トップエスイー修了制作

組込みシステムのオフショア開発のための形式仕様記述方式の検討

富士通株式会社　福永　吉晃　y_fukunaga@jp.fujitsu.com

開発における問題点

組込みシステムのハードウェアアクセス機能を提供するミドルウェアのオフショア開発において，対応ハードウェアの数,制約条件の多さ，また上流設計工程での仕様確認やレビューによるオフショア先とのコミュニケーション負荷の高さから，設計工程で機能の一貫性/整合性を効率よく担保できていない

手法･ツールの適用による解決

自然言語に依存せず，仕様と設計を分けて記述できる形式仕様記述であるVDMに着目.
ハードアクセスのソフト仕様と設計を明確に分離した記述モデル，ハードアクセス機能の設計の一貫性/整合性を人手ではなく，ツールで検証する仕様記述モデル，フレームワークを構築した.

仕様記述モデル･フレームワーク

仕様モデル 仕様モデル

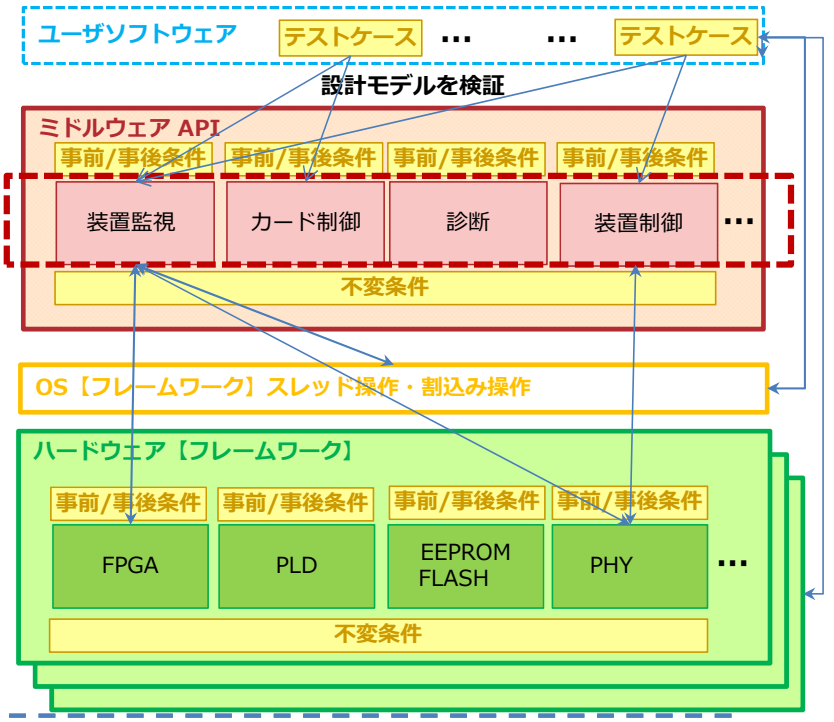
- ✓ ミドルウェアが提供するAPIの機能単位に不変・事前・事後条件を仕様モデルに定義.（設計モデルのインプット）
- ✓ テストケースをツール*により実行し，設計モデルが仕様を満たしているか検証（レビュー）　* VDM Unitと連携

設計モデル 設計モデル

- ✓ 仕様モデル(不変・事前・事後条件)を満たすように設計モデルを作成

フレームワーク フレームワーク フレームワーク

- ✓ 仕様モデル・設計モデル作成，テストケース実行に必要な共通的な操作(スレッド操作，割込み操作)
- ✓ ハードウェア別のレジスタ仕様とデバイスアクセス操作



評価

ミドルウェアの一部機能をサンプルに本モデルで仕様モデル・設計モデルを作成,テストケースによる検証を実施

- ✓ レジスタ仕様に反する操作　→事前条件違反
- ✓ スレッド起動を制約条件にした仕様モデル
  スレッド未起動の設計モデル→事後条件違反
- ✓ 割込み要因クリア漏れ　→事後条件違反

まとめ

- ✓ 仕様モデルと設計モデルを分離した，複数チーム利用も見据えた記述方式を考案.
- ✓ 設計モデルをテストケースの実行により検証できる事を確認.
- ✓ 本モデル適用によりオフショア先とのコミュニケーション負荷低減，レビュー効率向上による設計品質確保が見込める

今後の展開

- ✓ ミドルウェア全体への展開，効果(QCD)確認
- ✓ 仕様・設計モデル記述ルールの整備