7D－10

マイコンプログラムの仮想実行方式*

～ Dynamic Design Verification and Validation ～

三木 正章　片岡 欣夫　深谷 哲司　平山 雅之†
株式会社 東芝 研究開発センター システム・ソフトウェア生産技術研究所‡

1　はじめに

近年，冷蔵庫などのマイコン組み込み製品では機能および性能の高度化と複雑化が進んでおり，その信頼性を確保するための検証・試験が重要となってきている．特に，製品に組み込まれるソフトウェアの開発では，ハードウェアが並行して開発されるため，試験環境が開発後期になるまで整わないという問題がある．このため，試験を段階的に行うことが困難であり，工程の大幅な後戻りが発生することがある．

このような状況に対応するため，我々は状態遷移図を用いて仕様を記述するマイコン組み込みソフトウェアの検証作業を支援する方法として，仮想実行支援システムを提案する．システムの特徴の一つは，検証の対象となるソフトウェアのソースコードやそれを組み込むハードウェアが完成していない開発早期 (仕様作成) の段階でソフトウェアの検証を可能にすることである．今回は主にこの仕様作成の段階での支援方法を述べる．

2　仮想実行支援システム

仮想実行とは，計算機上で仮想的にソフトウェア / ハードウェアを実現することによって試験環境を整え，実際と同じような感覚でその仮想実現した製品を操作してソフトウェアを検証する，といった意味合いを持つ．仮想実行支援システムは，組み込みソフトウェア開発の各工程に対して，それぞれの工程で補う必要のある環境を仮想的に提供することにより，段階的な検証作業が出来るようにすることを目的としている．これらの仮想環境は場合によってはCPUシミュレータとして，あるいは状態遷移図で記述された仕様を解釈しハードウェアを駆動する仮想実行エンジンとして提供される．仮想実行支援システムは3段階での検証作業を支援する．

［状態遷移仕様作成支援］ 状態遷移図で記述された仕様に基づき，仮想的なハードウェアを動作させることを可能にする．これはハードウェア環境が全く整っていない開発初期に，その仕様の動作を確認する場合に用いる．

［仕様決定支援］ 状態遷移図で記述された仕様に基づいた制御ソフトウェアを仮想的に実現し，実ハードウェアを駆動する．これは既存製品に対するソフトウェア仕様変更の影響を確認するような際に用いる．

［プログラム部品 / 状態遷移エンジン作成支援］ 実際のプログラムをCPUシミュレータを利用して計算機上で動作させることを可能にする．これはターゲットCPUがない状態で，プログラムを試験する場合に使用する．

このように，仮想実行支援システムは組み込みソフトウェア開発の全工程に渡る検証作業を可能にする．

3　状態遷移図仕様作成段階の仮想実行支援

本稿では，2節で述べた支援システムのうち，状態遷移図仕様を作成する段階での支援ツールについて説明する．

3.1　特徴的な機能要求

支援ツールを実現するには，以下の４つの特徴的な機能を満たすことが必要である．これら４機能の実現は，検証時の作業効率や精度の向上に大きな影響を及ぼす．

［仮想実行の対象］ 本支援ツールの仮想実行の対象は，製品を制御するめのマイコンと，マイコンの制御対象である外部環境 — 例えば冷蔵庫では，コンプレッサやファン，センサ類を介して入力される温度等を指す — の二つである．外部環境はマイコンの状態に全く関知せず，任意のタイミングで任意のイベントを発生する．これらは互いに独立に振舞うので，それぞれ独立に仮想実行する必要がある．この独立性は特にイベント発生のタイミングが重要となる状況の検証を行う時に必要となる．

［状態遷移エンジン仕様の多様性］ 状態遷移図による制御仕様を解釈しそれにしたがって製品を駆動する状態遷移エンジンは複数の状態遷移図を並行に実行する．実現する際には，各遷移図の機能に対する性能要求に応じ，複数遷移図のタイムデスパッチや実行方式を製品毎に変更することで多様な製品仕様に対応する必要がある．

［作業支援］ 仮想実行支援ツールには繰り返し試験や長時間の自動試験など，検証時の入力履歴の管理・再利用に基づく作業支援が必要である．

---

*A Method of Embedded Software Verification
†Masaaki Miki, Yoshio Kataoka, Tetsuji Fukaya and Masayuki Hirayama
‡Systems & Software Engineering Laboratory, Research & Deveropment Center, TOSHIBA Corporation

［時間の取り扱い］ 検証の精度を高めるため外部環境とCPUに共通の時間経過を実現する必要がある．これによりタイミングに依存する検証が可能になる．

3.2 構成

3.1の機能要求を実現するため，本支援ツールは図1のように以下の4要素から構成される．各要素がそれぞれ並行に動作するように実装して，仮想実行対象の独立性を実現する．これにより，外部環境におけるイベントを任意のタイミングで発生させることができる．

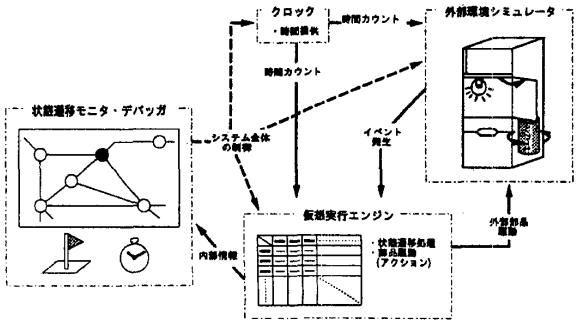


図 1: 仮想実行支援ツール構成

［仮想実行エンジン］ 状態遷移仕様を計算機上で実行するためのプログラム．マイコンを仮想実現したものにあたる．生成時に遷移図のスケジューリング方法等を取り込むことによって，エンジン仕様の多様性に対応する．

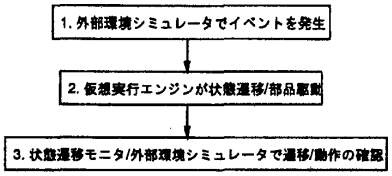
［状態遷移モニタ / デバッガ］ 仮想実行の状況を状態遷移図上で表示，また，マイコン内部で制御されるタイマやフラグなどの状態を表示して開発者の動作確認を支援する．また，上記モニタとしての機能に，全体の実行パターンを制御する機能 (run, stop, continue, step など) を組合せ，仮想実行デバッガとしての機能を実現する．

［外部環境シミュレータ］ 製品の制御対象を計算機上でシミュレートしそのユーザインタフェースを提供する．例えば冷蔵庫の場合，コンプレッサ，ドア，温度 (制御対象) などをシミュレートし，開発者はスイッチのオン / オフ，ドアの開 / 閉 (状態) を操作する．あわせて，操作履歴を管理・再利用することにより，検証作業効率を大幅に改善することを可能とする．

［クロック］ ツール全体に共通の時間を提供する．マイコンと外部環境はクロックが提供する時間を参照するため，時間の経過を早く / 遅くするような場合にも矛盾を生じることなく仮想実行できる．また，経過速度の変更は長時間に渡る試験の効率向上にも寄与している．

3.3 仕様検証の手順

実際の検証手順は基本的に1→3の繰り返しとなる．



不具合を発見しその近辺の仕様を詳しく調べたい場合などは，操作履歴の再利用，ブレークポイント / ステップ実行等を活用する．きわどいタイミングを検証したい場合は時間経過を遅くすることができる．

3.4 支援ツールの効果

実際に開発中の冷蔵庫の仕様を用いて本支援ツールを評価した結果，以下のような効果を確認した．

1. 仕様作成の段階で製品の動作確認が可能
2. 開発早期の段階で品質を作り込むことが可能
3. タイミング (時間) に関係する検証が可能

この支援ツールは具体的に仕様の動作を視覚化し確認するため，状態遷移図をトレースして誤りを検出する従来の検証方法では難しかった，仕様の抜けや勘違いを検出できるようになった．例えば，冷蔵庫は扉を開けたらランプが点灯するが，それが仕様自体に書かれていない場合，従来の検証方法では発見できない．しかし本支援ツールでは，計算機上で実現された冷蔵庫の扉を開けたときランプが点灯しない，等によって確認できる．

加えて，本支援ツールは時間の概念を取り込んだ仮想実行を行なうため，タイミングに依存する不具合の検出も可能である．例えば，コンプレッサが動き出した瞬間に一気冷凍スイッチを押したらどうなるか，タイマがカウント中に冷蔵庫内の温度が変化したらその情報はどのように処理されるのか，等を確認できる．

4 おわりに

マイコンソフトウェアを開発の全工程にわたって支援する仮想実行支援システムを提案，この支援システムのうちの状態遷移図仕様作成段階の支援ツールを詳細にわたり説明した．今後はより広範囲の支援 — 他の段階に対する仮想実行支援 — を実現していく．

参考文献

[1] 岸 他，状態遷移モデルに基づくプログラム部品合成システムの開発，情報処理学会ソフトウェア工学研究会，Vol.91, No.66, 80-18, 1991