SS2009形式手法WGポジションペーパー

佐原伸

CSKシステムズ & Tao Bears

開発現場でやりたくないこと

I. Word/Excelで書かれた仕様を検証すること

- レビューしかない
  - 現場では古いレビュー技法を行っている
  - 最新のレビュー技法はコードインスペクションに近い
    - 具体的データを考え、手で動かす

II.存在しない業務知識を勉強すること

III.現実に妥協すること

IV.残業すること

開発現場での形式手法適用：できたこと

I. モデル規範型形式仕様記述言語VDM++による仕様フレームワークを構築することにより、アプリケーション階層の仕様を記述した。陽仕様として作成し、回帰テストで妥当性検査と検証を行った。

II. 証券業務とモバイルFeliCaチップファームウェアの仕様で、ほぼ同じ考え方のフレームワークで、仕様を書くことができた。

III. 2関数26行について、洗練(refinement)を手作業で行った。

開発現場での形式手法適用： 課題

I. 陽仕様作成は「仕様を動かすための記述が必要になるので」、その前の陰仕様作成工程で、静的型チェック以上の妥当性検査や検証を行いたい。

II. Smalltalk環境やEclipse環境に比べて開発環境が十分とは言えないので、次世代VDM++ 環境を開発している Overture Projectの成果（Eclipse上に実装されつつある Overture Tool）を取り込みたい

今後、開発現場でやりたいこと

I. VDMからモデル検査への接続

- 例えば、陰仕様の検証で VDM ⇒ SAL 変換を行いモデル検査することが可能ではないかと考えている。

II.(2) VDMから証明への接続

- VDM証明課題 ⇒ HOL 変換をNewcastle大学で行っているが、これを開発現場で使うためには、何をすればよいか？

III.VDMからプログラムへの変換

- いまさらC++やJavaに変化したくないので、Lazy evaluationのできる関数型言語への変換を考えている。今さらVDMの手続き型機能は使うつもりが無いので Fancy VDM というサブセットの名前だけ考えているが、Funky VDMになりそうである。