トップエスイー修了制作

Event-Bによる離散コントロールシステムの分析手法の提案

東京大学大学院　　小林 努　　t-kobayashi@nii.ac.jp

開発における問題点

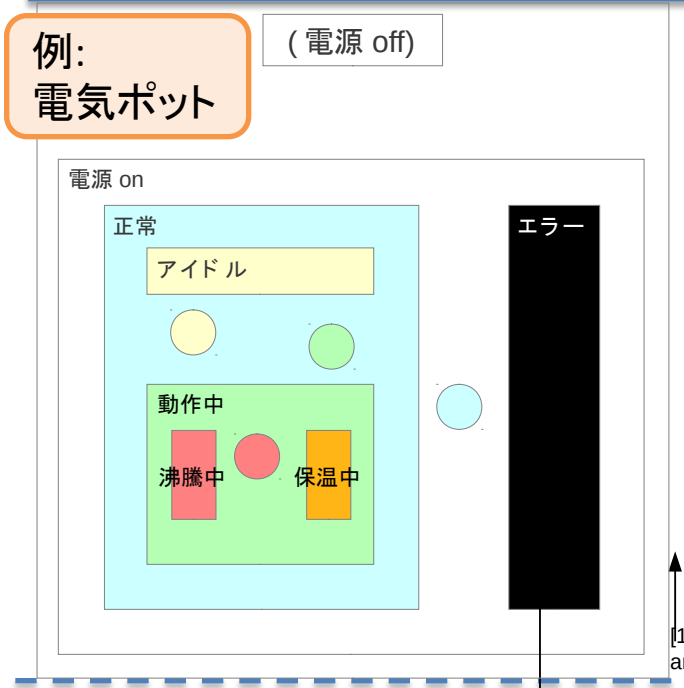
センサを用いて外部環境とやり取りするシステムのソフトウェアの検証を行うために、Event-Bを用いて仕様を詳細化しながら検証を行う手法が有効である。しかし、(1)仕様の段階的詳細化の手順の決定 (2)検証する要件の列挙 (3)センシングを含まない仕様と含む仕様との環境の値の検知タイミングの違いの扱い が難しい。

手法・ツールの適用による解決

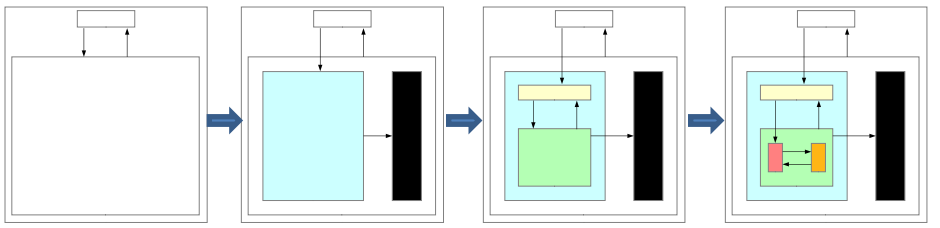
モードごとに振舞いを変えるソフトウェアのEvent-Bによる検証の手法をもとに新手法を提案した。新手法では(1)ソフトウェアのモードの階層的な定義、それに沿った詳細化 (3)時間差を吸収するモードの自動的な定義 により各問題を緩和した。また、既存手法でモードの定義から要件を自動的に列挙でき、(2)にも有効である。

階層的モード設計

例:
電気ポット



状態空間の段階的な分割としてモードを設計



- モードの階層構造に従ったリファインメント
- Event-Bで見通し良く仕様を記述できる
- モードの定義から検証項目が得られる[1]

[1] Fernando Dotti, Alexei Iliasov, Leila Riberiro, Alexander Romanovsky. Modal Systems: Specification, refinement and realization. In International Conference on Formal Engineering Methods – ICFEM 09, 2009

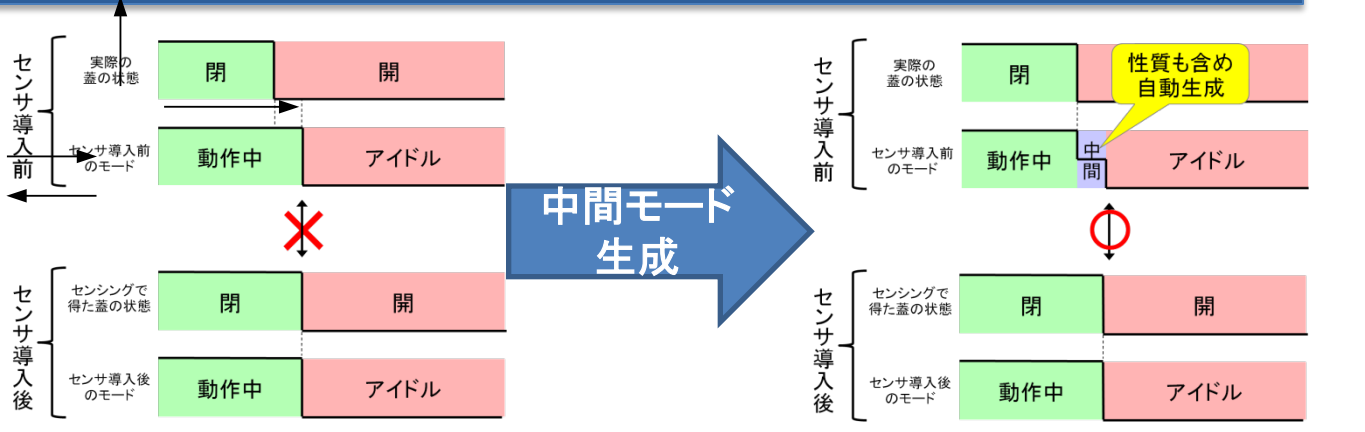
タイムラグを吸収する中間モードの自動生成

センサ・アクチュエータを操作するソフトウェアの仕様の詳細化は、Naïveに行うと一貫性を保てない

例: 蓋が開くと動作を止めたい

蓋センサの導入で検知タイミングが変化

同じ要件を検証できない



センサ導入前では「動作中ならば蓋が閉じている」が成立しない
→一貫性がない

センサ導入前でも「動作中ならば蓋が閉じている」が成立する
→一貫性がある