JaSST '05

モデル検査とその適用事例紹介

独立行政法人　産業技術総合研究所
システム検証研究センター
水口大知　　渡邊 宏

2005年1月24日(月)

システム検証研究センターの研究活動

① システム検証技術の基礎研究
- 数理的検証技法
- モデル検査技法や定理証明技法など

② システム検証の「フィールドワーク」
- 企業との共同による事例研究
- 技術者向けモデル検査研修コースの開発・実施

パートナー募集中！

受講者募集中！

システム検証研究センター

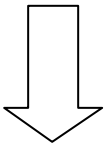
- ホームページ
  http://unit.aist.go.jp/cvs/
- お問合せ電子メール宛先
  informatics-inquiry@m.aist.go.jp
- 活動拠点
  - 千里中央（大阪府豊中市）
  - 尼崎（兵庫県尼崎市）
  - つくば
  - 臨海副都心（お台場）

発表内容

- モデル検査の組み込み開発への適用事例紹介
- 途中、モデル検査ツールの使い方を紹介

『フィールドワーク』

組み込み機器のソフトウェア仕様書にモデル検査を適用した



仕様書の不備を発見できた

H15年度実施

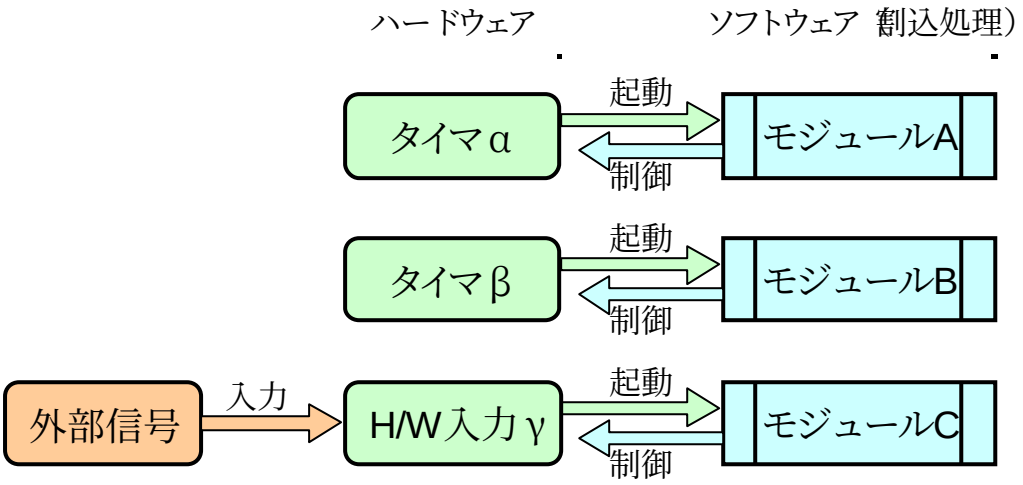
では、

- 検査対象は？
- 作業手順は？

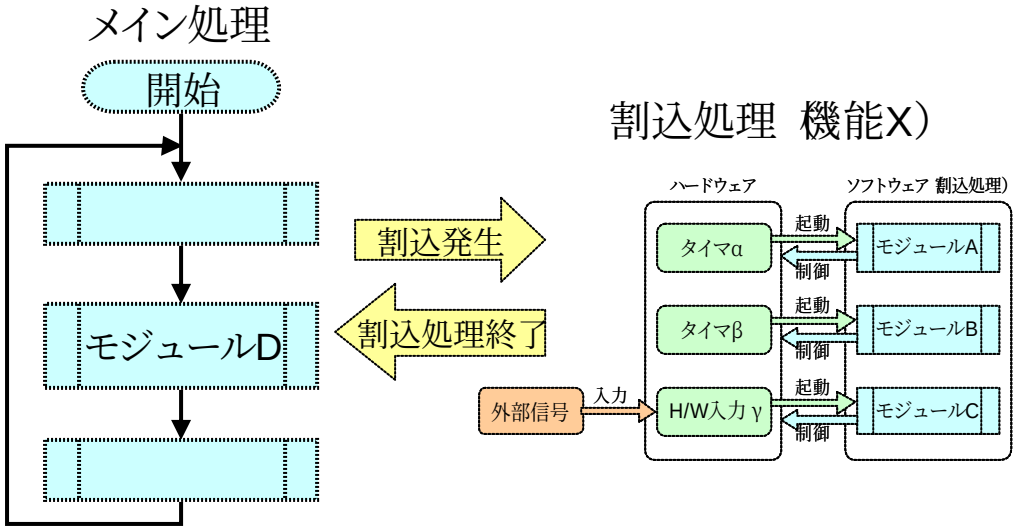
検査対象

- プログラム 製作仕様書
  - 企業で実際に開発途中にあった
- メイン処理と割り込み処理によって構成される組み込み機器
  - OSなし、多重割り込みなし
- 主な4つの機能X, Y, Z, Wを検査した
  - 20ページ／機能

機能X



機能Y



検査項目

- プログラム 仕様が機能仕様を実現していることを検査する。
  - 外部信号の異常が続いたらシステム停止
  - システムが停止中なら、CPUはある状態である
  - 外部信号が正常に戻ったらシステム再開
- あらゆる状況において検査項目が真であるか否かをモデル検査ツールにより検査
  - テストでは困難

機能Yの検査例

検査項目: システムの動作が中断状態にあるとき、CPUは状態Qであること

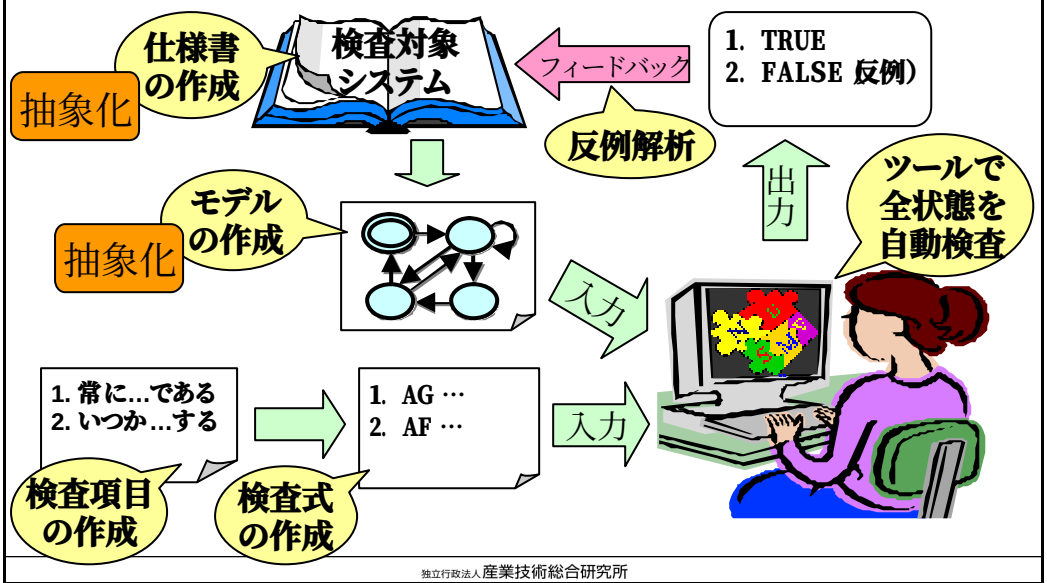
⇩ ツールで検査

検査結果：False
反 例：システムの動作が中断状態にあるとき、CPUは状態Qでないことがある

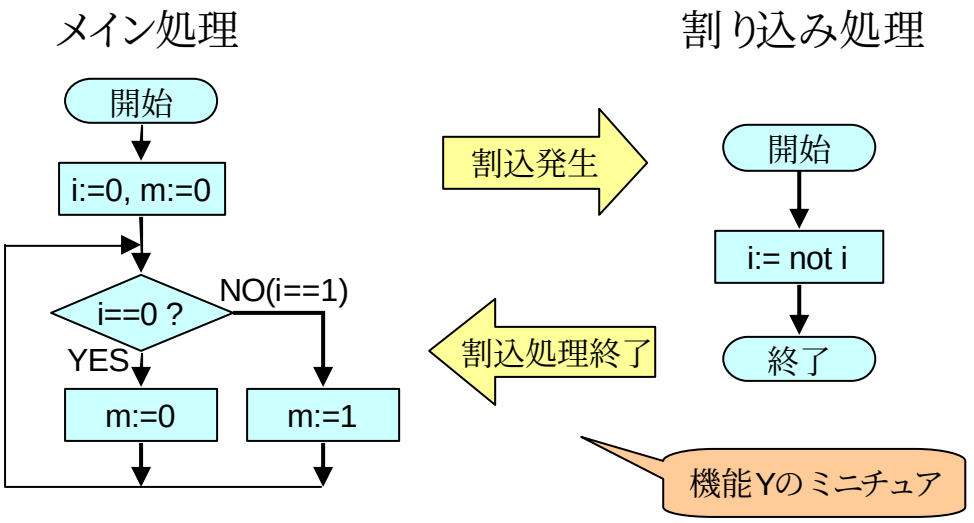
⇩ 反例の解析

原 因：モジュールDの実行中に、設計者が意図しないタイミングでタイマβによる割り込みが発生することがある

作業手順



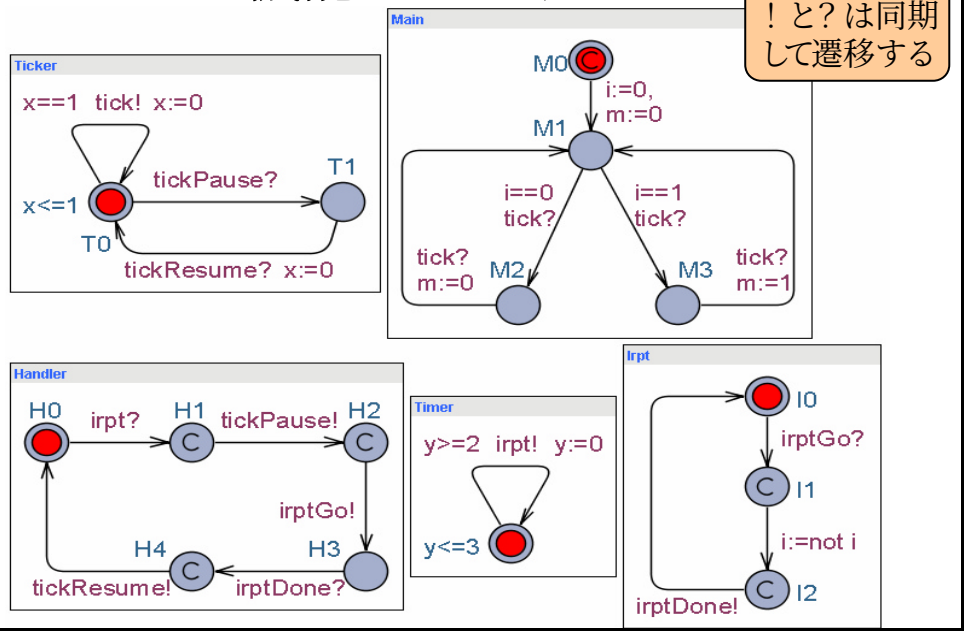
小さな例 :機能α



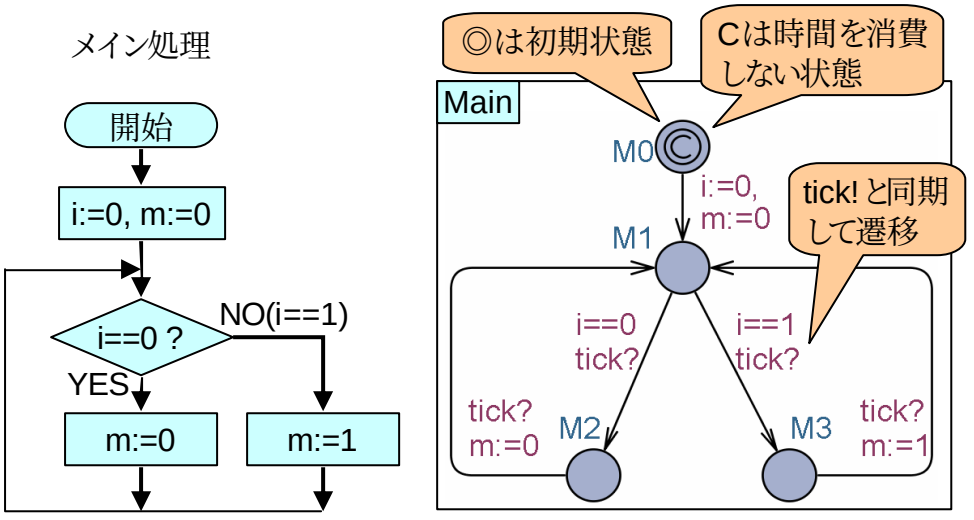
モデル検査器 UPPAAL

- モデル　＝　時間オートマトンのあつまり
- 検査式　＝　CTLの一部
- http://www.uppaal.com にて公開

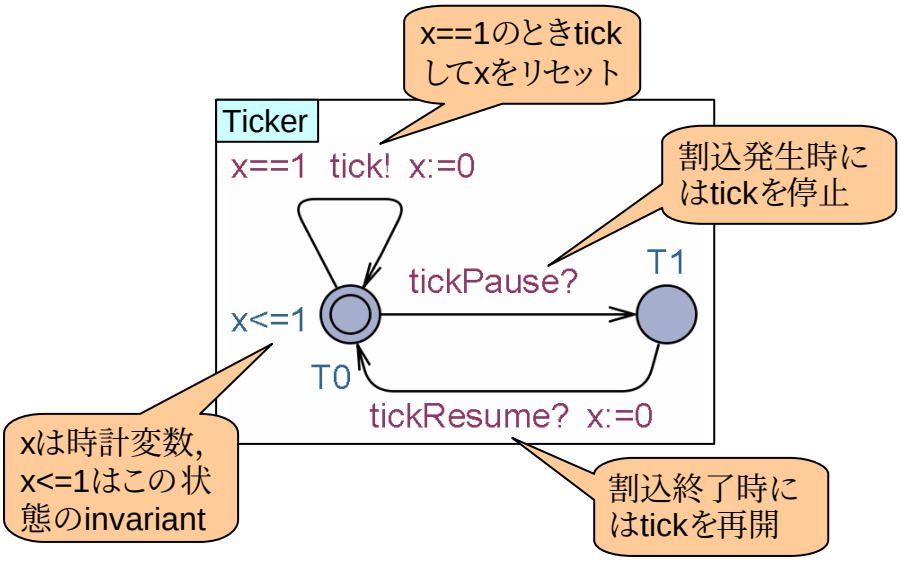
機能αのモデル



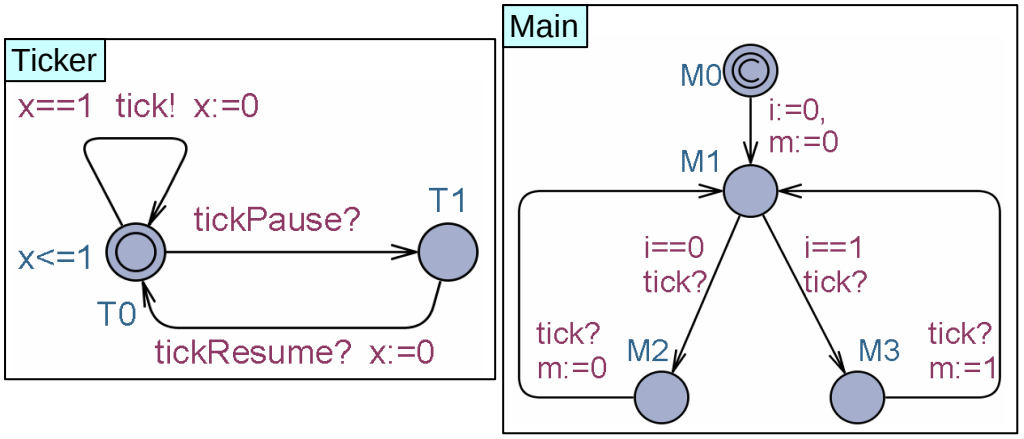
メイン処理のモデル(1/3)



メイン処理のモデル(2/3)

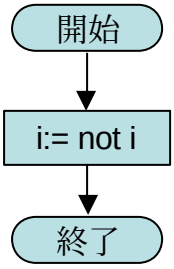


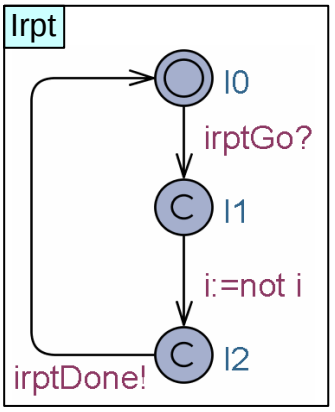
メイン処理のモデル(3/3)



割り込み処理のモデル

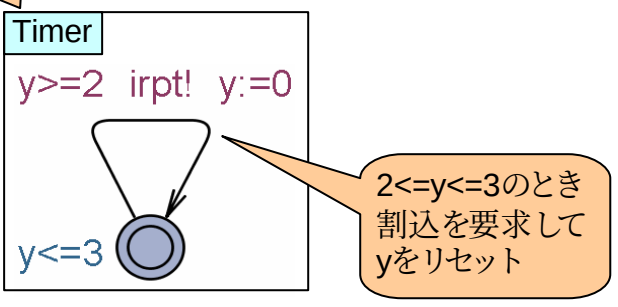
割り込み処理



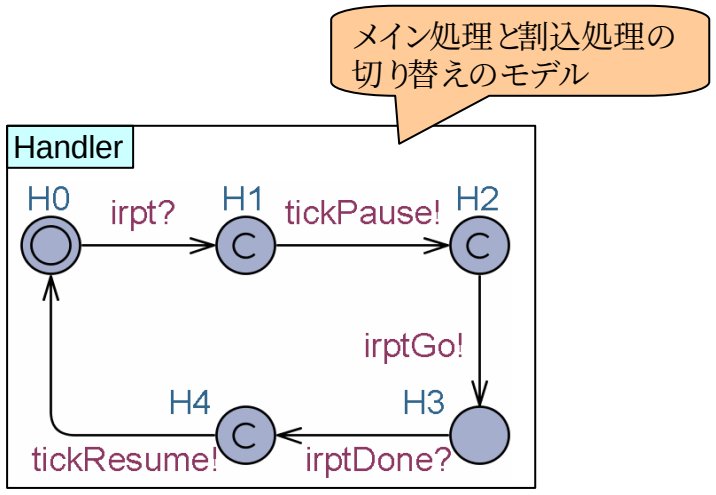


割り込みのモデル(1/2)

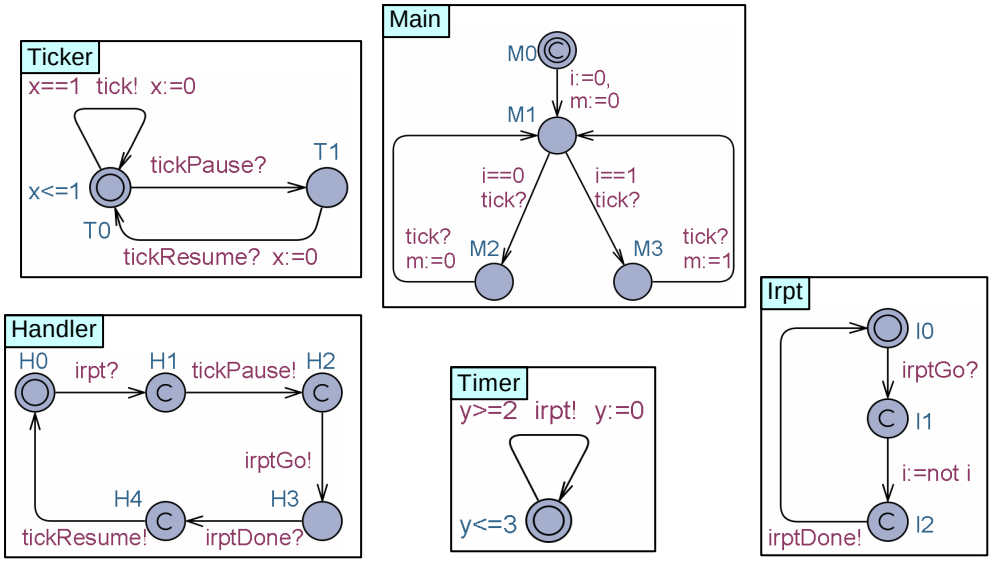
割込発生元のモデル



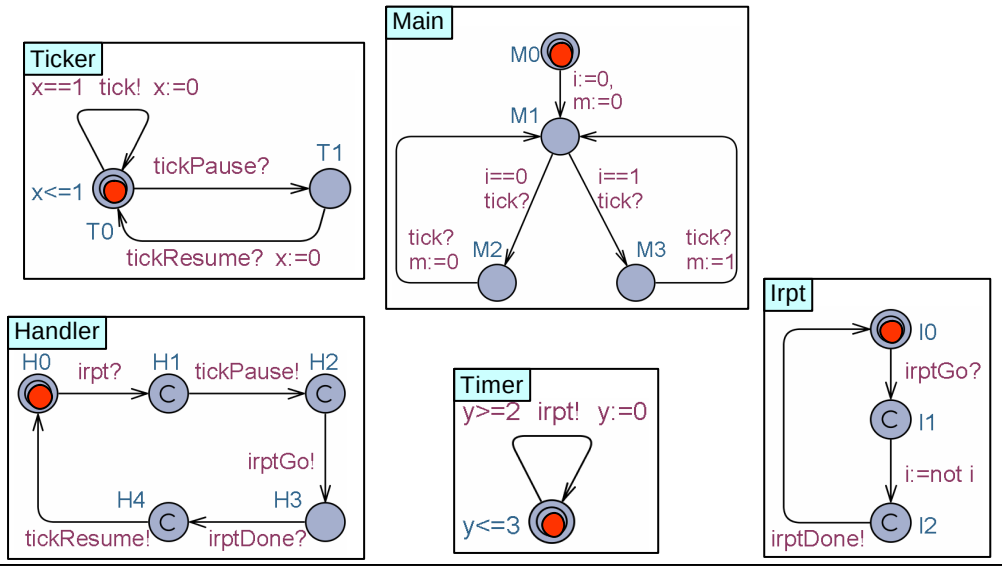
割り込みのモデル(2/2)



機能αのモデル(再掲)



動作のシミュレーション

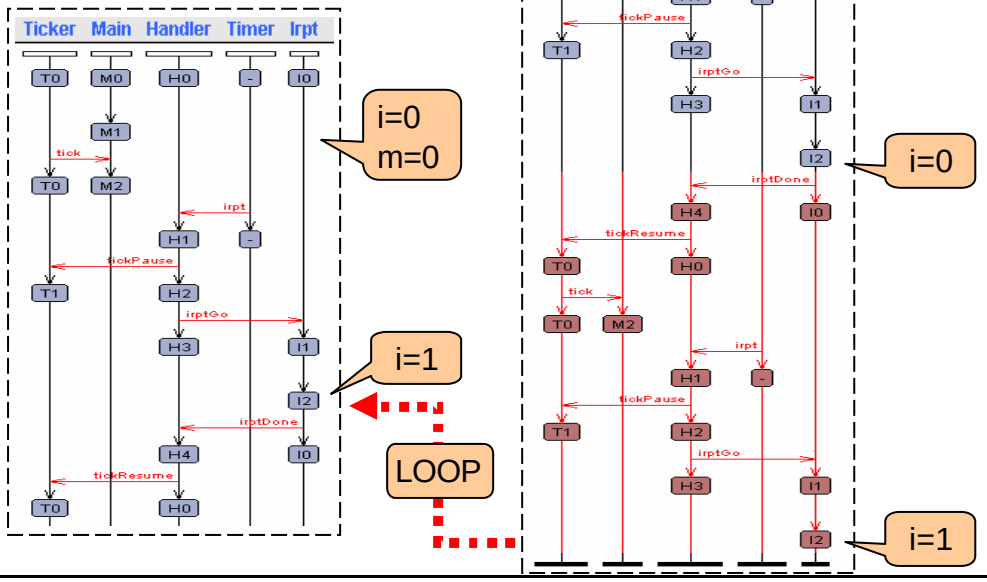


機能αの検査

検査項目	検査式	検査結果
デッドロックしない	A[] not deadlock	True
i=1となったらいずれm=1となる	i==1 --> m==1 ※AG(i==1 -> AF m==1)と同じ	False

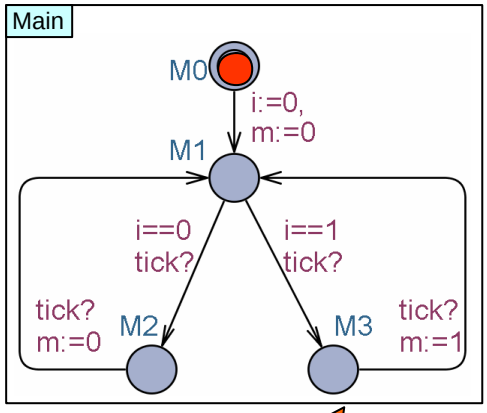
i=1となってもm=0であり続けることがある！

False の反例



Falseの反例解析

① M1へ遷移 (i=0, m=0)
② M2へ遷移
③ M2で割り込み発生して i=1
④ M1へ遷移 (m=0)
⑤ M1で割り込み発生して i=0
⑥ ②へ戻る



i=1となってもm=0であり続けることがある！

思いもよらないタイミングでの割り込み発生が原因

機能Y (再掲)

機能αと同様にモデル化できる

メイン処理

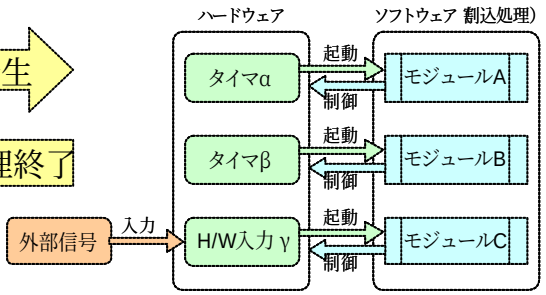
開始

モジュールD

割込発生

割込処理終了

割込処理　機能X）



機能Yのモデル

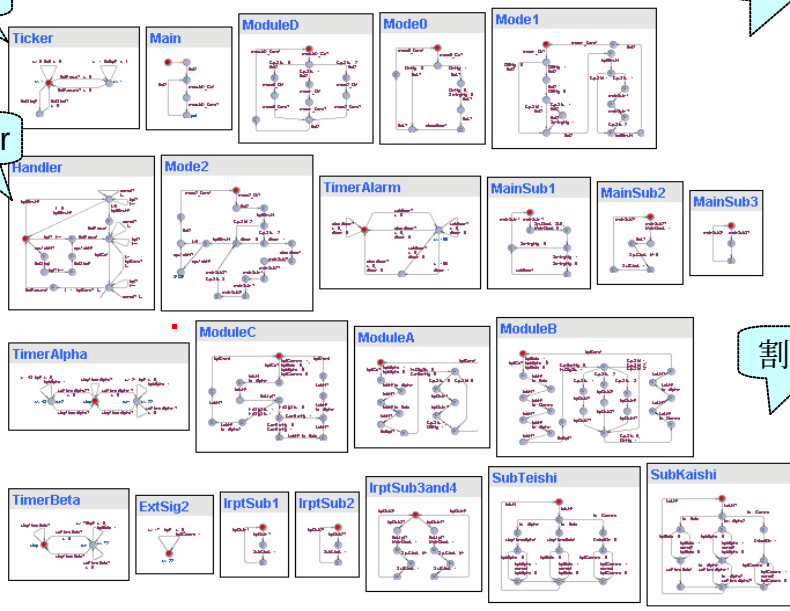
Ticker

Handler

Timer

メイン処理

割込処理



機能Yの検査例(再掲)

検査項目: システムの動作が中断状態にあるとき、CPUは状態Qであること

⇩ ツールで検査

検査結果：False
反 例：システムの動作が中断状態にあるとき、CPUは状態Qでないことがある

⇩ 反例の解析

原 因：モジュールDの実行中に、設計者が意図しないタイミングでタイマβによる割り込みが発生することがある

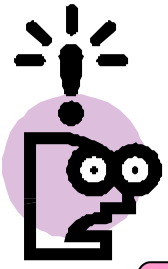
モデル検査の効能

Falseの反例が得られる

⇩

思いもよらないタイミングがわかる

- 思いもよらない 割り込み
- 思いもよらない 初期化 もれ
- 思いもよらない フラグup
- 思いもよらない invariantの崩れ

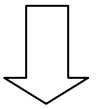


⇩

隠れた不備を発見するための重要な手がかり

モデル検査の副産物

モデル化や検査式の作成



- 仕様の理解が深まる
- 仕様の曖昧さがなくなる

まとめ

組み込みソフトウェア開発への モデル検査適用に
大きな手応えが得られた　独自の有効性をもつ）

- 組み込み機器はリアクティブ
- 部分はそうでもないが、組み合わさると一気に複雑に
- 外部環境やハードウェアも含めてモデル化して、
  実機試験の前に検査できる
- モデル = 外部環境 || ハードウェア || ソフトウェア
- あらゆる可能性を漏れなく確かめられる