大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

# 画像生成システムのSPINを用いた設計検証

所属：キヤノン株式会社　名前：森 博史

## 開発における問題点

私の担当する、画像生成システムは、制御ソフトが、複数のハードを並列に動作させ、プリント画像の生成を実現する。この画像生成システムの設計および検証は、人手で作業を実施。
そのため、並列に動作する複雑な本システムを、人手で開発作業を行うため、抜けや理解の誤りが発生し、問題流出する事が問題となっている。

## 手法・ツールの適用による解決

この画像生成システムに対し、機械的に網羅検証を可能とする検証機構を適用する事で、人手で発生する開発作業工程の抜けや理解の誤りを、設計段階で防止する。利用する手法・ツールとして、モデル検査の分野で用いられるSPINを利用して、網羅検証可能な機構の適用を行う。

## モデル化

### モデル化手順

1、画像生成システムの設計図面(クラス図/ハードブロック図)から、並列動作するソフトとハードを、プロセス抽出。
2、状態遷移図のアクションと遷移、実装から、プロセスの振舞をPromelaで記述。

### モデル抽象化

| 抽象化 | 抽象化内容 |
|---|---|
| 1 | 対象モジュールへの指示部を、任意の通信として抽象化<br>(ex) 自ソフトに対する制御ソフト |
| 2 | パイプライン上に繋がる複数のハードウェアを、<br>先頭・終端のハードのみに抽象化。 |
| 3 | 割込信号/ハンドラの振舞は、<br>単純な任意のタイミングの通信に見立ててモデル化 |

## 検証時間

前述の検証時間は以下。平均高々2分/項目で検証可能。

| | 検証内容 | 検証時間<br>(Total) |
|---|---|---|
| (検証内容1)<br>過去問題の検証 | 検証項目: 10項目<br>Promela: 240行、プロセス5つ。 | 16分52秒 |
| (検証内容2)<br>新プロジェクトの検証 | 検証項目: 3項目<br>Promela: 177行、プロセス4つ。 | 20秒 |

自開発(100項目)の検証時間比較。同等で適用可能性。

| 現プロジェクト (実装モデル検証) | SPIN適用時　(設計モデル検証) |
|---|---|
| 3分/項目　Total: 300分 | 2分/項目　Total: 200分 |

## 検証内容

### 検証内容1: 過去発生問題の検証

●題材の過去問題:
複数のハードウェアの同期不足でデッドロック
●検証式:
デッドロックを起こす状態の組合が無い事を検証

```
ltl spec1 { [] !( (RIP_IMG_GEN_HW@state_rip_hw_rendering)
    && (OTHER_HW@state_rip_other_hw_power_off) ) }
```

### 検証内容2: 新規プロジェクトの検証

●題材の検証対象:
新プロジェクトの新たな仕様内容のデッドロック。
●検証式:
新たな電源仕様で、デッドロックが無い事を検証。

```
ltl spec5 { [] ( RIP_Driver@abort_rip ->
      <>RIP_Driver@abort_rip_idle_rip ) }
```

## まとめ・今後の課題

以上より、私の担当する画像生成システムに対して、モデル検査のSPINの適用を検討した。
検証したい検証内容が、設計モデルで検証可能である事、検証時間も現プロジェクト相当で実現可能である事を検証できたため、適用可能性が見出せたと考える。

今後は、以下が課題であると考える。

・自開発部門への適用・定常運用。
SPINの記述は、知識習得を含め、導入コストが高い。既存の設計ドキュメントでPromelaを自動で生成・検証可能な機構。

・複雑な検証対象への適用。
検証内容の拡充。自部門の並行システムへの、広く適用が必要。