トップエスイー修了制作

組込みソフトウェアへの設計モデル検査の適用とPromelaコード生成の拡張

キヤノン株式会社　青木 仁志　aoki.hitoshi@canon.co.jp

開発における問題点

①ソフトウェアの大規模・複雑化によって網羅的な検証が求められてきている.
②SPIN/Promelaを利用したモデル検査により，網羅的な検証が可能になるが，Promelaの学習・記述工数や，設計モデルと検証モデルの乖離が問題となる.

手法・ツールの適用による解決

① SPINを利用したモデル検査により，モデル検査の有効性を確認する.
② 検証モデル作成にPromelaコード生成ツールの利用を検討し，ツールの適用可能性を検討する.

モデル検査による検証

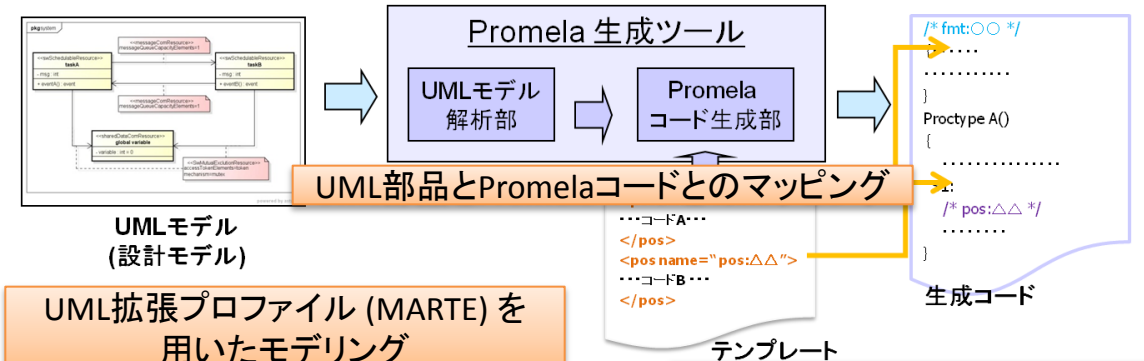
- 組込みデバイスドライバ (μITRON ベース) の検証モデルを Promela で記述
- 記述した検証モデルに対して SPINで検証を実施
  - 進行性
  - タスク間の状態の整合性
  - デバイス故障時の耐障害性

↓

- 2件の設計欠陥を検出
  - テストで発見が困難なケース

適用したPromela生成ツールの概要

Promela コード生成ツール [佐々木隆益: TopSE2010 修了制作] を適用



UML拡張プロファイル (MARTE) を用いたモデリング

テンプレートによるPromela合成

Promela生成ツールの適用検討と拡張

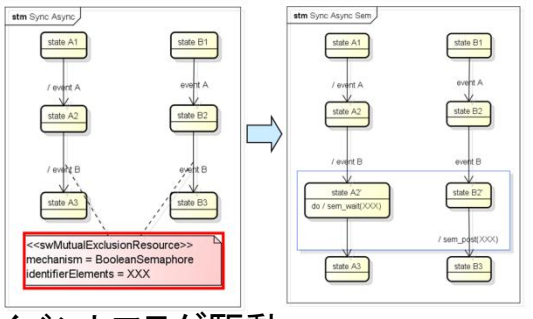
ツールと検証対象の性質を分析

設計	ツール	検証対象
メッセージキュー	○	○
マルチキャスト	○	—
非同期/同期通信	△（一方のみ）	○（混在）
メッセージ駆動	○	○
イベントフラグ駆動	×	○
条件/無条件遷移	○	○
スタック/リスト	○	—
キュー	○	○
動的な資源情報	×	○
タスク優先度	×	—

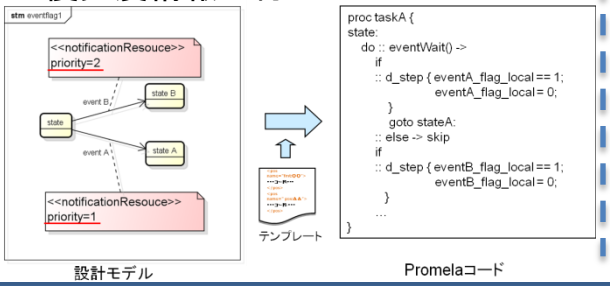
ツールを拡張することでモデル適用範囲の拡大を検討

ツールの拡張

・非同期/同期通信の混在
  - MARTE表記，セマフォの利用



・イベントフラグ駆動
  - 優先度情報の付加



評価・まとめ

評価

- 拡張部のテンプレートを実装
- 実装したテンプレートから，性質を満たす Promelaコードが生成できることを確認

まとめ

- 組込みデバイスドライバに対して，SPIN によるモデル検査を実施し，検証の有効性を確認することができた
- Promela 生成ツールの適用可能性を評価した
  - 現状では生成できない部分がある
- UMLの拡張、テンプレートの追加により自動生成できる可能性を示した