組込みソフトウェア開発における イン-デザイン モデル検査

－設計工程における仕様書のモデル検査の提案－

関西電力株式会社 電力技術研究所 篠崎 孝一
独立行政法人 産業技術総合研究所 システム検証研究ラボ 水口 大知
東光精機株式会社 NW機器開発部 石井 健志

概　要

•イン-デザイン モデル検査の提案

ソフトウェア開発の設計工程で、仕様書のモデル検査を行う。
仕様書の不備、早期検出 修正を目指す。

•イン-デザイン モデル検査の試行

実際の組込みソフトウェア開発について試行した。
モデル検査の導入教育を実施した。
開発者とモデル検査技術者が協力して検査を実施した。
現実的な時間で、導入して検査結果が得られる

発表の構成

1. イン-デザイン モデル検査
2. ソフトウェア開発工程への適用
3. 仕様書のモデル化
4. モデル検査の実施
5. 実施結果
6. 今後の取り組み

仕様書の問題点

個別の項目内は正しくても、別の項目と矛盾する

問題点の見落とし

異常時(*)処理が不十分

(*)例
- 突然の停電、電源復帰
- 操作手順誤り、ランダム操作
- 複数の操作を、同時に実施
- 機械的な故障発生

起こりうる問題
- デッドロック 無限ループ)
- 想定外動作の発生
- 動作の不安定

仕様書のチェック

過去の経験と異なる不具合は発見が困難

システムの理解が不十分になりがち

経験者の査読）

（レビュー会議）

全ての可能性を考慮することは、不可能である。

イン-デザイン モデル検査とは

設計段階で、仕様書の内容をモデル検査することにより、問題点を解消して設計の品質を上げる。

仕様書 → モデル検査

手戻りが減少して開発期間が短縮する。

仕様書までの 手戻りをゼロにする。

設計 → 製作（コード化） → 組込テスト → 販売 保守

影響の大きな手戻りの発生を未然防止する。

モデル検査の特質

網羅的な検査ができる
- モデルと検査項目だけ記述すればよい
- ツールが全ての状態遷移をつくして計算
- テストパターンが必要ない

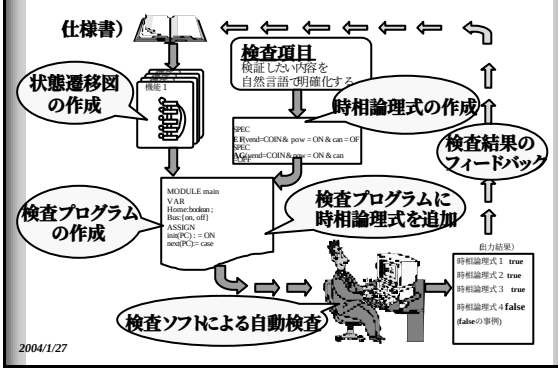
→ 検査ツールとして強力

状態数が巨大なモデルは扱えない
- メモリオーバーや計算の発散が起こる
- 検査の精度とモデルの状態数の板ばさみ

→ 仕様書の検査なら実用可能

仕様書のモデル検査は、ソフトウェア開発の効率化 品質向上に大きく寄与できる

イン-デザイン モデル検査の流れ



本研究でのモデル検査体制

ソフトウェア開発者	モデル検査研究者
・開発システム OK ・モデル検査 ？	・開発システム ？ ・モデル検査 OK

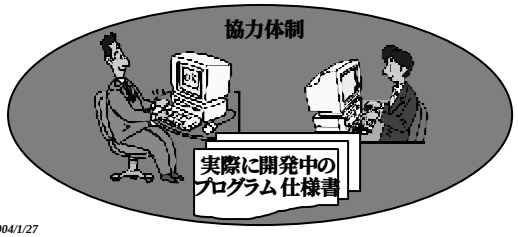


表1 モデル検査の教育

モデル検査の考え方	8時間
モデル検査言語（SMV）	30時間
モデル検査例題演習	50時間

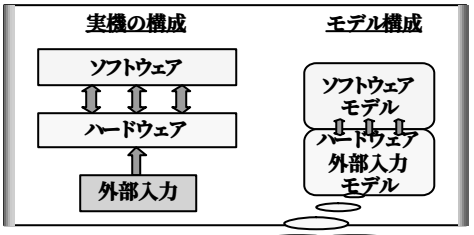
言語：SMV, Spin, etc.

合計 88時間

表2 モデル検査対象

CPU	8bit
OS	搭載せず
割り込み要因	8種類
記述言語	C言語
モデル検査対象	約600行
ステップ数	約600行 （全3500行のうち）

図3 モデル組み合わせの例

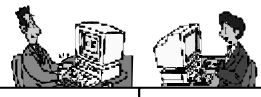


仕様書のモデル化には、
ノウハウが沢山あることが判明

発表の構成

1. イン-デザイン モデル検査
2. ソフトウェア開発工程への適用
3. 仕様書のモデル化
4. モデル検査の実施
5. 実施結果
6. 今後の取り組み

表3 使用した計算機環境



CPU	32bit
動作周波数	3GHz
メモリー	4GB

表4 ソースコードに対するSMVデータ

項　目		数　量
C言語のソースコード		約600行
SMVソースコードの行数	ハード部分	約700行
	ソフト部分	約1200行
SMVでの状態数		約3000万

表5 モデル検査に要した時間

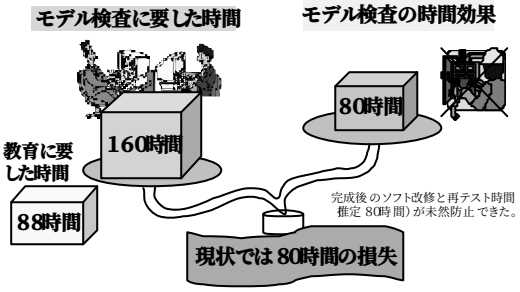
作業内容	項　目	時間
仕様書のモデル化	ハード部分	4
	ソフト部分	2
モデルのコード化	ハード部分	2
	ソフト部分	4
モデル検査（SMVの実行時間）		132
検査結果 「false」の反例解析		16

合計160時間

表6 検出できた不備の要因

不備の要因	件数
開発者が想定していない変数に対する不正なアクセス	3
開発者が想定していない割り込みの発生	1
開発者が想定していない外部入力	1
割り込み処理のオーバーヘッド	1
仕様書の記入不足	1

モデル検査の効果算定



イン-デザイン モデル検査の実用性

教える方も初めて教えた

実用ノウハウも集まっていない

最低限の効果算定方法

80時間の損失

現実的な時間で実施できた。

実用可能なレベルにある

取り組みで判明した課題を改善して実用性能を、さらに改善できる

表7 イン-デザイン モデル検査の課題

項　目	説　明
1.導入教育の効率化	専門書はあるが, 実用面に重点を置いた教材がない.
2.モデル化のノウハウ蓄積	最初からノウハウを知っていれば, もっと効率的に実施できた.
3.検査手法の操作性向上	モデル検査器（SMV）の操作性が悪い.

今後の取り組み

- 開発者向けの教材開発
- モデル化ノウハウの習得と蓄積
- モデル検査器の操作性の改善
- 検査を行う仕様書のレベル（上/下流）の指標検討

産業技術総合研究所システム検証研究ラボを中心に企業向けセミナーを準備中