トップエスイー修了制作

Event-Bを利用した 安全要求仕様の導出と検証方法の提案

株式会社クレスコ　豊　裕介　y-toyo@cresco.co.jp

開発における問題点

安全要求仕様の作成は, システム仕様が確定する前に行われる為, (1)システムの動き, コンポーネントの性能および故障の動きに対して技術者間で共通の認識を持つのが難しく, 仕様を導出しにくい. また, 導出された仕様は, たいてい自然言語であり, (2)仕様作成段階で検証が出来ないという問題が存在する.

手法・ツールの提案による解決

数学的記述, 段階的記述, 証明による検証の特徴を持ち, 上流工程の仕様記述に適したEvent-Bでの解決を試みた. 単純にEvent-Bを適用するだけでは仕様記述は出来ても, 証明が困難になることが判明したので,「故障を考慮しない正常系モデルを確立し, 故障と対策を同時にモデル化する方法」を提案した.

Event-B適用の検討

【Event-B】

- システムレベルのモデリングと分析の為の形式手法
- 数学的記述(集合・定数, それらの関係性の定義)
- リファインメント(段階的記述)

上位モデルの性質を保つ

Model1 → Model2

Model1に対して
・機能の追加
・記載粒度詳細化
が可能

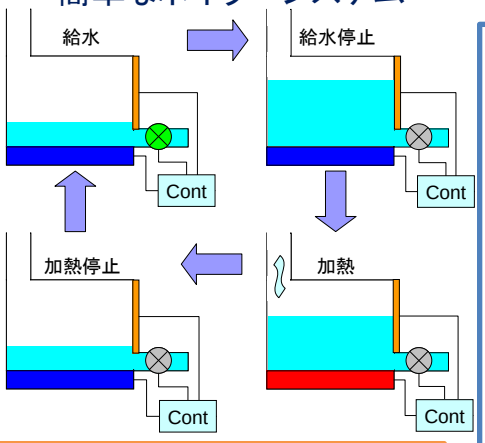
- 証明(どのイベントが発生しても, 性質が成り立つか？)

今回のアプローチでの使い方

数学的記述・・・コンポーネントの性能の仮定
リファインメント・・・コンポーネントの動作, 故障, 対策の記述を徐々に追加
証明・・・安全な状態が常に成立する事の確認

【適用実験】

簡単なボイラーシステム



安全状態：溢れ、空焚きなし
ポンプ、ヒータの故障　⇒　停止
センサ故障　⇒水位と異なる値

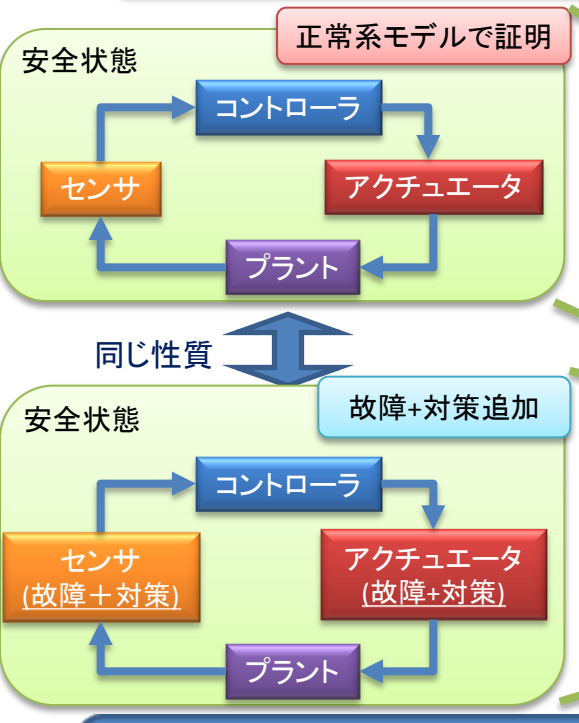
リファインメントによる段階的記述

故障と対策を含めて徐々にシステム化

水位の変化
↓
センサ(故障, 対策含)
↓
コントローラ
↓
ポンプ(故障, 対策含)
↓
ヒータ(故障, 対策含)
↓
安全状態の証明

モデルが複雑になり過ぎて、証明困難

提案方法と効果, Event-B適用のメリット



正常系モデル確立
「故障と対策」追加
↓
水位の変化
↓
センサ, コントローラ
ポンプ, ヒータ
↓
安全状態の証明
↓
ポンプの故障, 対策
↓
ヒータの故障, 対策
↓
センサの故障, 対策

仕様を導出し, 証明出来た！

メリット:
ポンプとヒータの性能を仮定し, 水位との関係性を定義
⇒具体的なコンポーネントが決まっていなくても, 仕様を導出した.

提案方法の効果:
正常系モデルで証明を行うことで, 以降のモデルの証明作業を楽にし, 安全状態が成り立つ仕様の検証に成功した.

まとめ

提案方法のポイント

- 故障を考慮しないシステムを早期にモデル化 → 証明
- 故障と対策を追加し,「故障を考慮しないシステム」と同じように見えるリファインメント

今後の課題

- 実例を増やす (他システム適用, 故障のバリエーション)
- 実開発のプロセスへの組み込みの検討
- 各種安全規格を意識したモデル化の検討

NII 国立情報学研究所 National Institute of Informatics
トップエスイー ～サイエンスによる知的のものづくり教育プログラム～