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適用検討

キヤノン株式会社　　八巻智和

開発における問題点

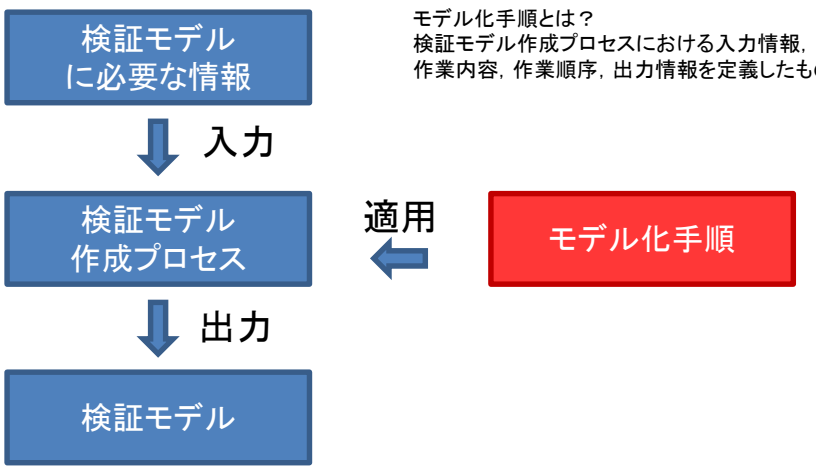
1. ソフトウェアの大規模化・複雑化に伴い再利用開発が行われているが，タイミングに起因する不具合が開発後期で発見されている
2. 一般的な解決策としてモデル検査による網羅的検証が採用されているが，検証モデルの作成に属人性があり適切な検証を行えないケースがある

本手法による解決

既存ソースコードに対し機能を拡張するケースにおいて，割込みハンドラとプロセス間で共通のリソースにアクセスする場合のタイミングに起因する不具合検出を目的に，詳細設計工程において属人性を低減してモデル検査が行えるように，モデル化手順を規定する

モデル化手順に基づく検証モデル作成イメージ

【本モデル化手順に基づく検証モデル作成の特徴】
- ●検証モデルの作成に必要な情報を定義している
- ●開発プロセスで規定しているドキュメントにおいて，検証モデルの作成に必要な情報ごとに，その情報を取得すべきドキュメント名称および記載位置を定義している
- ●それらの情報をどのような順序で，どのように使用し検証モデルに変換するか定義している
- ●検証内容によって検証方法を定義している
  例：時相論理式，アサーション

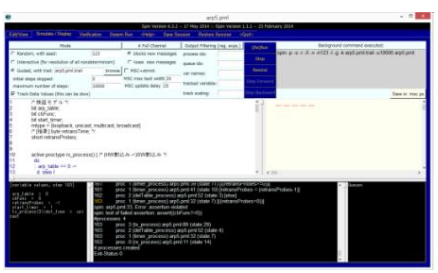


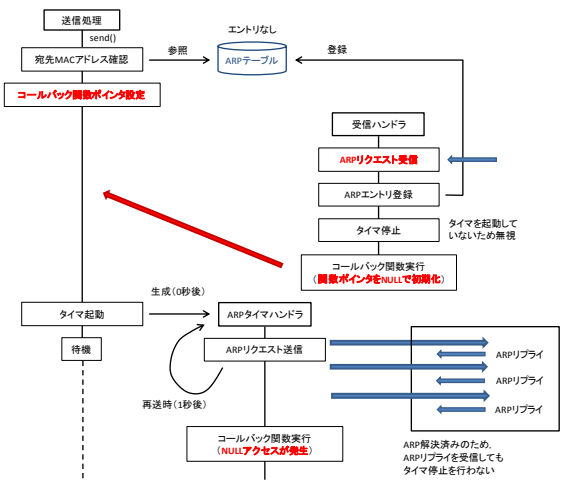
モデル化手順とは？
検証モデル作成プロセスにおける入力情報，作業内容，作業順序，出力情報を定義したもの

適用実験と今後の課題

モデル化手順に基づき，「送受信によってトリガされるARP（Address Resolution Protocol）テーブルのエントリ登録，削除」を題材にモデル検査を実施した．

【評価項目1】
モデル化手順に従って作成した検証モデルは，目的とする不具合を検出できるか？
➡プロセスと割込みハンドラの共有リソースアクセスタイミング問題を検出





【評価項目2】
現行の開発プロセスへモデル化手順を適用できるか？

対象機能/範囲	既存ドキュメントに記載あり.
再利用/新規作成	既存ドキュメントに記載あり.
共有リソース	既存ドキュメントに記載あり.
共有リソースへのアクセスタイミング	既存ドキュメントに記載不足あり. 複数の記載（フローチャートおよび共有リソース説明）から推測は可能であった.
プロセス単位	既存ドキュメントに記載あり.
プロセス優先度	既存ドキュメントに記載あり.
プロセスにおける処理内容	主要処理（ユニキャスト）に関しては記載があるが， サブ処理（ブロードキャスト、マルチキャスト）に関しては記載なし．設計段階で開発者は実装イメージあり.

➡一部記載されていなかった情報要素をドキュメントテンプレートに追加すれば適用可能

【今後の課題】
- ●検証モデル作成に必要な不足情報要素をドキュメントテンプレートへ追加
- ●適用実験をさらに繰り返し，モデル化手順をブラシュアップ
- ●別目的のモデル化手順を作成