
Abstract
ET: Enhanced tool (solution strategy)
The effectiveness of software fault tree analysis in supporting the design of safe software has been demonstrated. An enhanced tool / method is described for the design of product lines of safe software based on a technique for building a fault analysis tree containing subtrees that can be reused across multiple products within the same product line. Examples are provided confirming the effectiveness of its support for product line development in design.

Question - [Method/means of development]
<model-type / solution strategy>
What is the most tractable way of ensuring that an entire line of software products is safe?

<artifact-type>
The artifact being produced is a family of software implementations. The question is the best way to ensure that the implementations never enter unsafe states.

Results - [Procedure / technique]
<model-type / solution strategy>
The authors propose a technique for constructing reusable fault analysis trees. By building trees in a bottom-up fashion, and by documenting the trees’ findings in a concise table, the technique promises to provide significant leverage for the identification of sub-trees that may be reused for the analysis of multiple products within the same family. The authors’ proposal essentially takes what we have learned about producing reusable software and applies it to the problem of reusing safety analysis models.

Validation – [Example]
<model-type / solution strategy>
The authors apply their technique to a “family” of two applications. They successfully demonstrate that their technique does produce some sub-trees that apply to both products. It is, of course, questionable whether the technique will be usable in the real world (under the usual pressures of a business environment), meaning that additional external validation would be beneficial in future work.