2B-03

ユースケースシナリオの欠陥検知を目的とした形式手法の適用

大坪 稔房† 山口 潔† 岡野 信保† 來間 啓伸‡
(株)日立製作所 情報・通信システム社 生産技術本部†
(株)日立製作所 横浜研究所‡

1. はじめに

近年，ソフトウェアの高信頼化に向けた取り組みとして形式手法の適用が組込み系ソフトウェアを中心に広まっているが，エンタプライズ系システムに対しても形式手法を適用しようという動きがある[1][2]。しかし，組込み系ソフトウェアと比べて，エンタプライズ系システムは一般的に規模が大きく複雑であり，形式手法を適用する場合のコストも大きくなると考えられる。そのため，コスト対効果を考え，検証の有効性を確保しながら形式手法の適用にかかるコストを低減することが現実的な方策として望ましい。そこで，過去のプロジェクトにおける上流工程の成果物を題材として，検証対象をユースケースシナリオに絞り，VDM++を用いた検証実験を行った。本稿では，検証に要した工期，発見した不良と重要度を比較することにより，検証対象をユースケースシナリオに絞った場合の検証の有効性について述べる。

2. VDM++

VDM++[3]は，仕様記述言語を用いてシステムの仕様を記述し，その実行を通して検証を行う形式手法である。形式手法には SPIN や Event-B などのように網羅的な検証や完全性の検証が行えるものがあるが，VDM++はそれらとは異なり網羅性や完全性は保証できない。他方，SPIN や Event-B と比べて，VDM++は形式手法に関する専門的知識を必要とせず，プログラミング言語に類似した仕様記述言語やソフトウェアテストに類似した検証方法は現場の技術者に導入しやすい。そのため，SPIN や Event-B と比べて適用コストが小さく，テスト時の手戻り防止によるコスト削減を目的とした検証に適している。

本実験では，コスト対効果を考え，検証の有効性を確保しながら形式手法の適用にかかるコストを低減することを目的としているため，VDM++を用いることにした。

3. 検証対象の絞り込み

VDM++を成果物の検証に用いる場合，検証対象の設計書の記述内容に基づき VDM++で仕様記述を作成する。この時，検証対象とする設計書の記述が詳細であるほど仕様記述も詳細になる。しかしながら，仕様記述が詳細であるほど検出できる不良は増えるがコストも増大する（図 1）。そのため，本実験では，設計書の記述が比較的詳細でなく，しかも，不良を見逃した場合に手戻りによるコストが大きいと考えられる上流工程の成果物に対して VDM++を適用することにした。

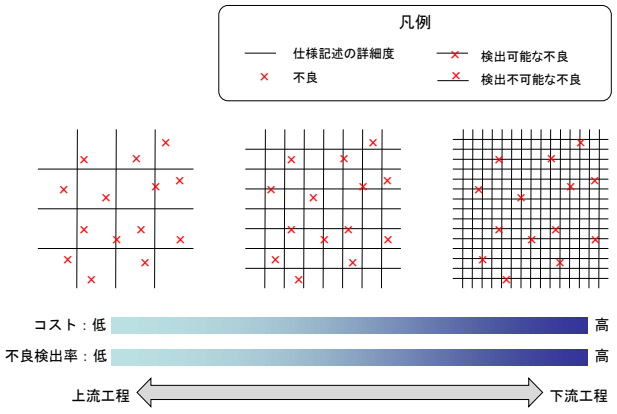

図 1 仕様記述の詳細度とコスト・不良検出率

また，検証の有効性を確保しながら VDM++の適用にかかるコストを低減するためには，検証対象を成果物の中で検証効果が高い設計書に絞り込むことが有益である。一般に，検証対象とする設計書を絞り込むと不良検出率も低下すると考えられる。しかし，不良検出率が低下しても，見逃した場合の手戻りによるコストが大きいと考えられる不良が検出できれば VDM++を適用する効果は高いといえる。本実験では，上流工程において主にシステムの挙動について記述する設計書であるユースケースシナリオに着目した。ユースケースシナリオの記述に起因する不良が後工程で発見された場合，影響がシステムの多くの箇所に波及し，手戻りなどの重大な影響を及ぼす可能性がある。これらのことから，上流工程の成果物の中で検証対象をユースケースシナリオに絞り込むことにした。

4. 実験

4-1 実験概要

4-1-1 題材

題材としたプロジェクトのシステムは 7 つのサブシステムからなり，その内，1 サブシステム分のユースケースシナリオを検証対象とした。検証対象としたユースケースシナリオの量を表 1 に示す。

表 1 ユースケースシナリオの量

ユースケースシナリオ数	9
ユースケースシナリオステップ数	51 ステップ

Applications of Formal Method for Detecting Defects in the Use Case Scenario
† Toshifusa Ootsubo, Kiyoshi Yamaguchi, Nobuyasu Okano, Information & Telecommunication Systems Company, Hitachi, Ltd.
‡ Hironobu Kuruma, Yokohama Research Laboratory, Hitachi, Ltd.

4-1-2　作業者

本実験の作業者とスキルを表 2 に示す。

表 2　本実験の作業者とスキル

作業者	役割	スキル（経験）	
		ＡＰ開発経験	形式手法経験
作業者Ａ	実験全般	13 年	3 年

4-1-3　検証方法

本実験では，システムが正しい状態にあるための条件を業務知識から得た上で，ユースケースシナリオの開始から終了までの間にシステムが不正な状態に陥らないことを検証した。

4-1-4　検証の有効性の確認方法

検証対象をユースケースシナリオに絞った場合の検証の有効性は，VDM++の適用工期が VDM++を用いなかった場合の不良除去工期に対して小さくなることで確認する方法を用いた。

4-1-5　実験手順

実験手順を表 3 に示す。

表 3　実験手順

項番	作業
①	設計書の理解
②	VDM++の仕様記述作成
③	仕様記述の実行
④	③の工期と不良除去工期の比較

4-2　実験結果

4-2-1　VDM++の適用工期

VDM++の適用に要した工数を表 4 に示す。

表 4　工数

作業	工数
設計書の理解	7 人時
仕様記述	9.5 人時
実行	1.5 人時
合計	18 人時＝約 2.25 人日

作業者は 1 名のため，工期は 2.25 日とした。

4-2-2　発見した不良

発見した不良の件数は 2 件であった。以下，発見した 2 件の不良をそれぞれ不良 A，不良 B と記す。

4-2-3　不良の重要度

発見した不良のプロジェクトにおける評価を表 5 に示す。これらの不良はどちらも上流工程で作り込まれた。また，これらは運用テスト以降で発見されたものであり，不良の除去は，当座の運用を可能にするために行う暫定的な対策と，不良の根本原因を除去するために行う恒久的な対策の 2 段階で行われた。

表 5　プロジェクトにおける不良の評価

不良	重要度	暫定対策工期	恒久対策工期
不良 A	高（運用不可）	4 日	約 2 ヵ月
不良 B	中（回避策あり）	なし	約 2 ヵ月

4-2-4　工期の比較

不良 A,B について VDM++適用に要した工期と暫定対策および恒久対策に要した工期との比較を示す。

表 6　工期の比較

不良	暫定対策工期との比較	恒久対策工期との比較
不良 A	2.25 人日 ＜ 4 日	2.25 人日 ＜約 2 ヵ月
不良 B	2.25 人日 ＞ なし	2.25 人日 ＜約 2 ヵ月

5. 実験結果の評価

恒久対策工期については，不良 A, 不良 B のいずれよりも VDM++適用工期が非常に小さい。したがって，VDM++を適用したことにより，恒久対策に掛かったコストを大幅に低減できたと言える。

暫定対策工期については，不良 A よりも VDM++適用工期の方が小さいが，不良 B は暫定対策を必要とせず工期は発生しなかったため，VDM++適用工期の方が大きい。しかしながら，VDM++適用工期である 2.25 日の中で不良 A と不良 B の両方を発見していることから，不良 A と不良 B の両方の暫定対策工期を合計した値と比較すると VDM++適用工期の方が小さい。したがって，不良 A と不良 B の両方の暫定対策に掛かったコストを低減できたと言える。

しかも，不良 A については，重要度が「高」であり不良により運用できない状態になることを考えると，上流工程で VDM++を適用することの効果は大きいと言える。

以上のことより，VDM++の適用工期を低減しながら検証の有効性を確保できることが確認できた。

6. まとめ

過去のプロジェクトにおける上流工程の設計書に対して，検証対象をユースケースシナリオに絞り VDM++を適用する検証実験を行った。その結果，VDM++の適用工期を低減しながら検証の有効性を確保できることが確認できた。

参考文献

[1] Dependable Software Forum, “形式手法活用ガイド【改訂版】,” 独立行政法人情報処理推進機構, 2012 http://sec.ipa.go.jp/reports/20120928.html.

[2] 独立行政法人情報処理推進機構 形式手法適用実証 WG, “情報系の実稼働システムを対象とした形式手法適用実験報告書,” 独立行政法人情報処理推進機構, 2012 http://sec.ipa.go.jp/reports/20120420.html.

[3] 石川冬樹, 荒木啓二郎, VDM++による形式仕様記述, 近代科学社, 2011.