トップエスイー修了制作

RTOSスケジューリング機能の段階的詳細化によるモデル化

株式会社リプルズ　岩本信一　siwamoto@ripples.bz

RTOSにおける課題

組み込み機器用ソフトウェアは,
・製品出荷後の書き換えが通常不可能
・短納期であるためにテストによる検証が不十分
であるため，形式手法による検証が強く求められる.

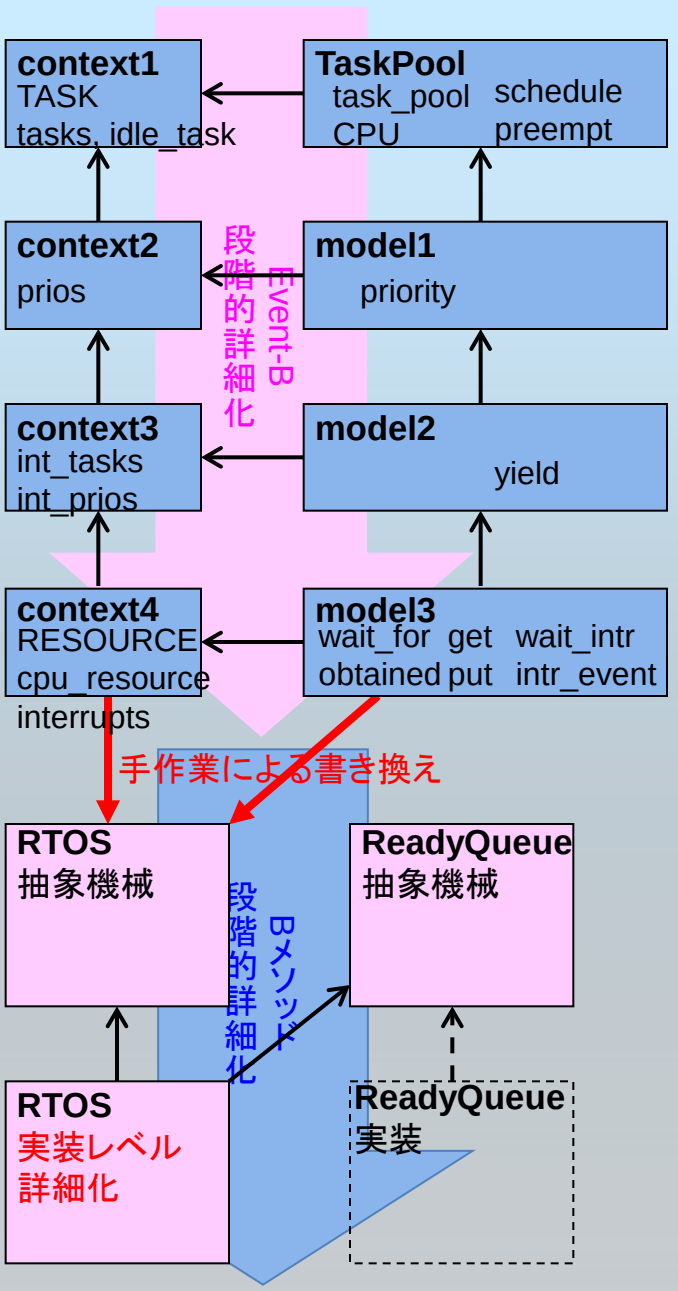
組み込み機器用のOSであるRTOSは形式的に検証されたものがほとんどない　→　利用に不安がある.

手法･ツールの適用による解決

既存のAPIやコードに形式手法を適用した例はある.

RTOSを形式仕様記述し，RTOSの仕様を検証しながら，コードを自動生成することで，形式的に検証済みのRTOSを得ることを試行する.
・Event-Bによる仕様の段階的詳細化
・Bメソッドによる実装レベルへの詳細化

RTOSスケジューリング機能の段階的詳細化



マルチタスキングの導入
マルチタスク環境下で、高々1個のタスクがCPUを獲得する

優先順位の導入
最も高い優先順位をもつタスクがスケジューリングされる

割り込み優先順位、割り込みタスクの導入

(割り込みも含めた)リソース(獲得、解放)の導入
割り込みタスクはcpuか割り込みを待つ
通常タスクはcpuか他資源を待つ

手作業による書き換え

ラウンドロビン導入
・ReadyQueueの組み込み

Event-B
・非形式的な要求から段階的に情報を抽出し，形式的なモデルを構成できる
・段階的詳細化をシステム解析/モデル化に使うことができる

Bメソッド
・Event-Bとの親和性が良い
・コード生成が可能である

形式仕様記述からコードが生成できる

今後の課題

・実用に耐えるRTOSを形式仕様記述から構築
・このRTOSを利用するアプリケーションが形式的に(自動)検証できるアプリケーション開発環境の開発