JAIST Repository
https://dspace.jaist.ac.jp/

Title	RTOSを用いた組込みソフトウェア設計の検証手法の提案と事例への適用
Author(s)	飛鳥，誠
Citation	
Issue Date	2007-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/3592
Rights	
Description	Supervisor:岸　知二，情報科学研究科，修士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

RTOS を用いた組込みソフトウェア設計の検証手法の提案と事例への適用

飛鳥　誠（510004）
北陸先端科学技術大学院大学　情報科学研究科
2007 年 2 月 8 日

キーワード：モデル検査,SPIN,RTOS,μITRON,設計検証

近年、組込みソフトウェアの開発規模は拡大しており、品質の確保が難しくなって来ている。そこで、ソフトウェアの信頼性を確保するためにモデル検査を利用しようとする試みが活発になってきている。モデル検査は、状態遷移系のモデルの取り得る状態を自動的・網羅的に探索し、そのモデルの振舞いの正しさを検証する技術である。この網羅性が、現在のレビュー、テストベースの方法では保証しにくくなって来ている部分であり、モデル検査の持つ非常に大きな魅力である。しかし、実用にあたっては問題点もある。１つ目は状態爆発の問題である。計算機の性能の向上によって従来に比べてかなり大きなモデルを一度にモデル検査する事が可能になっている事は確かであり、これがモデル検査を実際のソフトウェア開発に利用することの可能性を大きく広げたことも確かである。ただ、それでもソフトウェアのモデルの取り得る状態数は非常に大きいため、現在のところ、最終的な実装レベルの情報が全て詰め込まれたモデルを一度にモデル検査する事は不可能に等しい。2 つ目の問題として、検証ノウハウの不足が挙げられる。モデル検査の組込みソフトウェア開発への適用は新しい試みであるため、一般的な検証手法はまだ存在していない。そのため、事例検証を行い、その結果を元に検証手順を整理する必要がある。これが、将来的な一般的な検証手法の確立に繋がる。

また、近年の組込みソフトウェアの開発においては RTOS を利用する事も多くなっている。RTOS の上で動作するアプリケーションをテストする場合、その振る舞いをまったく意識せずにシステム全体のテストをすることは難しい。モデル検査においてもこれは同じである。しかも、モデル検査においては RTOS のスケジューリングポリシーを考慮したモデルを作成する事が状態数の抑制にも繋がる。実際の組込みソフトウェア開発を意識してという意味でも、モデル検査の際の状態数を考慮してという意味でも、RTOS を利用することを意識してモデル検査手法を体系化することは有効である。

本研究の目的は、大きく２つである。１つ目は、組込みソフトウェアのモデル検査手法を提案することである。2 つ目は、提案手法を実事例へ適用することである。本研究で目指す「組込みソフトウェアのモデル検査手法」は、μITRON 使用の RTOS を利用するマルチタスクのソフトウェアを対象とする検証手法である。ただし、提案する検査手法は、単純にモデル検査だけの手順を意味してはいない。本研究では、検証を意識した設計アプローチとモデル検査を並行して行ってゆくことを想定している。ここでは検証を意識した設計

アプローチとは、マルチタスクのソフトウェアの設計段階で、ディスパッチの発生するタイミングと割込み許可区間に関して細かく意識して設計することである。これらの点を意識して設計を行うことが検証を意識した設計に繋がるのは、結果的にこれらを設計段階で意識しておく事が、モデル検査時にその探索空間を小さくし状態爆発を抑える事につながるからである。

本研究での成果について述べる。本研究では、まずμITRON 仕様の OS を利用したマルチタスクの組込みソフトウェアを検証する際の検証手法を提案した。次に、事例検証の過程で必要であったメールボックスシステムコールのエミュレーションライブラリを作成し、作成したライブラリがμITRON の仕様に合っているかどうかの検証を行った。最後に、提案した手法をカーオーディオの事例に対して適用し、提案手法の評価を行った。提案した手法を用いる事で、設計対象のシステムをモデル検査可能な大きさで、かつ意味のあるモデルにする事ができた。

論文の概要を示す。本論文では、まず 2 章において本研究において関係のある技術を、第 3 章では本研究で提案するマルチタスク組込みソフトウェアの設計検証手法について述べる。第 4 章では本研究で作成したメールボックスライブラリについて記し。第 5 章で、事例に基づいてカーオーディオの事例を提案手法を用いて設計した例を示す。最後に、第 6 章でまとめとする。