

OS技術は品質向上に貢献するか？

早稲田大学
基幹理工学部 情報理工学科
中島 達夫

社会安全のための組込みLinux



コード量が爆発して稀にしか実行されない
コードのバグを取りきれない

- 組込み機器は我々の生活を豊かにしたり、生活の安全を守ったりする。
- 機器の障害は社会に大きな影響を与える可能性がある。

基盤ソフトウェアの重要性

- 現状のシステムはどの程度過去から進歩しているのか？
 - 現在のシステムは過去の英知を本当に利用しているのか？
 - 実時間性能: 基本的な優先度逆転問題の扱い
 - セキュリティ: 古い部分と新しい部分の両方が混在
 - 障害に対する取り組み: フォールトインジェクション
 - 現状の組み込みソフトウェアは30年前のメインフレームソフトウェアと本質的に何が違うのか？
 - リソース制約等の条件をハードウェアの進化がカバーしてきた。
- 大規模ソフトウェアを高信頼に構築する
 - OSアーキテクチャ
 - ソフトウェア工学
 - 分散コンピューティング
 - ハイパフォーマンスコンピューティング
 - リアルタイムコンピューティング
 - ディペンダブルコンピューティング

どのようなことが問題となりそうか？

- オープンソースの品質の問題
- OSレベルでの信頼性の向上
- アプリケーションのアイソレーション
- OSインタフェースのカスタマイゼーション

- アプリケーションを変えたくない、カーネルも変えたくないが本音だけど、これでは問題は本質的に解決できない。
 - 技術的に最小限の努力でできることは何か？

オープンソースの品質の問題

- 多くのユーザにより利用されることにほとんどの問題は解決されている。
 - 使用頻度が少ない機能はバグが存在する可能性が高い
 - 以上の機能がある程度の頻度で使用されると障害の発生につながる。
 - 製品の数が多くなると問題が発生する確率も大きくなる。
 - そのため、必ずテストは必要となる。
 - カーネルの大きな変更があるとテストをやり直す必要がある。
- モジュール化、モジュールの細分化
 - モジュールは大きくなるとバグの発生率も大きくなる
 - カーネルを完全に作り替えるか、変更を最小限にしないとイケない。

OSレベルでの信頼性の向上

- 障害への対応、セキュリティ、リアルタイム
 - アプリケーションをアイソレーションされた複数のプロセスに分割することにより信頼性は大きく向上する
 - 障害が発生したプロセスのみを再起動する
 - プロセス毎に最小の権限を与える
 - 複数のサービスを同じスレッド上で実行しないようにする
 - 優先度逆転が最小限となるようにプログラムをすることにより応答性の低下を最小限とする。
- プロセス管理機能の強化
 - プロセス間の優先度の伝搬
 - プロセス毎の詳細な権限の割当
 - プロセスの障害監視が重要
 - プロセスグループの扱い
- OSインタフェースの変更が必要となる
 - 既存のOSが信頼性やセキュリティ面で問題が解決しないのはカーネルインタフェースの変更ができないからでは？

アプリケーションのアイソレーション

- 信頼できないアプリケーションを他のアプリケーションから分離する
 - 仮想マシン (XEN, Vmware)
 - 複数のハードウェアをエミュレーションする
 - 複数のOS分のリソースが必要
 - 仮想OS (Vserver, Jail)
 - アプリケーションからは複数のOSが存在するように見える
 - アクセス許可がないリソースはみえない
 - カーネルのカスタマイゼーションは困難

OSインタフェースのカスタマイゼーション

- スレッドの扱い
 - 周期実行、デッドラインミスの通知
- 障害の監視
 - プロセスの障害検出
- プロセス間通信
 - プロセス間のスレッドの優先度監視

次世代の組み込みOS

- 現状のOSが昔と大きく変わらないのはアプリケーションやハードウェアに本質的な大きな違いがないから。
 - 小型化、低価格化: 将来もこの前提は正しいか?
- ハードウェアの変化
 - ヘテロジェニアスマルチコア
- アプリケーションの変化
 - 様々なインタラクションデバイスの統合
- OSに新しい機能が必要となっていく可能性が高い

将来へ向けて

- テスト技術、ソフトウェア設計技術、フォーマルメソッド等の技術はソフトウェアの品質向上に重要な役割を果たす。
 - 自動的なテストパターンの生成、プロダクトライン／コンポーネントアーキテクチャ、モデル検査
- しかし、ソフトウェアの品質はOSのインタフェースの出来具合にも依存している
 - カーネルAPIとそのセマンティクス
 - 非機能的要件を実現するための基本プリミティブ
 - 特に、ヘテロジェニアスマルチコアと多様なインタラクションデバイスは分散処理のリインベントを必要とする。
 - 新しいOSアーキテクチャの必要性

将来へ向けて

- 分野の複雑さに比例して関連するコミュニティの数も増えてきている。
 - オープンソース
 - 組込みシステム
 - ディペンダブルシステム
 - リアルタイムシステム
 - ハイパフォーマンスコンピューティング
 - 分散コンピューティング
 - OSアーキテクチャ
 - ユビキタスコンピューティング
 - インタラクションデザイン
- Linuxはヘルシンキ大学で開発された....
 - ヘルシンキ大学にはOS研究は存在しない。