研究開発成果13 ／情報通信・エレクトロニクス・メカトロニクス関連技術

Bメソッドによる高信頼ソフトウェアの実践的開発

Practical Development of High-reliablility Software using B-Method

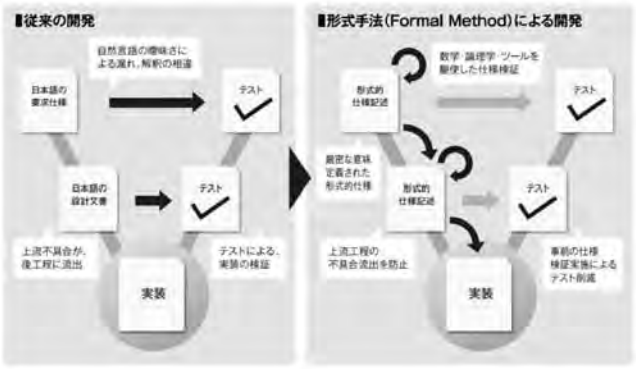
情 報 シ ス テ ム 部　堀　　武司・橋場　参生
ものづくり支援センター　奥田　　篤

■研究の背景

近年のソフトウェア信頼性への要求の高まりに伴い、数理的技法に基づき仕様定義や設計を行う「形式手法」が注目されています。当場と北海道の中小企業を中心として組織された研究コンソーシアムでは、要求定義～設計～実装までの過程の正しさを数理的に証明出来る形式手法「Bメソッド」による高信頼ソフトウェア開発技術の技術導入に関して、実践的な取り組みを進めています。

■研究の要点

1．Bメソッドを導入した高信頼ソフトウェア開発プロセスに関する実践的ノウハウ獲得
2．通信セキュリティ、組込み制御分野などのソフトウェア開発への試験導入の実施
3．形式手法の導入によるソフトウェア品質と生産性の改善度合いの分析



形式手法による開発の流れ

検証ツール（Atelier-B）による仕様の整合性検証

■研究の成果

1．セキュリティ国際規格ISO 15408に則った暗号通信ソフトウェア開発への適用試験を行い、セキュリティ要求と設計の間の一貫性を形式的に証明する事が出来ました。
2．自動車ECU制御ソフトウェア開発への適用試験を行い、上流工程の形式的仕様記述から段階的詳細化によりプログラム導出を行い、不具合発生件数ゼロを達成する事が出来ました。
3．今後は、本研究で得られた技術ノウハウに基づき、技術者向け教育コースや、開発作業支援ツールの開発を予定しています。

北海道電子機器㈱、㈱ミクロスソフトウェア、㈱リック、㈱ヴィッツ
北海道大学、㈱産業技術総合研究所