

「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、既存のソフトウェ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、領域内の他のチームと情報交換をおこない、最終的に全体を1つのものとしてまとめられるように全体コンセプトを提案した。また、来年度以降の開発において重要となる基幹技術に関する妥当性を検証するためのプロトタイプ開発をおこなった。来年度は、組込みプロセッサを用いてより実用的なプロトタイプ開発を進める。

2. 研究実施内容

本年度は他のチームの研究成果と統合を可能とするための議論を進め全体のアーキテクチャを明確にした。また、全体アーキテクチャの中における本提案が開発するシステムの位置づけを明確にした。

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が、それぞれの各サブシステムが提供する機能を明確にする必要がある。そのためには、それぞれのサブシステムの簡単なプロトタイプを作成し、問題点を明確にする必要がある。本年度は、インテルの ia32 アーキテクチャ上に各サブシステムの構築をおこなった。

診断回復サブシステムは、ハードウェアやソフトウェアの障害を統一的に管理するシステムであるが、本年度は L4 マイクロカーネル上にプロトタイプシステムを構築し、どのようなタイプの異常を検出し、回復することを可能としていくかに関して検討した。特に、Linux カーネル内のデータ構造の振る舞いに着目し、ブラックボックスモニタリングとホワ

イトボックスモニタリングの利点を統合したハイブリッドなモニタリング手法に関して検討をおこなった。データ構造に注目することにより、異常が発生した場合は異常が発生したデータ構造を修復することにより、異常検出と回復を統合できる可能性がある。また、診断回復サブシステム自体の信頼性がシステム全体の信頼性を向上する場合非常に重要なポイントとなる。そのための基盤として高信頼制御用 OS サブシステムが利用可能かに関して検討をおこなった。

高信頼制御用 OS サブシステムは、各コンポーネントの再起動を容易に実現可能とする制御処理向けの OS である。OS は各コンポーネント間の依存関係を管理し、あるコンポーネントの障害が発生すると他の依存関係を持つコンポーネントも自動的に再起動する。本年度は、L4 マイクロカーネル上に簡単なシステムを構築して実用的なシステムを構築する際の問題点を明らかにした。具体的には、各プロセスのクラッシュを検出するための機能と各プロセスのエージングを制御するためのプロアクティブリカバリシステムの開発をおこなった。多くの複雑なシステムでは、異常が発生した場合に実際に何が起きているかを分析することが極めて困難であることが多い。そのため、問題が発生する前にプロアクティブリカバリを用いてシステムを回復することはシステム全体の信頼性を飛躍的に向上する可能性がある。

動的機能分散管理サブコンポーネントはマルチコアチップ上に複数の OS を動的に機能分散するための機能を提供する。本年度はマイクロカーネル上に複数の OS を動作させても実時間制約を満足するためのメカニズムを実装した。従来の機能分散は各機能を異なる CPU に割り当てていたが、CPU 数が少ない場合は、複数の機能を同一の CPU に割り当てる必要がある。本年度は、シングルコアチップを対象に簡単な実験をおこない問題点を明らかにすることにより、次年度以降に開発するマルチコアチップをターゲットとしたシステムを開発する上でのノウハウの獲得をおこなう。具体的には、ia32 のデュアルコアシステム上で Linux と L4 を同時に動作するシステムの構築をおこなった。本システムでは、1 つ目の CPU で L4 を起動する、L4 はシステム全体の物理メモリを管理し、そのうちの一部のメモリを 2 つ目の CPU で動作する Linux が使用可能なようにする。また、割り込み処理を両方の OS で使用可能なように割り込みハンドラの仮想化をおこなった。さらに、L4 上にハードディスクデバイスドライバを開発し、Linux カーネルからアクセス可能とするためのスタブを作成した。これにより、L4 上のデバイスドライバがクラッシュした場合でも Linux カーネルはクラッシュしないためシステム全体の信頼性が向上することが実証された。

マルチコア仮想化管理サブシステムは、ia32 上で動作する仮想マシンモニタの設計を通して仮想化によるオーバヘッドの考察を行った。特に、ハードウェアが仮想化の実現に必要な機能を提供しない場合として、プロセッサの持つ特権レベルの数が十分でない場合に生じる問題点について、実際に仮想マシンモニタの試作を通して検討した。通常のオペレーティングシステムは、これらのうち 2 レベルのみをカーネル実行用、ユーザプログラム実行用に使用する。従って近年開発されたプロセッサの多くは特権レベルとして 2 レベル

しか提供していないものが多い。しかし、ia32 プロセッサは特権レベルとして 4 レベル提供しているため、仮想マシンモニタの実行にカーネルとは別の特権レベルを使用することが可能である。近年開発された仮想マシンモニタは、このように 3 レベルの特権レベルを使用している。マルチコア仮想化管理サブシステムは、特権レベルとして 2 レベルしか提供していないプロセッサもサポートするため、ia32 プロセッサを用いて特権レベルを 2 レベルしか使用しない仮想マシンモニタを試作し、仮想メモリアーキテクチャを用いることで、低レベル仮想マシンにおいて仮想的にプロセッサの特権レベルをエミュレーションでできることを明らかにした。

本提案により開発するシステムと他のチームが開発するシステムとの関係を明確にすることも本年度の計画では重要である。特に、プロジェクト全体で使用するプラットフォームの検討や中間評価でおこなうデモンストレーションに関する議論をおこなった。

来年度は、本年度の研究成果を踏まえて、システム全体のアーキテクチャの見直しをおこなう。また、組込みプロセッサを利用したプロトタイプシステムを構築することで、組込みシステムにおいて使用する場合の問題点の検討をおこなう。

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(筑波大学大学院 助教授)

②研究項目

- ・ マルチコア仮想化サブシステム