佐原　伸
（株）CSKシステムズ製造グループVDM推進課
2009年6月18日

SS2009形式手法WG ポジションペーパ

1. 開発現場での形式手法適用

(1) できたこと

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。

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。

2関数26行について、洗練(refinement)を手作業で行った。

(2) 課題

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。

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。

2. 開発現場でやりたいこと

(1) 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。

(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？

(3) 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。

3. 開発現場でやりたくないこと

Word/Excelで書かれた仕様を検証すること

存在しない業務知識を勉強すること

現実に妥協すること

残業すること