研究課題別中間評価結果

1． 研究課題名： ディペンダブルシステムソフトウェア構築技術に関する研究

2． 研究代表者： 前田 俊行 （東京大学大学院情報理工学系研究科 助教）

3． 研究概要

本研究課題は、静的プログラム解析技術（プログラムを数学的理論に基づいて解析することで、プログラムを実行することなく、その性質を知る技術)、特に型理論とモデル検査理論に基づき、システムソフトウェアの構築・検証技術を実現することで、システムソフトウェアの高信頼化を目指している。例えばメモリ安全性（プログラムが不正なメモリ操作を行わないこと）や並行実行安全性（プログラムが複数同時に実行されても同期ロックに不整合が生じたりしないこと）等を検証することを目指している。

従来のソフトウェア高信頼化の理論研究では、ややもすると机上の議論にとどまり、実際的な議論や現実的な検証ツールの開発といった点が不十分であった。これに対し本研究では、理論に基づき、既存の C 言語やアセンブリ言語等を対象にして、実際に実用的な検証ツールを開発することを目指している。またこれに加え、実行時のディペンダビリティ支援機構と連携してプログラムの実行時の振舞い・データ等の情報を参考にすることで、事前に利用方法や運用環境などが完全には想定できないような「オープンシステム」においても、システムの開発・運用サイクルを通して、プログラム検証を効果的に利用する手法についても検討している。

より具体的には、(1)システムソフトウェアを記述可能な型付きアセンブリ言語の設計・実装、(2)C 言語から型付きアセンブリ言語への変換器の設計・実装、(3)モデル検査技法に基づくシステムソフトウェアの解析、の三項目について研究を行っている。

尚、本研究領域ではすべての研究チームが一体となって実用的な成果を目指して研究を進めているが、そのために各研究チームから選抜されたメンバーによる「コアチーム」を形成し、個別の研究活動を越えた研究開発を行っている。これまでに、システム開発者と発注者や利用者などのステークホルダとの間でディペンダビリティ要求を合意するための手法ならびにツールの検討を進め、報告書を発行した。当チームからはコアチームメンバとして前田俊行、松田元彦がコアチームに参加し、P-Bus 仕様の形式的定義および、この定義を行うための仕様記述言語の設計・実装等を行った。

4． 中間評価結果

4－1. 研究の進捗状況及び研究成果の現状

本研究課題で取り組んでいる型検査及びモデル検査は、ディペンダビリティ実現のための中核技術として位置づけられ計画に沿って着実に研究開発が進んでいる。コアチームや他のチームと検討を行い、開発するツールのチーム間での共用も考えて具体的な成果につなげてきている。型検査器及びモデル検査器の実装については、当領域の全体との整合性を図りつつ P-Bus/P-Component の一部の検査ができるようになった点は高く評価できる。コアチームへの研究代表自身の参加など領域全体の活動に対しても大変積極的であり、特に P-Bus 仕様の形式的定義に大きく貢献している。研究費の執行も特に問題は見当たらない。

コアチームに関しては、全チームが一体となって一つの成果を追求するという進め方の新しさ及び領域の方針として掲げたオープンシステムにおけるディペンダビリティとして捉えるという課題の困難さもあり、コアチームの立ち上がりには時間がかかったが、グラフを利用してディペンダビリティの合意を定義する D-Case や、そのための具体的なゴールを規定するメトリックスなど、D-Core と呼ばれるチーム全体の軸となる指針を打ち出し、統合的な考え方が整理されてきている点は評価できる。

4－2. 今後の研究に向けて

個別チームとしての研究は実用性の高いテーマなので、ユーザーの使用内容や結果などのデータを蓄積し、

メーカーやツールベンダーとの協業も視野に入れて、今後の計画を考えていくと良い。また、ソフトウェア検証に関しては完全性を求めることは難しいので、できる部分とできない部分とを明確にして順次進めていくことも重要である。オープンシステムディペンダビリティ実現を目指して、運用時を含めて検証技術を利用する枠組みを確立して、実用化につなげていくことが重要である。今後は検証技術に関して領域全体でもリーダーシップを発揮し、フォールトインサーションやデバッグ技術との連携をとり、可能な応用分野に適用し、積極的な挑戦を続ける事を期待する。

コアチームとしては、既存の手法との差別化、科学としての普遍性、実用に供するための具体化の点でさらなるブレークスルーが必要となるが、能力の高い各研究チームのメンバーからなるコアチームメンバが勇気をもって新しい挑戦を継続して行くことによって可能になると考える。また、実用化に向けてメーカーとの連携を深めていくとともに、コアチームの方針に基づいて各チーム個別のテーマ間の関連付けを強化して行くことも必要と思われる。本チームからは、コアチームの方針を踏まえつつ、アプリケーションも含めたシステム全体にわたっての検証ツールの適用や、ランタイムを含む開放系に対する検証ツールの適用を進めて欲しい。

4－3. 総合的評価

他の研究課題と補完的であり他の研究チームとの議論を重ねながら研究方向を適合させている。計画に沿って順調に進捗し、成果も具体的に出ており、高く評価できる。理論から実用化までを目指した良い研究であり、大きな成果を期待したい。これまでの研究成果や今後の研究開発活動の成果を元に、特許の取得を期待したい。