要求工学における FTA とフォーマルメソッド

本論文は、実効的かつ明確な要求工学のための FTA(故障木解析)と形式技法に関する研究である。すなわち、システム解析、設計、検証を支援するためにどのように故障木を形式的に正しく構築するか、FTA と形式技法の一貫性のある結合とはどのようなものかということについて述べる。

本研究では、従来の故障木の不正確さの問題に着目し、最初に時間論理の単調性に基づいた新しい形式的故障木の構成モデルを提案する。そして、CafeOBJ(複数の論理的な基礎に基づいた広範囲にわたる仕様記述言語)で OTS（観測遷移機械）を記述し、実際にどのように形式的にシステムをモデル化し、仕様を記述し、検証をするのかを OTS による故障木の解析結果から説明する。そして CafeOBJ の定理証明の技術を補うものとして、どのように OTS のモデル検査を Maude(CafeOBJ の兄弟言語)を使って行うかも議論する。新しい形式的故障木解析は、安全性の解析(FTA)と要求解析(OTS/CafeOBJ による形式的仕様記述と検証)の組み合わせをより矛盾のないものにするため、OTS モデルに基づいて提案された。
最後に、より詳しい説明と形式的故障木の意味論の分析を紹介し、どのように故障木解析の結果をシステムの形式的仕様へと変換するかを共通署名と OTS のフレームワークを使って説明する。

本研究での技術的な貢献は次の通りである：

- 本研究では、統合プラットホーム OTS/CafeOBJ の上で研究を行った。OTS/CareOBJ は FTA と形式的仕様と検証の組み合わせをより滑らかに矛盾なく行える；
  - 故障の事象の分割は、故障木の正確さを保証するキーポイントとなることを確認した。つまり、副事象は、与えられた論理ゲートを通じてそれらの主事象から生じなければならない。故障木の正確さを保証するための方法として、時間論理に基づいた形式的故障木の構成モデルを提案する；
  - システム設計と検証を支援するために、FTA から具体的な要求（安全性の仮定と確約）を導出するための方法を提案する；
  - どのように故障木の仕様を書き、故障木の最小カットセットの自動計算を実現するかを CafeOBJ の（TRS）項書き換え系を用いて説明する；
  - どのように OTS を CafeOBJ で形式的にモデル化し、記述し、検証するかを FTA の分析結果に基づいて説明する；
  - 最も重要なこととして、OTS の基本概念を導入することにより、新たな形式的故障木解析を提案した。新規性は、OTS の共通フレームワークを使用することにより、OTS/CafeOBJ でシステムの仕様を記述したり、検証するときに、故障木解析の結果を直接使えることが可能になった点である。したがって、安全性解析とソフトウェア要求の仕様のために共通の意味論モデルを構築した；
- 加えて、CafeOBJ の定理証明技術の補完として、提案方法をより完全なものとするためにどのように OTS を Maude でモデルチェックするかを説明する。

キーワード: 故障木解析、形式技法、要求工学、定理証明、モデルチェック、CafeOBJ, Maude