

FTAに基づくEvent-Bリファインメントの手順化

佐藤直人

開発における問題点

- 【目標】**
Event-Bをソフトウェア開発に適用し、仕様が要件を満たすことを検証したい。
- 【課題】**
- リファインメントを軸とするEvent-Bモデリング方針の策定が困難
 - 教科書や先行事例は「結果」のみで、モデリング方針策定までの思考過程は読取り困難

手法・ツールの提案による解決

- リファインメントの手順化により、左記モデリング方針策定の「思考過程」を定型化
- 上記手順に従うことで、Event-Bモデルの作成・検証が可能

アプローチ

【リファインメントの難しさ】

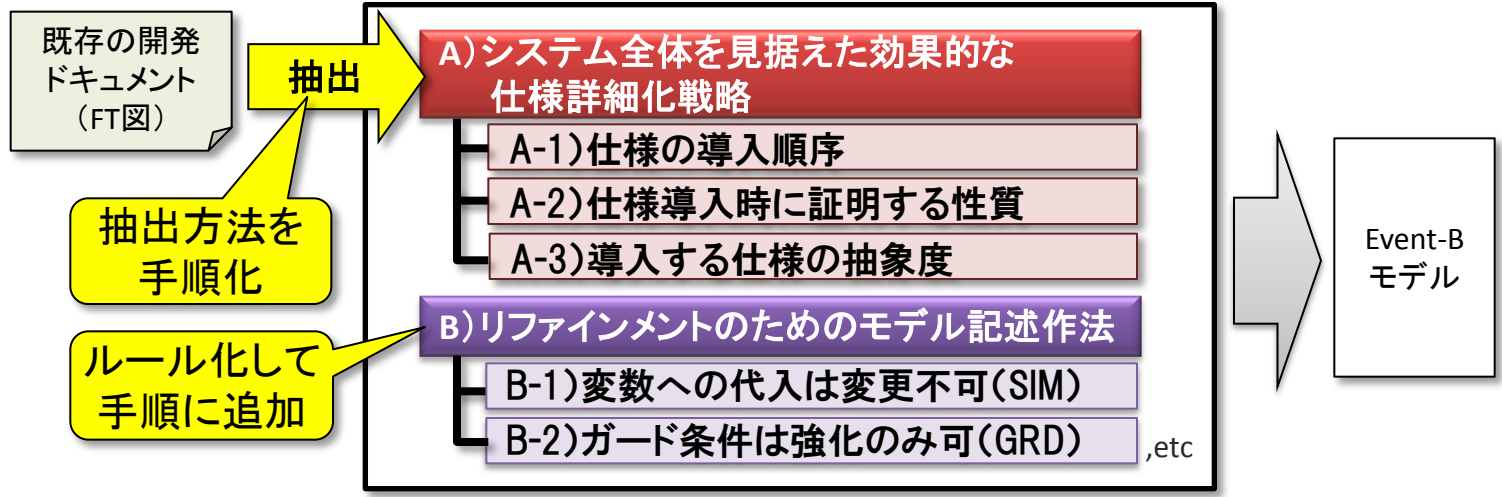
- 仕様詳細化戦略とモデル記述作法を同時に考慮
- モデル記述手戻り防止のためには、システム全体の正確な理解が必要



【アプローチ】

- 既存の開発ドキュメントから、システム全体を見据えた効果的な仕様詳細化戦略を抽出
- モデル記述作法は、ルール化して手順に追加

【リファインメントに必要な情報】



適用実験

- 提案したリファインメント手順を評価するため、2件の適用実験を実施
- その結果、Event-Bモデルの作成・証明に成功し、提案手順の有効性を実証

【適用実験結果】

| No | 対象システム | モデル規模 (マシン数) | 証明責務総数 | 自動証明数 | 対話証明数 | 自動証明率 |
|-----|-----------|--------------|--------|-------|-------|-------|
| (1) | 多重系制御システム | 11 | 121 | 92 | 29 | 76.0% |
| (2) | 信号制御システム | 5 | 63 | 59 | 4 | 93.7% |

【適用実験(2)に使用した信号制御システム】

