トップエスイー修了制作

組み込みソフトウエア開発における モデル検査スタンダードの考案

三菱電機マイコン機器ソフトウエア(株)　片岡 久宜　h-kata@mms.co.jp

モデル検査を業務に適用する上での問題点

・モデル検査技術は弊社として新規性が高く、導入コストがネックとなる。
・流用開発がほとんどである為、ベースの検証モデルがない状態でモデル検査を適用することは、作業効率が非常に悪い。

手法・ツールの適用による解決

「SPINを用いてベースの検証モデルを作成」
「流用開発における再利用可能なモデル検査の手順を構築」

検証モデルの設計

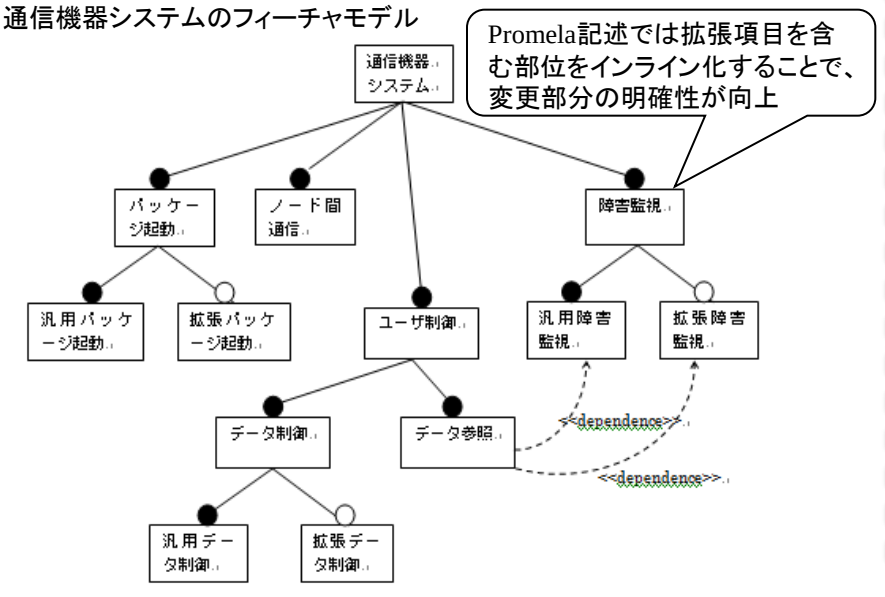
業務で扱う通信機器の組み込みソフトウエアにおける「類似した仕様のパターン」を検証モデルの対象とし、そこから「検証モデルの要求仕様」と「検査項目」を抽出。その後、「フィーチャモデル」を用いて詳細設計を実施。

仕様パターン	モデル化の優先度
監視システムは、ユーザーから通信用パッケージの制御(データ制御や再起動)を可能とする	高
…	…

検証モデルの要求仕様
ユーザーからの制御によって、通信用パッケージは再起動可能であること
…

検査項目一覧	
到達可能性	…
進行性	ユーザーからの制御によって、通信用パッケージは再起動すること
安全性	…
応答性	…

通信機器システムのフィーチャモデル



再利用性の考慮

フィーチャモデルの拡張項目"○"を元に検証モデルの拡張項目を抽出し、拡張項目に対応した検証モデルと検査項目の再利用性を明確化。

■検証モデルの再利用性
拡張項目毎に再利用可能な検証モデルの部位を明確化
（○:検証モデルの修正不要、×:検証モデルの修正要）

拡張項目	検証モデルの部位			
	A	B	C	D
通信用パッケージに対するユーザー制御の追加	×	○	○	×
…	…	…	…	…

■検査項目の再利用性
拡張項目毎に再利用可能な検査項目を明確化
（○:再利用可能、△:一部修正して再利用可能、－:再利用不要）

拡張項目	検査項目番号			
	(1)	(2)	(3)	(4)
通信用パッケージに対するユーザー制御の追加	－	△	○	－
…	…	…	…	…

有効性の確認

有効性の確認では、拡張項目に今回作成した検証モデルを適用。

比較対象	作成したPromelaコード量	作業時間	ライン数による作業時間の正規化(Min/Line)
ベースのモデル作成時	300Line	20時間	4.0
拡張項目適用時	141Line	1時間7分	0.48

拡張項目適用時における1ラインあたりに要する作業時間は、ベースの検証モデル作成時の約8分の1に短縮

今後の展望

・更なるコスト軽減(Promela記述の自動テンプレート生成等)
・サンプル的なプロジェクトに対して、本検証モデルを適用
・モデル検査がソフトウエア開発プロセスに定着できるよう、取り組み