

ソフトウェアシステムのリスク低減に対する形式手法からのアプローチ

アーキテクチャ科学研究系 教授

中島 震



研究背景・目的

ソフトウェアシステムが社会基盤の重要な構成要素となる時代が到来しました。装置機器を中心に発展してきた産業分野や応用セクターが次々とソフトウェア化しています。つまり、ソフトウェア抜きに、イノベーションを考えることができません。新たなサービスの実現にソフトウェア技術が中心的な役割を果たすからです。ソフトウェアシステムは私たちの日常生活を支えることから、求められる信頼性を達成する技術への関心が高まっています。一方、「当たり前の不具合」という言葉に代表されるように、ソフトウェアに絶対的な信頼性はあり得ません。期待される安全性を明確化し、ソフトウェアシステムがもたらすリスクの低減をすることが求められます。本研究課題は、形式手法や自動検証の方法を用いて、このリスク低減問題に科学的な方法を導入することを目的としています。

研究内容

20世紀のソフトウェア工学は生産性向上の技術確立が主要な課題でした。ところが、多くの失敗プロジェクト経験を経て、品質の高さが生産性の向上につながる事が認識されています。そこで、高い信頼性を目指す技術開発に重心が移り、形式手法や自動検証の方法を活用したソフトウェア開発に関心を集めるようになりました。テクノサイエンスによる方法であり、適用限界の範囲で活用法を示します。本研究課題は、産業界との協業経験を踏まえて、理論と実践の両面から「うまく使う方法」を集積する一方、従来のソフトウェア工学手法と自動検証の組み合わせによるプログラム信頼性向上を実現します。また、ソフトウェア開発で重要な技術移管が教育の問題を含むものであると考え、形式手法の基礎を学習する力

リキュラムを整備しました。しかし、ソフトウェアシステムがもたらすリスク低減を考える際、大規模システムの挙動を正確に把握できないという本質的な問題に遭遇します。定量的な機能外要求を対象として、現状の還元論による方法に加えてシステム思考を採り入れたソシオテクノサイエンスの研究を行っています。

産業応用の可能性

- 形式手法および自動検証の基本を学習する標準カリキュラム
- 不具合のあるプログラムの欠陥箇所を自動発見することでテスト工程の工数を削減
- モデルベース解析によって開発上流工程で定量的な機能外要求の妥当性を確認

