平成 19 年度
実績報告

「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」
平成 18 年度採択研究代表者

中島　達夫

早稲田大学　理工学術院　教授

高機能情報家電のためのディペンダブルオペレーティングシステム

1. 研究実施の概要

本提案では，既存のソフトウエア資産を有効に利用しながら，システム全体の信頼性,制御系と情報系処理の融合，次世代の超高機能情報家電構築へ向けた機能拡張性を大幅に向上する情報家電向け仮想実行環境の構築をおこなう．本提案において開発する超高機能情報家電向け仮想実行環境は，現状の Linux を用いた場合の開発においてアドホックになっている障害管理，入出力管理，リソース管理，マルチコア管理を共通フレームワークとして提供することにより，コストを増加させず信頼性や機能拡張性を向上する．

本年度は、各コンポーネントのプロトタイプシステムの開発をおこない、提案するアイデアの有効性の検証をおこなった。また、全チームの成果を統合するため P-Bus との融合に関する検討をおこなった．

2. 研究実施内容

本提案では、診断回復サブシステム、高信頼制御用 OS サブシステム、動的機能分散管理サブシステム、マルチコア仮想化サブシステムの 4 つのサブシステムの構築をおこなう。

1 つ目のサブシステムである診断回復サブシステムは、システム全体の診断をシステマティックにおこなうことを可能とする。2 つ目の超高信頼制御用 OS サブシステムは I/O 管理や診断回復サブシステムの信頼性を向上する基盤を提供する。3 つ目の動的機能分散管理サブシステムはマルチコア上で複数の OS 間の動的スケジューリングを管理する。4 つ目のマルチコア仮想化サブシステムは、マルチコア上で動作する複数の OS のアイソレーションを行なう。

以下、各サブシステムに関する今年度の研究実施内容の概要に関して述べる．

診断回復サブシステム:

本年度は、昨年度開発したプロトタイプシステムの改良をおこなった. 診断回復サブシステムのプロトタイプシステムは ia32 プロセッサ上の L4 オペレーティングシステム上に構築している。本プロトタイプシステムは、Linux カーネル内のデータ構造の一貫性を監視し、非一貫性を発見した場合は、一貫性を回復するように修復処理を実行する. 現状の実装では、Linux カーネル内に、各データ構造をモニタリングするためと、修復するためのカーネルモジュールを追加し、それらのモジュールを L4 オペレーティングシステム上に実装した監視システムにより制御するようにしている。

有効性を示すケーススタディとして攻撃を受けたマシンのプロセスサブシステムの修復が可能なことを示した. また、データ構造をモニタリングするプログラムを容易に作成するための仕様記述手法に関する検討もおこなった。来年度は、SH4 プロセッサで動作する動的機能分散管理サブシステム上に実装する。また、Linux 内のデータ構造のモニタリングを最適化するため、Linux のカーネルスペースをメモリマップを用いて L4 オペレーティングシステム上で動作する監視システムから直接アクセス可能とするなどの最適化をおこなう。

超高信頼制御用 OS サブシステム:

本年度は、昨年度のプロトタイプシステムの改良と L4 オペレーティングシステムの SH4 上への実装をおこなった。

制御用 OS の信頼性を高めるためのミドルウエアの構築をおこなった. 本システムは ia32 プロセッサ上の L4 オペレーティングシステム上にプロトタイプシステムとして構築されている. 本システムは、異常時に回復をおこなうためのチェックポイント機能とエラーを仮想化するための機能から構成される. 本年度は、有効性を示すためにデバイスドライバの信頼性を向上するためのフレームワークの構築をおこなった.

また、標準ハードウエアプラットフォーム上に移行するために、L4 オペレーティングシステムを SH4 上への実装をおこなった。また、SH4 プロセッサで動作する動的機能分散管理サブシステム上で L4 オペレーティングシステムと Linux カーネルが同時に動作するようにシステム全体の変更をおこなった。来年度は、超高信頼制御用 OS サブシステム全体を SH4 プロセッサ上に動作する動的機能分散管理サブシステム上に移植をおこなう。また、超高信頼制御用 OS サブシステム上で診断回復サブシステムを動作するように改良をおこなう。

動的機能分散管理サブシステム:

SH4 上のシングルプロセッサ上の仮想化サブシステムとして実装をおこなった。本システムは、L4 オペレーティングシステムと Linux オペレーティングシステムを1つのプロセッサ上に同時に実行することを可能とする. 動的機能分散管理サブシステムは独自のスケジューラを持ち、複数のオペレーティングシステムをそれぞれのアプリケーションの優先度に応じて実時間性を失わずに実行することを可能とする. また、低優先度の割り込みが高優先度のプロセスの実行を妨げないことを保証する.

本システムの有効性を示すために、Linux カーネルを異常発生時に容易に再起動可能となることを示した．つまり、Linux カーネルの外部からカーネルを強制的に再起動することを可能とした．来年度は、SH4 マルチコアプロセッサ上で動作するようにシステムの拡張をおこなう。

マルチコア仮想化サブシステム:

本年度は、昨年度の x86 上のプロトタイプの拡張と SH4 上への実装を行なった。

マルチコアへの対応を調査検討するため、x86 上のプロトタイプ実装を拡張し、デュアルコアプロセッサ上に実装を行なった。この拡張では、マルチコア仮想化サブシステムが CPU コアを管理し、各コアに Linux オペレーティングシステムを割り当てブートさせることを可能にした。マルチコア仮想化サブシステムが CPU コア、メモリ、割り込みの割り振りなどの資源管理を行なうことで、マルチコアプロセッサ上で動作する複数オペレーティングシステムのアイソレーションを可能にする。

また、標準ハードウェアプラットホームに対応するため、SH4 シングルプロセッサ上に実装を行なった。SH4 はプロセッサの提供する保護レベルが 2 レベルのみであり、また固定された仮想メモリ領域の属性、ソフトウェアアップデート TLB による仮想記憶の実現、レジスタバンクの提供など、x86 とは異なるプロセッサアーキテクチャを持つ。これらに対応するように、マルチコア仮想化サブシステムを設計、実装した。Linux オペレーティングシステムには、そのカーネルのソースコードに数行の変更を加えるのみで、マルチコア仮想化サブシステム上で動作させることができた。

3. 研究実施体制

(1)「早稲田大学」グループ

①研究分担グループ長:中島　達夫(早稲田大学、教授)

②研究項目

・診断回復サブシステム、高信頼制御用 OS サブシステム、動的機能分散管理サブシステム

(2)「追川」グループ

①研究分担グループ長:追川　修一(筑波大学、准教授)

②研究項目

・マルチコア仮想化サブシステム