Title	要求工学におけるFTAとフォーマルメソッド
Author(s)	向，剣文
Citation	
Issue Date	2005-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/974
Rights	
Description	Supervisor:二木　厚吉，情報科学研究科，博士

Fault Tree Analysis and Formal Methods for Requirements Engineering

This thesis is concerned with fault tree analysis (FTA) and formal methods for more efficient and precise requirements engineering, i.e., how to develop the fault trees in a formal correct way, and how to combine FTA and formal methods in a consistent way to assist system analysis, design, and verification.

In this thesis, focused on the incorrectness problem of traditional fault trees, we first propose a new formal fault tree construction model based on monotonicity of temporal logic, and demonstrate how to formally model, specify, and verify a system based on the analyzing results of fault trees with observational transition system (OTS) of CafeOBJ (a wide spectrum specification language based on multiple logical foundations). And as a complement of theorem proving technique of CafeOBJ, we also discuss how to model-check OTSs with Maude (a sibling language of CafeOBJ). A new formal fault tree analysis is then proposed based on the OTS model in order to make the combination of safety analysis (FTA) and requirements analysis (formal system specification and verification with OTS/CafeOBJ) more consistent. Finally, we present some further discussion and analysis of formal fault tree semantics and demonstrate how to transform the results of fault tree analysis into formal system specifications by using the common signature and framework of OTS.

The technical contributions of our work are as follows:

- We carry out our study on a unified platform – OTS/CafeOBJ, which makes the combination of FTA and formal system specification and verification more smooth and consistent.
    - We identify decomposition of fault events as a core issue that guarantees the correctness of the fault trees, i.e., the sub events must formally result in their top event through the given logic gate. As for a solution, we propose a formal fault tree construction model based on temporal logic to guarantee the correctness of the fault trees.
    - We propose an approach to derive concrete requirements (safety assumptions and commitments) from FTA so as to guild and assist system design and verification;
    - We demonstrate how to write fault tree specification and realize automatic calculation of minimal cut sets of fault trees with term rewriting system (TRS) of CafeOBJ;
    - We demonstrate how to formally model, specify, and verify OTSs with CafeOBJ based on the analyzing results of FTA.
    - Most importantly, we further propose a novel formal fault tree analysis by introducing the basic concepts of OTS. The point is that, by using a common framework of OTS, it is possible to use the results of fault tree analysis directly, when specifying and verifying the system with

OTS/CafeOBJ. Therefore, we build a common semantic model for safety analysis and software requirements specifications.

- In addition, as a complement of theorem proving technique provided by CafeOBJ, we also demonstrate how to model-check OTSs with Maude, which makes our method more complete.

Key words: *Fault Tree Analysis, Formal Methods, Requirements Engineering, Theorem Proving, Model Checking, CafeOBJ, Maude*