# Article Analysis: Safety-Critical Software Engineering and Fault Tree Analysis

The article I chose to analyze is titled, “Fault tree analysis for composite structural damages” published by the Journal of Aerospace Engineering in 2013. The purpose of this article is to “introduce a fault tree methodology to synthesize various damage modes of composite structures by identifying possible damage causes [1].” Fault tree analysis (FTA) was introduced by Bell Laboratories, and is a “method in system reliability, maintainability, and safety analysis [2].” FTA is a deductive process wherein combinations of failures that could cause undesired events are tested using a tree structure. The top node of the tree is the undesired (or top) event, and the children are damage causes that can contribute/lead to the occurrence of the top event. As stated by Bill Vesely of Nasa, “Deductive models backwardly resolve the causes for an event [3].” This article applies the FTA method to the problem of reducing damage to composite airframes.

“In the past decade, the usage of composite materials in commercial aircraft has grown significantly [1].” The authors of the article state that these types of structures are “susceptible to impact damage caused by bird strike, hail and tools impact [1].” They go on to mention that the breakdown of such structures occurs due to multiple damage modes and their interactions. “FTA can model root causes and identity weak links of a large system [1].” In this study, the authors apply FTA to a variety of damage causes using a tree structure, and analyze the results on a macroscopic level [1].” The majority of the article discusses this analysis, for a carbon fiber reinforced plastic (CFRP) composite structure.

The two types of analysis performed in this study are qualitative and quantitative; however, for FTA the focus is qualitative data. The important aspects of this analysis are structure importance, probability importance, and relative probability importance analysis. Structure importance analysis “is to analyze the degree of importance of every basic event influencing the top event, regardless of its probability of occurrence [1].” Next is probability importance. According to Zeng et al., “probability importance reflects the influence of the unreliability of the basic event to that of the top event [4].” Finally, relative probability importance is introduced to “measure the variation of top event probability from the basic event itself [1].” In this study, the authors use these techniques to determine the importance ranking of various damage causes to the CFRP composite structure.

My stance on the topic of Fault Tree Analysis is that it is an extremely useful and beneficial technique in resolving the causes of any system failure. “It provides a framework for thorough evaluation of a root event [3]” that needs to be prevented from occurring. I believe that it is a valuable tactic in safety engineering as it can provide useful information about how certain aspects of a system can contribute to the damage of the overall system. This information is crucial as it can be used to identify “main damage contributors so that actions and resources can be prioritized [1].” The concept of FTA relates to software architecture because just like software architecture, FTA is a tool that gives engineers the ability to purposely design excellent and elegant systems. Knowing how a system can potentially fail, will allow engineers to preplan and develop systems that avoid or combat such failures. Software architecture focuses on system design, analysis, and validation; and since FTA provides a means for maintaining the system once it has been created, they both go hand-in-hand.

## References

[1] X. Chen, H. Ren, C. Bil. (2013, May.). “Fault tree analysis for composite structural damages.” Journal of Aerospace Engineering. [On-line]. 228(9), pp. 1466-1474. Available: https://www.researchgate.net/publication/270620520_Fault_tree_analysis_for_composite_structural_damages [Jul. 16, 2016].

[2] S. Pilot. “What is a Fault Tree Analysis?” Internet: http://asq.org/quality-progress/2002/03/problem-solving/what-is-a-fault-tree-analysis.html, Mar. 2002 [Jul. 17, 2016].

[3] B. Vesely. “Fault Tree Analysis (FTA): Concepts and Applications.” Internet: https://www.hq.nasa.gov/office/codeq/risk/docs/ftacourse.pdf, [Jul. 17, 2016].

[4] S. Zeng, T. Zhao, J. Zhang. “Design and Analysis of System Reliability.” Beijing University of Aeronautics and Astronautics Press (2001).