Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

— Master's Thesis —

Marking boundaries of fault trees and architectural description languages

What is it all about?

Fault trees are a prominent reliability modeling language extensively used in the industry daily. Since their inception as static fault trees in 1962, many extensions are proposed to fault trees to mitigate their limitations, e.g., dynamic fault trees, Boolean-logic driven Markov processes, state/event fault trees [KGF07], etc. Each extension has its pitfalls and a trade off exists between expressiveness, the existence of semantics, and an efficient analysis framework. While fault trees remain an effective way of conducting dependability studies, another domain of architectural description languages exists in a parallel world. The proponents of these formal design/architecture description languages for dependability studies argue that system descriptions should be used to automatically conduct dependability analysis. To this end, the COMPASS toolchain [BCK+09] offers a framework where a thorough formal analysis starting from an architecture description can be performed. We believe that state/event fault trees [KGF07] lie at the boundary of fault trees and formal design languages. The thesis of our work is: "State/event fault trees can be easily subsumed by COMPASS input language, i.e., SLIM". To support this thesis, we will study state/event fault trees and SLIM language to translate SEFTs to SLIM. At present, we neither have enough test vectors to provide an automatic translation nor can we provide sufficient proof of accuracy. However, from the available literature on state/event fault trees, we will try to qualitatively argue about the accuracy and effectiveness of our approach. In the test cases where we have quantitative results, we will use COMPASS to run the analysis.

What is to be done?

There are three parts of this work:

1. Translate SEFT constructs to SLIM,
2. Perform case studies to prove the accuracy of our approach,
3. Define an automatic translation from SEFTs to SLIM. For this, we will need SEFTs written in their standard syntax.

Requirements

- High motivation to work on the topics of dependability and reliability.
- Motivated enough to do work with different tools especially when things does not seem to progress.
- Familiarity with topics: model checking, Petri nets, Python. **The Most important trait to complete this thesis is a motivation to work hard to see results.**

What you can expect

- A work place in our student room.
- Access to our coffee machine.
- We will work together towards advancement of this interesting topic.

Contact

- Shahid Khan, shahid.khan@cs.rwth-aachen.de, Tel. 0241/80- 21212.

References

[BCK+09] Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri, The compass approach: Correctness, modelling and performability of aerospace systems, International conference on computer safety, reliability, and security, Springer, 2009, pp. 173–186.

[KGF07] Bernhard Kaiser, Catharina Gramlich, and Marc Förster, State/event fault trees—a safety analysis model for software-controlled systems, Reliability Engineering & System Safety **92** (2007), no. 11, 1521–1537.