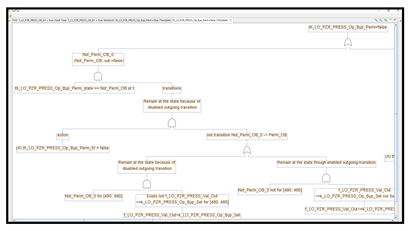
NuFTA 2.0: New Templates and an Automatic Generator of Fault tree for NuSCR

Junik Son, Yonghyun Kim, Kukbin Jeong, Dong-Ah Lee, Junbeom Yoo

Division of Computer Science and Engineering, Konkuk University

NuFTA 2.0



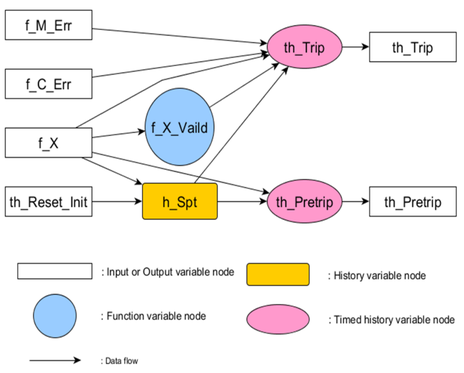
◎ A CASE tool for software fault tree analysis

◎ Automatically generate fault tree, logic formula and minimal cut-sets using NuSCR

◎ Introduce the concept of set and change the template

◎ Performs backward analysis using a fault that expert defined

NuSCR : Formal specfication Language for NPPs



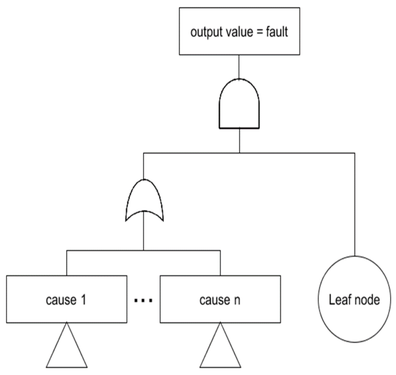
◎ NuSCR

A formal software requirements specification method of KNICS(Korea Nuclear Instrumentation and Control System) RPS(Reactor Protection System)

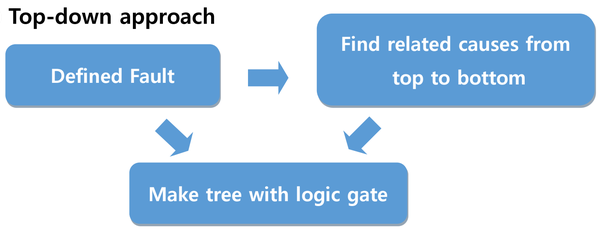
◎ 3 Variable model

- Function variable node (SDT)
  : mathematical functional behavior of a system
- History variable node (FSM)
  : state-based behavior of a system
- Timed history variable node (TTS)
  : timed-related behavior of a system

Software Fault Tree Analysis



◎ Top-down approach



◎ A hazard analysis method for software of safety critical systems

◎ Used language dependent templates

◎ Quality of FTA is depends on experts knowledge and experience

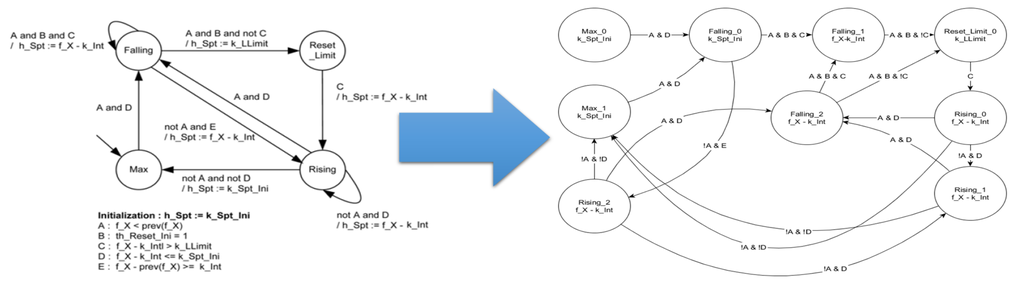
Expansion of FSM and TTS

◎ FSM and TTS have states whose output value selected by previous state's output value and ingoing transition's assignment

- It's difficult to analyze one state's total output value

◎ Solution : Annotated FSM and TTS

- One state has all previous state's names, an ingoing condition, all outgoing conditions and output value
- Reordered transitions which present new states relation



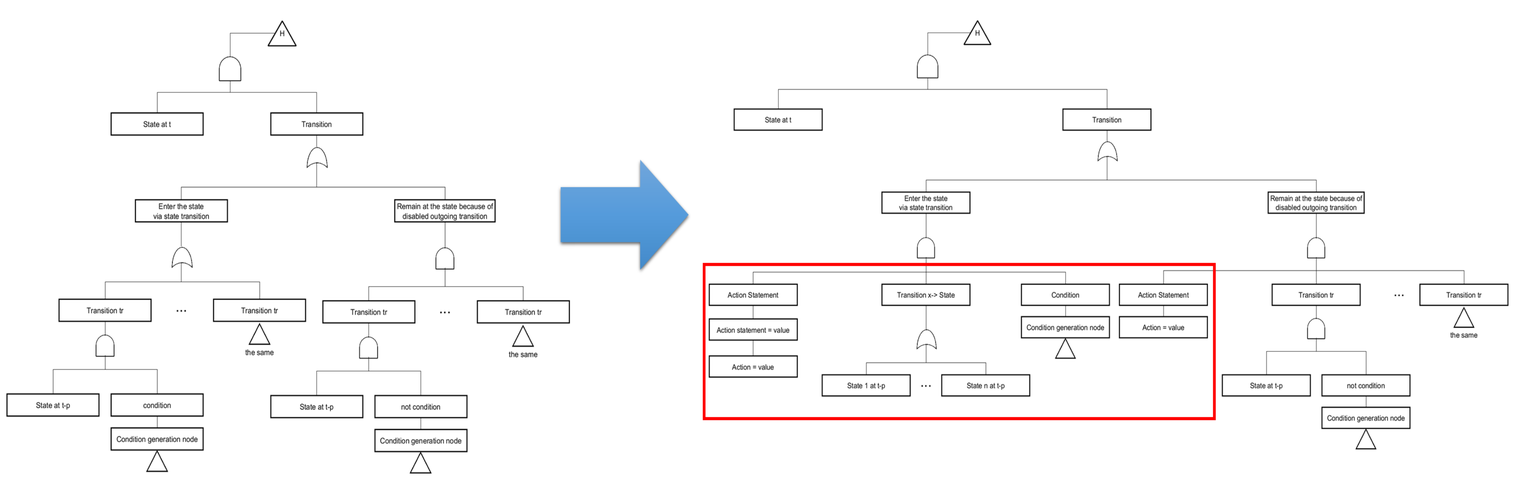
◎ Action statements is able to be causes when output of other variable node is appeared in an output of a current variable node

◎ The previous version of the template for FSM and TTS generates duplicate conditions in a tree

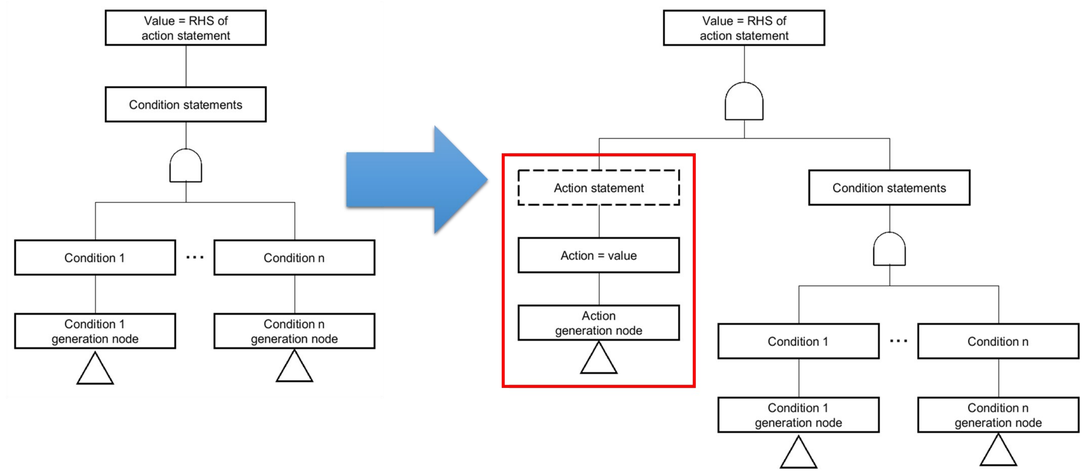
◎ Solution : Change the template

- Add an action statement in the new version of the template
- In the case of "Enter the state via state transition" in FSM or TTS, condition statements are modified when an assignment of state is related to value of input.
- In the case of "Remain at the state because of disabled outgoing transition" in FSM or TTS, the output value of the action statement is a value which was a previous cycle output value of current Node.

New Templates for NuFTA - FSM

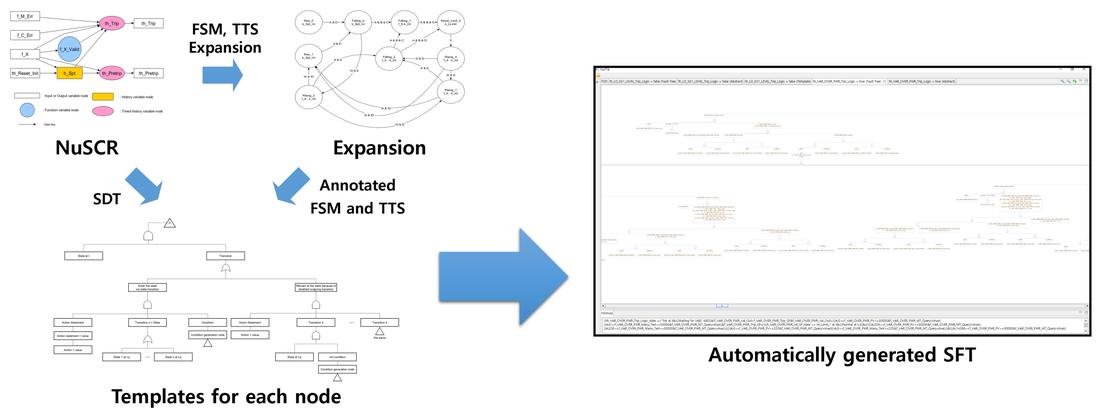


New Templates for NuFTA - SDT

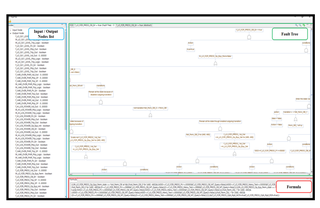


Automatic SFTA from NuSCR

◎ NuFTA 2.0 reads XML files written in NuSCR and automatically draws the fault tree according to an expert-defined fault.

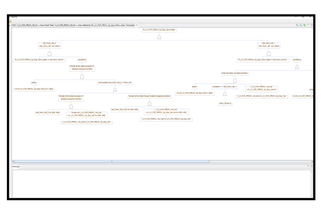


Generated Output of NuFTA 2.0



A full fault tree & formula

Abstract fault tree



Subtree

Cut-sets

◎ Generate fault tree and formula using fault that user defined

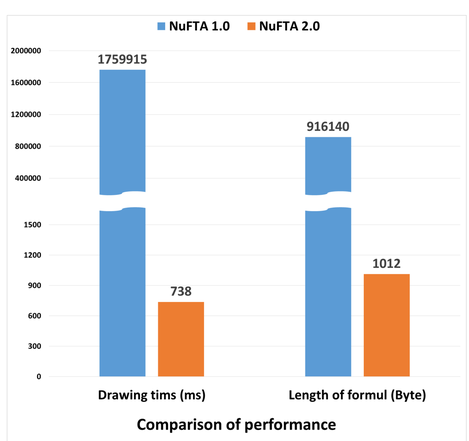
◎ Generate abstract fault tree

- This is composed of logic gate and variable node which is related to the fault that user defined

◎ Generate subtree

◎ Generate cut-sets using fault tree and formula

Conclusion & Future Work



Comparison of performance

◎ We prosed a CASE tool which automatically generates fault tree, logical formula and minimal cut-sets from NuSCR to assistance Fault Tree Analysis

◎ We improved fault tree drawing time and length of formula compared to the previous version

◎ We will study how to extract minimal cut-sets and analyze time constrains in TTS for analysis of multiple cycles.