ソフトウエア IV&V（独立検証及び妥当性確認）の研究と実証
Research and Empirical study on Software Independent Verification and Validation (IV&V)

情報技術開発共同センター
Information Technology Center
奥田一実、片平真史、宮本祐子、石濱直樹
Kazumi Okuda, Masafumi Katahira, Yuko Miyamoto, Naoki Ishihama

Abstract

Software IV&V (Independent Verification and Validation) technology has been studied after the space shuttle Challenger accident was occurred. Jaxa is also applying new methodologies of IV&V to software in real space projects. Several techniques have been applied and known as effective approach to high reliability software development in JAXA. In this research, the new methodologies were studied and applied to support project team's software development. As a result of this study, the applicability and effectiveness are confirmed.

1. はじめに

本研究では平成 12 年度より高信頼性ソフトウエア開発技術の１つとして、ソフトウエア IV&V 技術の構築及び実プロジェクトへの適用を実施してきている。また、本研究は、奈良先端科学技術大学院大学、大阪大学大学院、電気通信大学との共同研究のもと実施している。

2. 研究の概要

本研究は、図１のとおり、新規技術の研究、研究成果を受けた技術実証、及びプロジェクト IV&V の適用を繰り返し改良し継続的に実施している。この成果はガイドラインとして纏めている。

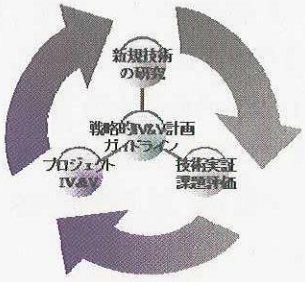

図１　IV&V 研究及び実証の作業フロー

平成 16 年度は以下の項目について研究を行った。

(1) ソフトウエア IV&V に関する新規技術の研究

高信頼性ソフトウエアの試験技術を体系化し、宇宙分野への適合性を検討した以下のソフトウエア IV&V の新規技術について、実プロジェクト評価作業において研究を実施した。

上流工程に関する技術

- 自然言語/形式的仕様モデル(モデル検査)
- 航法誘導制御系モデル化技術
- 仕様記述に基づくモデルシミュレーション
- 衛星データ処理系チェックリスト
- メタモデル言語仕様とモデル検査技術の調査
- 設計故障耐性の評価技術

下流工程に関する技術

- コードチェックの評価技術
- 下流工程におけるリバースエンジニアリング
- 形式的仕様モデルに基づく試験ケース自動生成・自動実行アルゴリズム
- 試験網羅性評価法

共通技術

- トレーサビリティ詳細分析技術
- インタフェース整合性検証方法
- COTS/再利用ソフトウエアの評価法
- コードクローン技術を用いた信頼性解析
- 不具合分析を用いた信頼性解析

(2) 実プロジェクトへの適用

以下の実プロジェクトにソフトウエア IV&V 技術を適用し、プロジェクトにおける課題抽出するとともに、手法の実証を実施した。

- 宇宙ステーション関連（３プロジェクト）
- 人工衛星（３衛星）
- 地上装置（２システム）

(3) 動向調査、情報交換

NASA や ESA の IV&V 担当者との情報交換を実施し関連会議へ参加した。特に、IV&V 分野における各種手法の比較・整理など国際協力につ

いて調整を行い、実施計画を設定した。第４回クリティカルソフトウエアワークショップなどを主催し、JAXA の IV&V 研究内容および IV&V 活動状況について報告・意見交換を実施した。

3. 成果の概要

(1) 上流工程に関する技術

要求仕様書の記載時の留意事項を一般文献や NASA JPL などの研究者から得た情報を元に宇宙用の要求仕様記述評価ガイド（IV&V 用）を策定した。

また、昨年度までに研究・開発した、要求仕様書の形式的仕様モデルの評価のための自然言語による入力方式を用いた形式的仕様モデルのモデル検査を実証し、実プロジェクトでの適用経験から作業効率などの観点で、モデル検査（一貫性解析、完全性解析、トレーサビリティ解析、リーチャビリティ解析）の手法を改良した。

上記で考案した状態遷移モデルに基づくモデル評価技術に加え、フローチャートなどのアルゴリズムなどを評価するために、新たにフローチャートのモデル化技術（フローモデル）を導入し、制御系ソフトウエアの評価手法を施行した。また、SPIN などのモデルとの連携によりシミュレーション環境を構築・実証した。

昨年度、評価方法および評価作業時間に制限のある人工衛星の IV&V 評価を実現するために、衛星姿勢制御系ソフトウエアチェックリストを作成したが、本年度は同様にこれまでの不具合やレビュー経験を元に、衛星データ処理系ソフトウエアチェックリストを作成し、実際の作業で有効性を評価した。姿勢制御系と同様に形式的仕様モデルを用いた解析が時間･方法に制限がある実施できない場合に、チェックリストによる評価で十分な成果をあげることができた。

(2) 下流工程に関する技術

昨年度から更に多機能なコードチェックツールを使用し、開発側で解析を実施することにより、より厳密な分析を行うことができた。バグの洗い出しだけではなく、開発者側がコーディング時にコードの品質向上を更に意識する結果となった。

一方、ソフトウエア試験の網羅性を確保するために、形式的仕様モデルに基づく試験ケース自動生成アルゴリズムを開発し、実プロジェクトへ適用しその手法の適合性を確認した。主な作業ステップを以下に示す。

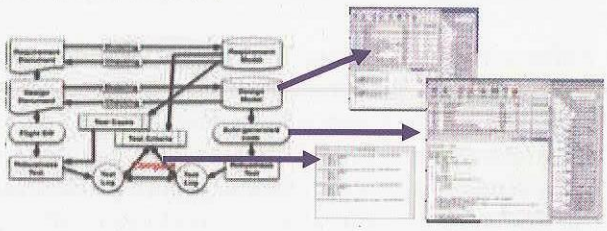

図２仕様モデルを用いた自動試験作業イメージ

(3) 共通技術

その他、共通技術として、市販の要求管理ツールを活用したトレーサビリティの充足性を確認するための分析技術を検討し、実プロジェクトにおいて実証した。仕様のトレース箇所の欠落・誤りのみではなく、設計内容の不整合などの洗い出し作業にも有効であることが確認できた。また、コードクローン技術や不具合分析を用いた信頼性解析を検討し、信頼性上考慮が必要なモジュール及び再確認すべき観点などを抽出することができた。

4. まとめ

これまでの研究において、上流工程から下流工程までの一通りの評価方法を準備した。特に、ソフトウエア IV&V の研究を通じて、

- 宇宙開発で利用できるソフトウエア開発技術を研究・実証し、適用性を判断した上で実用化させる。
- 実プロジェクトのソフトウエアを評価し、適切なフィードバックをかける。

が十分に可能であることが実証できた。実プロジェクトへの適用数が増加する傾向にあるため、要員の増強を図り、評価方法の追加充実を図るとともに、プロジェクトの特性およびソフトウエア IV&V 作業の制約などから作業方法をサイジングできるアプローチ（戦略的 IV&V）についての検討を平成１７年度に開始する。