the time partitioning mechanism for high reliability system is proposed. We realized the partitioning OS with proposed time protection mechanism. This partitioning OS is open to the public as open source software.

研究分野：　情報科学

キーワード：　組込みシステム　RTOS　高信頼システム　パーティショニング

１．研究開始当初の背景

近年、車載システムなどの人命に関わる高い信頼性が求められる組込みシステムは、ISO26262 や IEC61508 といった、機能安全規格への対応が求められている。機能安全規格へ対応するには、機能の重要度に応じて安全度水準（SIL/ASIL）を割り付け、その安全度水準に応じて、機能安全規格で定められた開発プロセスに従って開発を行わなければならない。

1 つのシステム（コンピュータシステム）は、複数の機能（アプリケーション）で構成されていることが一般的である。特に車載システムではコンピュータシステムである ECU の増加が問題となっており、異なる ECU で実現されていたアプリケーションを一つの ECU で実現する ECU 統合が推進されている。アプリケーション毎に重要度が異なっている場合でも、それらが同一のシステム上で実現された場合は、最も重要度の高いアプリケーションの安全度水準でシステム全体を開発しなければならないことや、あるアプリケーションを変更した場合、その変更が他のアプリケーションに対して影響を与えていないか確認するため、システム全体を再検証する必要があり、開発・検証コストの増加を招くという問題がある。

この問題を解決する方法として、リアルタイム OS が提供するパーティショニング機構を用いて、各アプリケーションの独立性を実現し、各アプリケーションを本来の安全度水準で開発可能とする方法が挙げられる（図 1）。パーティショニング機構には、メモリ保護、時間保護、アプリケーションの再起動等があるが、現状産業界で使用されているリアルタイム OS には次の問題がある。

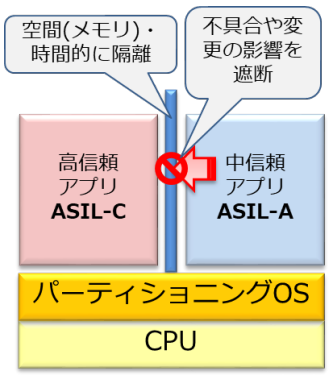

図1 複数アプリの実行と
パーティショニング

(1)時間保護の単位が小さい

車載システム向けのリアルタイム OS の標準仕様である AUTOSAR OS では、時間保護とメモリ保護を提供している。メモリ保護はパーティショニング機構として問題ないが、時間保護は個別のタスクや割込みハンドラの実行時間の超過を監視する実行時間監視の機能は提供するが、それらがまとまったアプリケーションの単位に対しての時間保護は提供しない。そのため、あるアプリケーションに含まれるタスクが変更されてその実行タイミングが変わった場合（実行時間は超過していない場合でも）、他のアプリケーションのタスクの実行タイミングが変化する可能性がある。

(2)高速応答性を実現する時間保護仕様がない

航空機向けのリアルタイム OS の標準仕様である ARINC653 では、時間保護の機構として、システムに周期を設けて（システム周期）、その間の時間を各アプリケーションに割り当ててアプリケーション単位にスケジューリングを行う周期実行ポリシーを提供している(図 2)。この機構は、厳密な時間保護の方式であり、割込みを一切使用することができない。航空機はその性質から高速な応答性が要求されないため割込みが無くても問題ないが、車載システムでは、マイクロ秒単位の割込み応答が必要となるため、そのままでは使用出来ない。

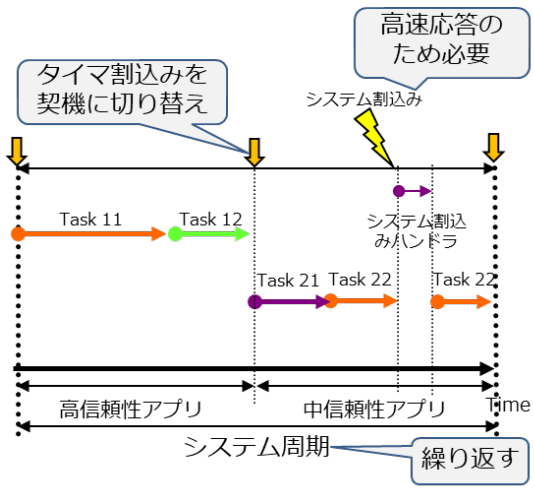

図2 シングルスレッドプロセッサ
における時間保護

２．研究の目的

本研究の目的は、車載システムなどの高い信頼性が求められる組込みシステム向けのパーティショニング機構の実現とその機構を持つリアルタイム OS であるパーティショニング OS の実装を開発することである。本パーティショニング機構を用いることにより、複数の異なる安全度水準のアプリケーションを一つのコンピュータシステム上で実行することが可能となる。これにより、システム全体の開発・検証コストを下げることがで

きる。研究成果は学術論文として発表することに加えて、社会で広く活用されるようオープンソースとして公開することにより、安心安全な社会の実現に貢献する。

３．研究の方法

A) 高信頼組込みリアルタイムシステム向けの時間保護機能

(1)(2)の問題を解決するため、周期実行ポリシーをベースに高速応答性を実現する時間保護機構を実現する。具体的には、システム割込みと呼ぶ、どのタイミングでも受け付け可能な割込みをサポートする(図 2)。時間保護のため、システム割込みの実行時間や受け付け回数は制限する。

B)高信頼組込みリアルタイムシステム向けパーティショニング OS の実現

A)で実現した時間保護機能と、既存のメモリ保護機能を統合して、高信頼組込みシステム向けパーティショニング OS を実現する。このパーティショニング OS により、複数の異なる安全度水準のアプリケーションで構成されたシステムを実現することが可能となる。

複数のアプリケーションを独立に実行する手法として、組込みシステム向けの仮想マシンの研究開発が盛んに行われているが、これらの手法は複数の OS を可能な限り改変無くかつ低オーバヘッド実行することを第一にしており、パーティショニングを実現することを目的としていない。そのため、手法によっては、メモリ保護も実現されていない場合がある。また、時間保護については、ラウンドロビンスケジューリングで実行するだけであり、個々のアプリケーションの時間要件に応じたスケジューリングはサポートしてない。また、仮想マシンを用いることにより実行オーバヘッドが大きいという問題がある。それに対して、提案手法は、アプリケーション間のパーティショニングの実現を第一目的としており、機能安全規格への対応が求められている実社会の要望に答える研究である。また、複数の OS を実行することには目標としていない。そのため、各アプリケーションの実行には仮想マシンを使用しないため、実行オーバヘッドを低く抑えることが可能である。

４．研究成果

高信頼組込みリアルタイムシステム向けの時間保護機能としては、割込みをサポートした時間保護機構を検討して実現した。

高信頼組込みリアルタイムシステム向けパーティショニング OS の実現として、提案した機構を実装した RTOS をオープンソースとして TOPPERS プロジェクトから公開した。ベースの RTOS としては、車載システムの標準仕様である ATUOSAR OS を用いた。さらに、マルチコアに対応させた（図 3)。

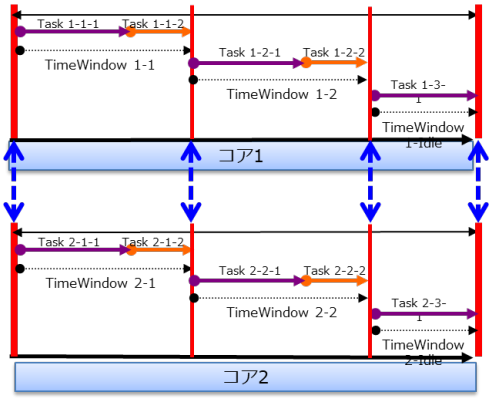

図3 高信頼組込みリアルタイムシステム向けの時間保護機能
マルチコア拡張

当初予定では、マルスレッド CPU 向けの機構を検討する予定であったが、マルスレッド CPU の開発がキャンセルとなったため、代わりにシングルスレッド CPU 向けの仮想マシン機構を用いた仮想マシンの検討と実現を行った。仮想マシンは、車載システム向けのマイコンが持つ仮想化機能を用いた。実現した仮想マシンは車載システムの要件である、リソースの使用量、実行オーバヘッドの低減、高いリアルタイム性を実現するために、仮想マシンとホストの RTOS を一体化した構成としている（図 4)。安全度水準が高い車載アプリケーションは、ホストの RTOS で実行し、安全度水準が低い車載アプリケーションは仮想マシン内で実行する。提案した機構を元に設計及び実装を行い評価を行った。評価の結果、提案機能は車載システム要件を満たしていることを確認した。

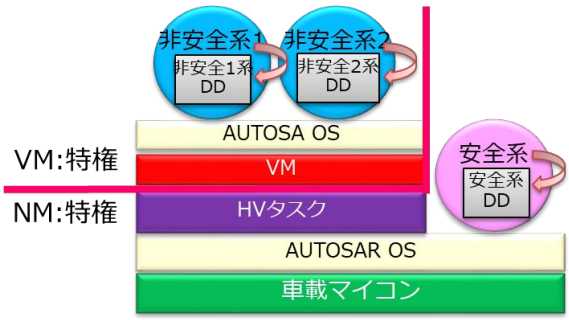

図4 車載システム向けの仮想マシン

また、実現した仮想マシンを用いて割込み応

答時間を高速化する手法を検討・実現した。車載システムの高機能化により、これまで社内で開発したソフトウェアのみを用いて開発していたシステムに対して、外部で作成されたソフトウェア（外部ソフトウェア）を組み合わせてシステムを実現したいという要求が出ている。外部ソフトウェアは安全度水準が低い一方、高い応答性が要求される場合がある。この様な外部ソフトウェアを既存のソフトウェアと分離して実行する方法として、仮想マシンを用いる方法がある。仮想マシンの実現は実行オーバヘッドが問題となるが、近年車載システムにおいてもハードウェア仮想化支援機能を搭載したプロセッサが登場しており、それらをサポートした仮想マシンモニタも開発されている。本研究では、ハードウェア仮想化支援機能を利用した仮想マシンを用いて、外部ソフトウェアの分離と高い割込み応答性を実現する機構を実現した。実現した機構は、VM-ISR0 と VM-ISR1-と呼ぶ、通常より高い優先度の割込みハンドラを実現可能である。これらのハンドラは、仮想マシン内で実行されるが、ネイティブマシン経由で呼び出されることで、高速性を実現している（図 5）。

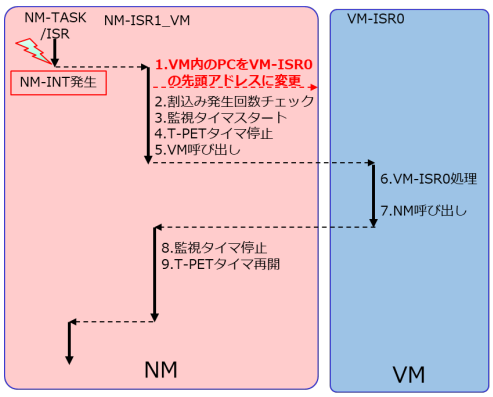

図5 VM-ISR0の呼び出しシーケンス

さらに、保護機構を持った RTOS 上で動作する割込み応答を高速化するフレームワークを実現した。
近年、車載システムの複雑化・高性能化が進んでいる。複雑化に対応するため、 AUTOSAR プラットフォームの使用が一般化しており、更に機能安全への対応のため、 RTOS の保護機構によるパーティショニングを行うことも多い。一方、高性能化として高速な割込み応答が求められているが、 RTOS が提供する通常の割込み機構では要件を満たさないという問題がある。そこで、 RTOS 実行中も割込みを受付可能な、 OS 管理外の割込みと呼ばれる機構により、実現する手法が用いられている。しかしながら、 OS 管理外の割込みは、メモリ保護や時間保護が有効でないという問題がある。本研究では、 RTOS と独立した OS 管理外割込みの保護機構を提案し、提案機構を実装して、実行オーバヘッドや RTOS の変更量等を評価した。提案機構は、OS 管理外の割込みである ISR1 として動作し、各種監視・保護機能を有効にして低い安全度水準の短周期処理を実行することにより、高速な割込み応答時間と保護を両立する（図 6）。提案機構を実装し評価した結果、非機能要件も満たすことを示した

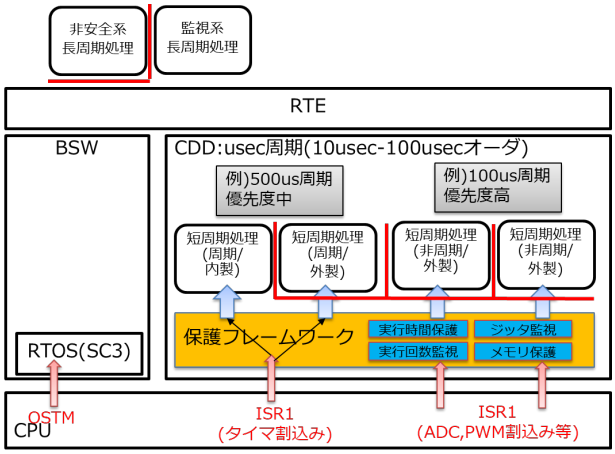

図6 車載システム向けの OS管理外割込みパーティショニング機構

5．主な発表論文等

〔学会発表〕（計　4 件）

1. 本田晋也，岡部亮，攝津敦，車載システム向けの OS 管理外割込みパーティショニング機構，第 47 回組込みシステム合同研究発表会(ETNET2018)，島根県隠岐郡，Mar 2018.
2. 本田晋也，岡部亮，攝津敦， 車載システム向けの仮想マシンの割込み応答性向上手法，情報処理学会研究報告，Vol.2017-SLDM-179,No.14，pp. 1-6，沖縄，Mar 2017.
3. 河田智明，本田晋也， TrustZone for ARMv8-M を利用した軽量メモリ保護 RTOS，Vol.2017-SLDM-179,No.14，pp. 1-6，沖縄，Mar 2017.
4. 本田晋也，鈴木均，樋口正雄，福井昭也，"車載システム向けハードウェア仮想化支援機能による RTOS 一体型仮想マシンモニタ"，情報処理学会研究報告，Vol.2017-OS-139,No.9，pp. 1-7，福岡，Mar 2017.

〔その他〕

1. 研究成果である，パーティショニング OS のソースコード公開用ページ
   http://www.toppers.jp/atk2-e-download.html

6．研究組織

(1)研究代表者

名古屋大学・情報学研究科・准教授
本田 晋也（HONDA SHINYA）
研究者番号：20402406