1N-6

組込みソフトウェアのモデル検証

本間洋光† 新村祐太† 齋藤理† 力武克彰†
仙台高等専門学校†

１．背景

近年，組込みシステムのソフトウェア開発にモデルベース開発と呼ばれる開発手法が使われるようになってきている．モデルベース開発とは UML 等の図表現を用いてシステムをモデル化し，モデルをもとにシステム開発を進める手法である．複雑化するソフトウェア開発に対し，モデルベース開発はシステムの全体像の把握を容易にし，ソフトウェアの再利用を促進することで生産性を高めることが期待されている．

モデルベース開発の効果を高めるためには仕様変更を容易に行え，再利用性の高いモデルを記述することが重要である．しかし，前述の要件を満たしたモデルは図の記法を学んだだけでは記述できるようにはならず，訓練と経験が求められる[1].

そこで，モデリング教育の参考資料の提供、モデルベース開発の普及促進を目的に UML モデリング推進協議会(UMTP Japan)から組込み分野向けに参考になるような様々なモデルをまとめた UML モデルカタログ[2]が発表された.

モデルカタログとは製品開発への適用が可能で，かつモデリング学習の題材となるモデルを公開するもので、利用者はその中から参考になりそうなモデルを選択し無償で開発に利用することができる.

しかし，モデルカタログはプラットフォームに非依存な PIM のみの提示となっているため，PIM から実装を意識したプラットフォームに依存した PSM に落としこみ，実装を行うという開発の流れが示されていない．よって具体的な活用法が不明である．また，PIM 自体については検証がなされておらず，PIM に設計上の誤りがある可能性もある.

Verification of Target Control UML Model Using Model Checking

Hiromitsu HOMMA†
†Sendai National College of Technology
989-3128 , Sendai , Japan

そこで，本研究ではモデルカタログに提示されたモデルの具体的な活用法を検討し，PIM の設計を検証することで，製品開発への適用や教育題材を前提としたモデルカタログの利用価値を高めることを目的とする.

２． 研究経過

我々は，モデルカタログの活用法を検討するため，複数のプラットフォームに対し PIM を PSM に落としこみ実装を行った．検証対象としてモデルカタログから目標制御モデルを選択した．目標制御とは計測値が目標値となるように制御を行う仕組みである。温度調節や物体の走行速度制御などに組込まれ利用される.

目標制御モデルを二種類の二輪ロボットシステムの走行プログラムへ適用した結果，一種類の PIM から異なるプラットフォーム用の PSM を作成し,実装可能であることを確かめることができた．しかしながら，目標制御モデルの実装では PIM 自体の検証は行なっておらず、今回の検証では顕在化しなかった欠陥が潜んでいる可能性もある．PIM の設計は PIM を利用して生成される PSM に直接影響を与えるため，十分な検証が必要となる．本稿では主に PIM の設計検証について検討する.

３．モデル検査と検証項目

本研究では形式手法の一つであるモデル検査を用いて，目標制御モデルを検証する．モデル検査によりモデルの厳密な検証が可能となり、仮に不具合が存在すればそれを指摘できる．結果，矛盾が見つからなければ信頼性の高いモデルであると証明することができる。

モデルの検証と一口に言っても様々な検証項目が考えられる．そこで本研究ではまず，モデルの矛盾やそれに伴う欠陥の有無を検証項目とした．ここでモデルの矛盾とは，複数のモデルの間に不整合が生じることであるとする.

モデリングにおいて，モデルから矛盾を排除し一貫性を持たせることは予期しない欠陥を生まないために重要な要素であるため，PIM の矛盾の有無の検証はモデルの品質向上に繋がる.

本研究ではモデル検査ツールに UPPAAL を採用し検証を行う．UPPAAL とはシステムの振る舞いを時間オートマトンを用いて表現し、検証したい性質を時間計算木論理の式を用いて検証することができるツールである．実時間が扱えることから，リアルタイム性が問われる組込みシステムに適している．

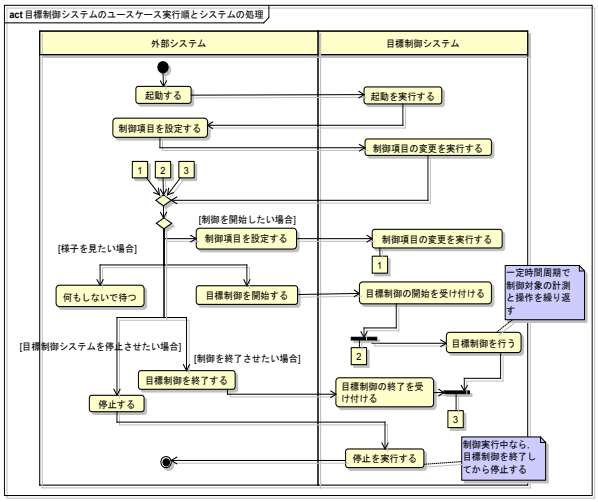

図１　目標制御　アクティビティ図

４．時間オートマトンモデル化と検証結果

目標制御モデルの矛盾の検証に当たり，目標制御の要求分析で用いられた図１に示すアクティビティ図を時間オートマトンに変換する．アクティビティ図からシステムが取りうる状態を読み解き，ユースケースに記述されたイベントが発生すると遷移するようにオートマトンを記述した．図１は、目標制御システムとそれを使う側の外部システムがパーティションに分けられて記述されている．そこで，これらは別のオートマトンとして記述した．

二つのオートマトンからそれぞれインスタンスを生成し，別のプロセスとして並行動作させる．これにより，目標制御システムが他のプロセスとは独立して周期的に動作するモデルが構築できる．以上を踏まえて図 2，図 3 に示す二種類の時間オートマトンを記述した．

５．検証項目の抽出

検証項目として図 4 に示すシーケンス図から以下の項目を抽出した．

・目標制御が一時停止したあと，制御再開することがある．

この項目について UPPAAL を用いて検証した結果，反例が見つからなかった．そのため検証したモデル間に矛盾が存在しないことが示せた．

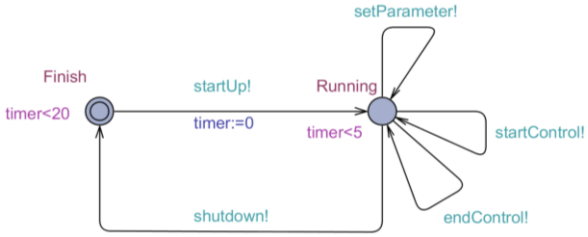

図２　時間オートマトン　外部システム

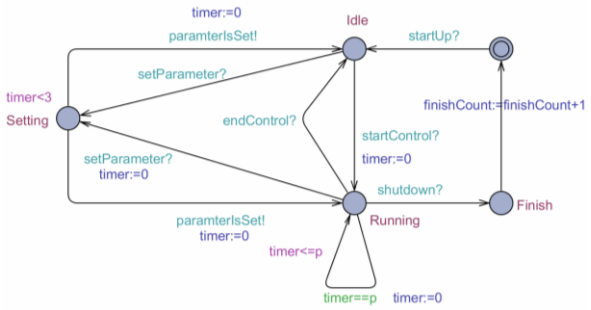

図３　時間オートマトン　目標制御システム

６．まとめ

モデルベース開発の利点とモデル作成の難しさを指摘した．この障害を軽減する手段としてモデルカタログについて紹介し，同時にモデルカタログの不完全さを指摘した．その解決策としてモデルカタログを用いた開発と，モデル検査による検証を行った．モデル検査においては矛盾が見つらないという結果が得られ，モデルの整合性という面では品質が保証された．

目標制御モデルでは排他制御が用いられているので，今後は複数の目標制御システムを並行して実行した際にデッドロックが発生しないか検討し検証内容を広げていく．

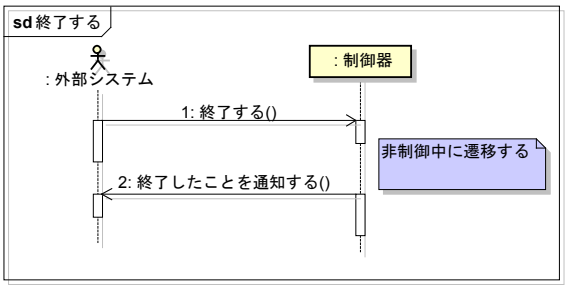

図４　シーケンス図

【参考文献】
[1] 近藤満：組込みソフトウェア開発の課題と対応，コンピュータ産業研究会（2007）
[2] UMTP 組込みモデリング部会：組込み分野のための UML モデルカタログ（2012.04.15）
http://www.umtpapan.org/themes/original2/pdf/built/ uilt_uml_catalog.pdf