NuFTA: A CASE Tool for Automatic Software Fault Tree Analysis

Sanghyun Yun, Dong-Ah Lee, Junbeom Yoo
Division of Computer Science and Engineering, Konkuk University
Dependable Software Laboratory
NuFTA

- A CASE tool for software fault tree analysis.
- Automatically generate and analyze software fault tree for an NuSCR output value.
- Combined with NuSRS 2.1 (A tool supports NuSCR).
Automatic SFTA from NuSCR

- Backward analyze a failure using templates for each NuSCR model.
Software Fault Tree Analysis

- Manually construct a fault tree and analyze with
- Quality of FTA is depends on expert’s knowledge and experience.

- Concernment: Software
  - No ware-out failure
  - Developer’s logic
NuSCR

- Formal requirement specification
- Modified SCR for Reactor Protection System
- Three models
  - SDT
  - FSM
  - TTS
Expansion of FSM and TTS

- FSM and TTS have states whose output value selected by previous state's output value and ingoing transition's assignment.
  - It is difficult analyze one state's total output value.

- Our solution: Annotated FSM and TTS
  - One state has previous state's name and output value
  - Reordered transitions which present new states' relation
Templates

- We use templates for mechanical generation of software fault tree.
- Templates support NuSCR models, respectively.

A template for FSM
Generated SFT

A full software fault tree

Sub fault tree
Conclusion & Further work

• We propose a CASE tool which automatically analyze software fault tree from NuSCR formal requirement specification.

• For backward analyze output value’s cause, we should consider all system’s state.
  – It is difficult analyze a system’s requirement specification which have large value.
  – NuFTA also need many time for that.

• We will interpret software fault tree to logical formula for use the result of analysis.