宇宙用途の FPGA 外部インタフェース回路開発に対するモデル検査適用

倉林翔[†1]　梅田浩貴[†1]　石垣雄基[†1]　植田泰士[†1]

概要：本稿では，宇宙用途の FPGA 外部インタフェース回路開発に対するモデル検査適用課題の対策を立て，その対策を基に開発したツールを示す.

キーワード：モデル検査，FPGA，上流工程，NuSMV

Application of model checking to FPGA external interface circuit development for space application

SHO KURAHAYASHI[†1]　HIROKI UMEDA[†1]
YUUKI ISHIGAKI[†1]　YASUSHI UEDA[†1]

Abstract: In this paper, we set up countermeasures for model inspection application tasks for the development of FPGA external interface circuit for space application, and show the tools developed based on the countermeasure.

Keywords: Model checking, FPGA, Upstream process, NuSMV

1. はじめに

宇宙用途製品の特徴は，製品の故障が起こった場合，交換等の修理は，製品の多くが実施できない．また、製品１つの故障がシステム全体の永久的な運用停止につながらないよう保証することも求められる．そのため，地上用途に比べて，格段に高い信頼性が要求され，開発時の検証が重要である[1].

また，宇宙用途製品は，大量生産品ではなく限定された開発数であり，且つ、開発期間が５年以上と長いため，過去事例が少なく，レビュー等の設計時の検証は属人性が高い．そのため，設計検証を行うには，過去の開発経験や不具合やその未然防止策の経験を有している人の検証観点を上手く活用して，検証することが重要である.

さらに，製品製造後の検証で問題が発生した場合，大きな手戻りが発生するため，より上流の設計段階での検証が重要である．そのような宇宙用途製品の開発において，設計の信頼性を高めるため，モデル検査の適用を検討した.

しかしながら，モデル検査を適用するには，以下に挙げる課題がある[2][3].

課題①：設計段階では，繰り返し設計を修正するため，仕様記述によるモデル等の修正が高い負荷となる.

課題②：経験のある技術者（以下、エキスパートという）が暗黙的な仕様も含めてモデル化しないと，あり得ない反例ばかり出力される.

課題③：反例の出力結果は，通常の開発業務と異なる状態で出力され，設計へ反映するかどうかの判断に必要な情報を分析することが高い負荷となる.

上記課題に対し，本稿では以下の解決方策をとった.

対策①：エキスパートが試行錯誤する思考経緯を可視化することで，通常の開発時に行う作業経過から，モデル検査に必要な情報を収集し，モデルの生成や検査を再帰的に自動で行い，モデルの修正負荷をなくす.

対策②：製品特性から暗黙的な仕様を表現する専用のルーリングを定義し，エキスパートがモデル検査の知識を必要とせず，モデルに反映し，あり得ない反例を防ぐ.

対策③：反例の出力結果を通常の開発業務で使用されている設計検証ビューへ変換して出力することで，通常の設計検証と同様な作業とし，分析する負荷をなくす.

2. 適用方法

(1) 適用先の特徴

本稿では，FPGA（Field Programmable Gate Array）の外部 IF（Inter Face）回路設計時に対して，モデル検査を適用した. モデル検査器は, NuSMV（A New Symbolic Model Verifier）[4]を利用した.

FPGA の外部 IF 回路設計では，クロック信号で信号タイミングの基を決めている．このクロック信号の立上り，立

†1 国立研究開発法人　宇宙航空研究開発機構
Japan Aerospace Exploration Agency (JAXA)

下りの１サイクルを１クロックと呼び，１クロック単位で各信号の入出力のタイミングを決定している．

FPGA の外部 IF 回路の動作は，回路図とステートチャートで表され，各入力信号パターンの複合的な組み合わせに応じて，出力信号を組み合わせたものをステートとして定義し，信号の入出力順序は，ステートチャートとして表現される．

また，IF 相手と双方向通信を行うため，入出力信号のタイミングが重要で，１クロックごとに各信号タイミングを考慮する必要があり，入出力信号のタイミングを調整する回路が FPGA の外部 IF 回路である．そのため，多数の信号間の関係を１クロック単位で設計するため，検討漏れが起き，不具合が発生してしまう．

さらに，宇宙環境では，高エネルギーの放射線の影響で，ビット反転（SEU : Single Event Upset）が起きやすく，そのビット反転が原因により想定外動作が起き，デッドロック等が発生する．このような不具合抽出には，過去の開発経験，知識が重要になる．

従来，過去の開発経験や不具合やその未然防止策の経験を有している人が，複数の信号動作をシナリオとして捉え，不具合の発生しそうなシナリオを回路図，ステートチャートから想定し，タイミングチャートを部分的に作成し設計検証している．但し、タイミングチャートには，１シナリオしか表現できず，手動で作成しているため，複数のシナリオを検証しようとすると，膨大な作業時間がかかり，網羅的な検証ができていなかった．そこで，モデル検査を適用し，その検証観点を網羅的に検証できるように，次項以降に示すツールを開発した．

(2) 開発ツール

今回開発したツールでは，従来の設計過程で，モデル検査に必要な情報が収集でき，エキスパートが意識せず，モデル検査を行うことができる仕組みになっている（図 1）．

従来の設計では，回路図，ステートチャートを人手で作成していた．開発ツールでは，作成の工程を思考部と作図部にわけ，思考部は一連の順序で記入していくことで，回路図，ステートチャート，タイミングチャートが系統的に作成できるようにした．思考部の中間生成物を，作図部では自動変換することで既存の設計過程を短縮し，さらに，中間生成物の表からモデル検査に必要な情報を抜き出し，自動で仕様記述言語に変換している．

また，モデル検査の爆発を防ぐため，既存の設計過程では作成しないフローチャートを中間生成物として自動変換している．検査項目に関係のあるシナリオを選択してもらうことにより，エキスパートが指定する検査項目に対して最小限の仕様をモデル化している．検査式も，時相論理式に自動変換できるにフォーマットに，開発ツールで誘導することで、エキスパートにモデル検査の専門知識が必要としないようにしている．

モデル検査の結果である反例は，仕様記述言語における変数の値の変化が出力されるが，その結果が設計検証として有用であるか，仕様記述言語の内容を理解していないと，分析ができない．さらに，暗黙的な仕様がモデルに実装されていない場合には，システムの動作として，起こりえない反例が出力される．

開発ツールでは，反例を従来の設計検証ビューであるタイミングチャートで表現することで，通常の設計検証と同様な作業で分析を行うことができ，反例を分析する作業負荷をなくすことと，途中の中間成果物からエキスパートがタイミングチャートを系統的に作成することで，モデル検査の結果自体を検証できるようにしている．

また，製品特性から暗黙的な仕様は，専用のルールで表現することで，効率的にモデル化することで，起こりえない反例を防ぐことができる．

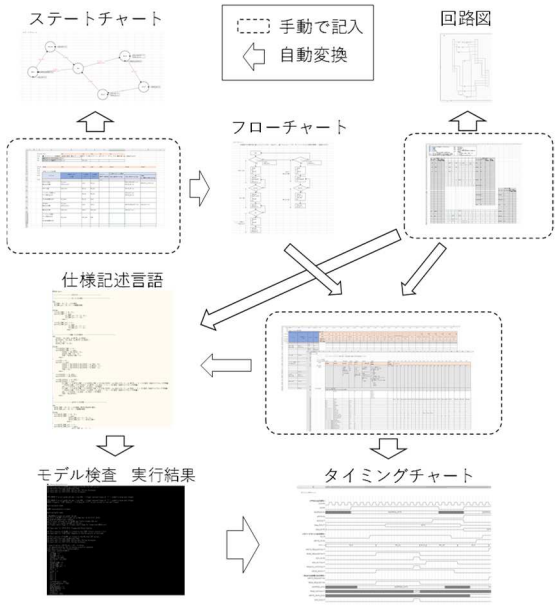

図 2　開発ツールの全体像

3. 終わりに

本稿では，宇宙用途の FPGA 外部 IF 回路開発に対するモデル検査を適用する際の課題と，課題を解決するための手法を提案した．今後，適用実験と改善を行い，継続的に FPGA 設計者が通常の開発作業内で，自然とモデル検査を活用した設計検証や保証を行えるかを検討する．

4. 参考文献

[1] 岡田崇志，喜多貴信，五島正裕, & 坂井修一. (2009). 耐永久故障 FPGA アーキテクチャ. 研究報告計算機アーキテクチャ (ARC), 2009(4), 1-8.

[2] 山口智也，足立憲保，加賀智之, & 大桑芳宏. (2012). 自動車制御ソフトウェア開発プロセスへのモデル検査の適用. 組込みシステムシンポジウム 2012 論文集, 2012, 188-196.

[3] 高田沙都子. (2012). モデル検査技術による上流工程での効率的な設計検証. 東芝レビュー, 67(11).

[4] “NuSMV: a new symbolic model checker”. http://nusmv.fbk.eu/, (参照 2018-11-29)