TOPPERSにおける
高信頼ソフトウェアへの取組み

2010年12月3日

高田 広章

NPO法人 TOPPERSプロジェクト 会長

名古屋大学 大学院情報科学研究科 教授
附属組込みシステム研究センター長

Email: hiro@ertl.jp　URL: http://www.ertl.jp/~hiro/

TOPPERSプロジェクトとは?

TOPPERS = Toyohashi Open Platform for
Embedded and Real-Time Systems

プロジェクトの活動内容

- ITRON仕様の技術開発成果を出発点として，組込みシステム構築の基盤となる各種の高品質なオープンソースソフトウェアを開発するとともに，その利用技術を提供

  組込みシステム分野において，Linuxのように広く使われるオープンソースOSの構築を目指す!

プロジェクトの推進主体

- 産学官の団体と個人が参加する産学官民連携プロジェクト
- 2003年9月にNPO法人として組織化
- それ以前は，名古屋大学(2002年度までは豊橋技術科学大学)高田研究室を中心とする任意団体として活動

TOPPERSプロジェクトの狙い

決定版のITRON仕様OSの開発

- ITRON仕様がかかえる過剰な重複投資と過剰な多様性の問題を解決(または軽減)

次世代のリアルタイムOS技術の開発

- 組込みシステムの要求に合致するし，ITRONの良さを継承する次世代のリアルタイムOS技術を開発

  Linuxと類似のOSをもう１つ作っても意味がない！

- オープンソースソフトウェア化により産学官の力を結集

組込みシステム開発技術と開発支援ツールの開発

- 高品質な組込みシステムの効率的な開発を支援

組込みシステム技術者の育成への貢献

- オープンソースソフトウェアを用いた教育コースや教材を開発し，それを用いた教育の場を提供

高信頼ソフトウェアへの取組み

高信頼性のための機能を持ったRTOS

- TOPPERS/HRPカーネル，HRP2カーネル
- AUTOSAR OS仕様ベースの保護機能を持ったRTOS
- SafeG：汎用OSとRTOSを安全に共存させるハイブリッドOS

RTOSの開発プロセスの整備

- トレーサビリティの起点となる仕様書の整備
- トレーサビリティの取れた設計ドキュメントの整備へ

RTOSの検証技術の研究開発と適用

- TOPPERS/HRPカーネルに対する検証
- 新世代カーネルに対する検証スイートの整備
- 形式手法の適用

機能安全規格準拠のRTOS

- TOPPERS/ASP Safetyカーネル

TOPPERS/HRP2カーネル

位置づけ

- TOPPERS新世代カーネルの1つで，保護機能を持ったリアルタイムカーネル
- TOPPERS/HRPカーネルをバージョンアップしたもの

機能概要

- TOPPERS/ASPカーネルに以下の機能を追加
  - メモリ保護機能，オブジェクトアクセス保護機能
  - 拡張サービスコール機能，ミューテックス機能
  - オーバランハンドラ機能
- メモリ保護ユニットを備えたプロセッサを有効活用できる

開発状況・リリース計画

- 名古屋大学において開発が進行中
- 今月中に，TOPPERS会員向けの早期リリースを開始

AUTOSAR OS仕様ベースのRTOS

次世代車載システム向けRTOSの仕様検討及び開発に関するコンソーシアム型共同研究

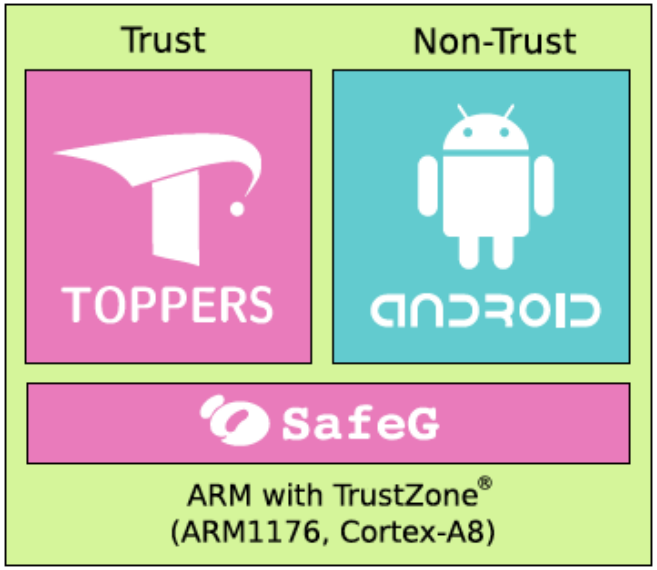
- 名古屋大学 組込みシステム研究センター（NCES）が呼びかけ，複数の企業の参加を得て研究開発を実施予定
- NCESの開発成果を利用して，AUTOSAR OS仕様をベースに，その問題点を修正したRTOS仕様と実装，検証スイートを開発
- 実装したRTOSは，TOPPERS/ATK2としてオープンソース化する計画
- 2011年4月に開始予定で，参加メンバを募集中

NCESのこれまでの開発成果

- AUTOSAR OS仕様をベースとしたRTOS仕様と実装，それをマルチコア向けに拡張したRTOS仕様と実装を開発
- 仕様案をTOPPERS会員向けに公開

SafeG

技術の概要



- 1つのマイクロプロセッサ上で，汎用OS（LinuxとAndroid）とRTOS（ASPカーネル）を安全に共存して動作させるデュアルOSモニタ
- ARM TrustZone技術を用い，RTOSをTrust状態，汎用OSをNon-Trust状態で実行
- 汎用OSにセキュリティホールがあり，特権モードで不正なプログラムが動作しても，RTOS側を保護できる

開発状況・リリース計画

- 名古屋大学において開発が進行中
- 今月中に，TOPPERS会員向けの早期リリースを開始
- 今後，マルチプロセッサ拡張などを計画

トレーサビリティの起点となる仕様書の整備

TOPPERS新世代カーネル統合仕様書

- μITRON4.0仕様をベースに，最近10年の新しい要求に対応できるように改良・拡張したカーネル仕様
- 下位ドキュメントとのトレーサビリティが取れるように，要求タグを付与する計画

2.6.3 タスクのスケジューリング規則

実行できるタスクは，優先順位の高いものから順に実行される【NGKI5001】．すなわち，ディスパッチ保留状態でない限りは，実行できるタスクの中で最も高い優先順位を持つタスクが実行状態となり，他は実行可能状態となる．

タスクの優先順位は，タスクの優先度とタスクが実行できる状態になった順序から，次のように定まる．優先度の異なるタスクの間では，優先度の高いタスクが高い優先順位を持つ【NGKI5002】．優先度が同一のタスクの間では，先に実行できる状態になったタスクが高い優先順位を持つ【NGKI5003】．すなわち，

TOPPERS/HRPカーネルに対する検証

TOPPERS/HRPカーネル

- TOPPERS/JSPカーネルに対して，メモリ保護やオブジェクトアクセス保護などの保護機能を追加
- 名古屋大学とJAXAの共同研究により開発
- JAXAがH-IIAおよびH-IIBロケットへの採用を決定

TOPPERS/HRPカーネルに対する検証

- JAXAがRTOSの高信頼性検証ガイドラインを策定
- それに従って，NEC通信システムがRTOSの高信頼性検証プロセスを構築し，TOPPERS/HRPカーネルに適用
- 約7000行のソースコードに対して，数万件のテストケースを開発

新世代カーネルに対する検証スイートの整備

TOPPERS/FMPカーネル向け検証スイートの開発

- 名古屋大学 組込みシステム研究センター（NCES）を中心とするコンソーシアム型共同研究により研究開発中
- テストプログラム生成ツール（TTG = TOPPERS Test Generator）を開発
  - TTGにより，テストプログラムの開発工数削減に加えて，テストケースの保守性・可読性の向上など，数々の利点を実現
- それを用いたテストケースを作成
  - FMPカーネル用APIテスト：約2500件のテストケース
- テストプログラムで実行が困難なパスを実行する命令セットシミュレータを開発中
- 共同研究終了の1年後にオープンソース化の予定

TOPPERS/ASP Safetyカーネル

概要

- (株)ヴィッツが機能安全規格IEC 61508 SIL 3に準拠したソフトウェア開発プロセスに基づいて開発したリアルタイムカーネル
  - ! (株)ヴィッツは，TÜV SÜDより，IEC 61508 SIL 3に準拠したソフトウェア開発プロセスの認証を得ている
- このリアルタイムカーネルを利用した製品に対して製品認証を得るために必要となる各種のドキュメントを含む

機能概要

- TOPPERS/ASPカーネルのサブセット

開発状況・リリース計画

- (株)ヴィッツにおいて開発が進行中
- 今月中に，TOPPERS会員向けの早期リリースを開始

成果物利用とプロジェクト参加のお誘い

- 開発成果物はウェブサイトから自由にダウンロードできますので，ぜひご利用ください
- プロジェクトの活動に参加したい方/活動を支援して頂ける方は，ぜひプロジェクトにご入会ください

HiQOS … High Quality Open Source

インダストリアルコントロールの新しいスタンダードへ

TOPPERSプロジェクトは，組込みシステム開発に有用な
高品質なオープンソースソフトウェアと教育コンテンツを開発し，
組込みシステム開発に新しいスタンダードを提案します

http://www.toppers.jp/