トップエスイー修了制作

Event-Bを用いた上流工程品質向上の施策について

富士通株式会社　北條　浩一郎　k.houjyou@jp.fujitsu.com

開発における問題点

ソフトウェア開発における不具合の**改修費用は下流(試験)工程で検出されるほど高額となる。**そのため、上流(設計)工程での不具合検出が重要である。しかしながら、自然言語にて記述された設計書では**曖昧さを完全に排除することが出来ない**ため、不具合が**潜在化してしまう**という問題がある。

手法・ツールの適用による解決

本提案は開発完了した実際の機能に対して形式仕様記述による設計書からの実装を行い、設計工程にてどの位(どの程度)の**不具合を検出することが可能であるか**を検証することを目的としている。特に**“曖昧な記述”**、**“全体像の把握”**といった観点を重点的に検証する。

アプローチ方法

これまでのやり方(課題)

- 構成管理規約 / 記載内容にまでは及ばない
- 自然言語による仕様記載 / 曖昧な記述が多い
- 個人のスキルに依存 / 全体像が良く見えない

上流(設計)工程に形式仕様記述言語を用いる

Event-Bによる形式記述

◆ 複雑なシステムをモデル化するための道具

✓ モデル指向型の形式仕様記述言
✓ 述語論理と集合記法
✓ **リファインメント**

【特徴】
• 抽象的なモデルの状態や状態変化を詳細化し具体的なモデルを構成する。
• 具体的なモデルでは変数が増えるとともに、これらの変数に対応する新たなイベントが追加される。

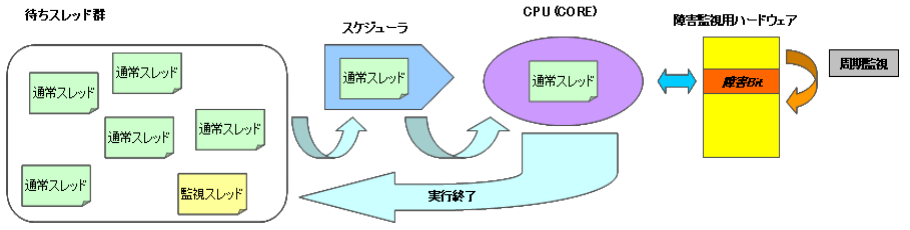
モデル化

段階的詳細化を使ったモデル化

システム監視ソフトウェアを8つのモデルにて表現

Model1	システム構成をモデル化	Model5	通常スレッドの動作を詳細化
Model2	システム実装上の制約をモデル化	Model6	スケジューラ動作を詳細化
Model3	各ソフトウェアの動作をモデル化	Model7	監視スレッドの動作を詳細化
Model4	障害検出の動作をモデル化	Model8	システム例外動作を詳細化

システム監視ソフトウエア概要



考察

23%の不具合を事前検出できた.

Event-B詳細

証明責務(総数)	自動証明	不変条件	ガード条件
57	45	11	94

➢ 不変条件と試験工程にて検出された**不具合3件が一致した**
⇒ 設計工程での品質向上には一定の成果があった
➢ 詳細化モデル(モデル4～8)のガード条件は**14件がソースコードと一致した**
⇒ **実際のソースコードが表現できるため、実装工程の工数削減も期待できる**
➢ 証明責務については、全57件中、45件が自動にて証明することができた
⇒ 約80%は自動にて証明できているため、手動証明のための工数はそれほど多く想定する必要は無い

- **全体像から具体的な1機能**までモデル化、詳細化することができた.
- ソフト/ハードの**役割を明確**に記載することができた
- 数式を使うことにより“より”、“以上”、“未満”といった**数値の扱い**を**厳密**にすることができる
- 複数ある状態を2つの状態に集約することにより、**複雑な判断を段階的**に記載することが可能となった

詳細化が進むことに比例して実装条件が明確となるため、モデル化ツールとしてはかなり有効である