

報告番号	※甲	第	号
------	----	---	---

主 論 文 の 要 旨

論文題目 高信頼性システム向けリアルタイム OS のテスト手法

氏 名 嶋原 一人

論 文 内 容 の 要 旨

IoT 社会に向かう中で、組み込みシステムの重要性が一層高まっている。また、組み込みシステムの高機能化・大規模化に伴い、マルチプロセッサやメモリ保護機能も必要となっている。一方で複雑化した組み込みソフトウェアの不具合が問題視されている。組み込みソフトウェア開発においては、プログラムの再利用性や、リアルタイム性を確保するために、組み込み向けリアルタイム OS を採用して開発することが一般的である。つまりリアルタイム OS は、組み込みシステムの品質を支える重要なソフトウェアであると言える。また、近年、自動車に搭載される電子制御ユニットにおいても高機能化・大規模化が進み、車載ソフトウェアの開発コストが急増している。1つの電子制御ユニットで実現する機能の数も増えており、複数のアプリケーションを1つのプロセッサ上に混在させたいニーズが増え、アプリケーション間での故障や不具合の伝搬を防止するために、メモリ保護機能の必要性も高まっている。車載ソフトウェア分野においては、開発の効率化、開発コストの削減を目的として、AUTOSAR という標準化されたソフトウェアプラットフォームの導入が、欧州を中心に進んでいる。AUTOSAR においても、重要な役割を持つモジュールの1つとして、メモリ保護機能を提供するリアルタイム OS が規定されており、やはりリアルタイム OS が電子制御ユニットの品質を支える重要なソフトウェアとなっている。

このように、リアルタイム OS の品質確保は重要な課題であるが、リアルタイム OS に特化したテスト手法やツールなどで、一般的に知られているものは存在しない。また、マルチプロセッサやメモリ保護に対応したリアルタイム OS は、歴史が浅く、テスト手法が確立されていないという問題がある。実際に、リアルタイム OS に対してテスト分析を行った結果、リアルタイム OS 特有の性質から、スクラッチでテストプログラムを開発・保守することが困難であることや、マルチプロセッ

サ環境やメモリ保護機能におけるテストの実現に課題があることが明確となった。リアルタイム OS のテストを各企業で実施する場合、同様の課題が発生し、各企業で課題解決に取り組むと重複投資となってしまう恐れがある。また、オープンソースのリアルタイム OS を実製品に利用する場合、製品の品質を保証するために、利用者はアプリケーションのテストだけではなく、利用したリアルタイム OS のテストも実施する必要がある。オープンソースのメリットを損なっていると言える。

本研究では、これらの問題を解決するために、リアルタイム OS に対するテストの課題や規模を明確にし、リアルタイム OS をテストするための手法やツールを考案するため、以下の4つの研究を実施した。

1つ目の研究として、 μ ITRON ベースのリアルタイム OS を対象に、テストプログラムを直接コーディングするのではなく、テストプログラムより抽象度の高いテストシナリオから、テストプログラムを生成するツールを開発した。まず、テストシナリオを形式的に表現するために、TESRY (TEst Scenario for Rtos by Yaml) 記法と呼ぶ記法を考案した。次に、TESRY 記法で記述されたテストシナリオから、テストプログラムを生成するツールとして、TTG (Toppers Test Generator) を開発した。テストプログラムを生成することで、テストスイート開発を効率化し、テストスイートの拡張性や保守性が向上したことを確認した。また、TTG で生成したテストプログラムを実行することで、仕様と実装に相違がある不具合や、ターゲット依存部の実装不具合を検出した。

2つ目の研究として、 μ ITRON ベースのマルチプロセッサ向け RTOS である FMP カーネルに対して、仕様ベースのブラックボックス API テスト、設計・ソースコードベースのホワイトボックス API テスト、および実行順序依存分岐テストを実施した。また、マルチプロセッサ向け RTOS に対するテスト手法として、マルチプロセッサに特化したテストケース設計ポリシーを策定し、プロセッサ間同期制御ライブラリ、拡張 ISS を開発し、マルチプロセッサ特有のコンフィギュレーションへの対応を行った。ASP カーネルと FMP カーネルに対する API テスト、FMP カーネルに対する実行順序依存分岐テストを完了し、かつテスト対象としたソースコードに対する C1 カバレッジを 100% とし、合計 70 件の不具合を検出して RTOS の品質向上に貢献した。

3つ目の研究として、AUTOSAR OS を対象に API テストを実施するため、TTG をベースとして、AUTOSAR OS 向けにテストプログラム生成ツール AKTG (Automotive Kernel Test Generator) を開発した。AUTOSAR OS 仕様の RTOS に対するテストでは、テストプログラムとは別に、RTOS のコンフィギュレーション情報に応じて、XML ファイルとコードやデータの配置を決定するためのヘッダファイルも用意する必要があるため、入力するテストシナリオのデータに応じて、AKTG でこれらのファイルも生成可能とし、テストに必要なファイルの開発コストを大幅

に削減した。テスト実行時間が膨大になる問題に対しては、連続して実行することが困難なテストケースを強制的にマージして実行する手法を考案した。実際に、商用 AUTOSAR OS である JulinarOs に対して本テスト手法を適用し、テストプログラム開発コストおよび、テスト実行時間の大幅な削減を実現した。

4つ目の研究として、メモリ保護機能に対応した AUTOSAR OS である ATK2 に対して API テスト、およびアクセス保護テストを実施した。AUTOSAR OS 仕様は、 μ ITRON 仕様と比べて、OS オブジェクトに設定可能なパラメータが多く、テストケース数が膨大となる問題に対して、テストケースの組み合わせツールを用いたテストケース生成を行った。アクセス保護テストでは、アクセス保護機能に対するテストパターンを導出し、テストのポータビリティ向上のため、プロセッサに依存する部分の明確化を行った。これにより、ATK2 の不具合を 19 件検出し、ATK2 の品質向上に貢献した。

以上の4つの研究成果により、提案したテスト手法、ツールが RTOS の品質向上に有効であることを示した。また、開発したツール、テストスイートの保守性、再利用性、拡張性の高さを示した。