Review Paper:

Fault Tree Analysis: A Review on Analysis, Simulation Tools and Reliability Dataset for Safety-critical Systems

Das Madhusmita*, Mohan Biju R. and Guddeti Ram Mohana Reddy
Department of Information Technology, National Institute of Technology Karnataka, Surathkal, INDIA
*madhusmitadas.197it004@nitk.edu.in

Abstract

Risk analysis is a crucial and prominent method to analyze the dependability attributes of safety-critical systems. Risk analysis comprises a wide variety of State-of-the-Art techniques. Out of these, this study only focuses on the Fault Tree Analysis (FTA) technique. Except for the evaluation techniques, we also paid attention to the survey of simulation tools along with the reliability datasets.

Keywords: Safety critical system, risk analysis, quantitative analysis, dependability attributes, qualitative analysis, sensitivity analysis.

Introduction

A safety-critical system evaluates the dependability attributes as its failure is a fatality to the environment[21]. In the current era, in every sector, usage of SCSs is increasing daily. Oil and gas refineries, transport, railway, aviation, medical, infrastructure, mining, automobile etc. are the industries that use the SCS. As the failure of the SCS is critical in nature, so risk analysis comes into the picture. To do the risk analysis, various State-of-the-Art techniques are available[8]. These are failure mode and effect analysis (FMEA)[31,7], failure mode effects and criticality analysis (FMECA)[7], hazard and operability study (HAZOP)[20], reliability block diagram (RBD)[23], fault tree analysis (FTA)[33], event tree analysis (ETA)[3], Petri-Net (PN)[37], Markov analysis (MA)[30,38], system availability estimator (SAVE) modelling language[15], architecture analysis and design language (AADL)[13], unified modified language (UML)[34], root cause analysis (RCA) etc. From the above list of risk assessment techniques, the FTA technique has been focused on in this survey.

The correctness of the aforementioned risk analysis techniques is measured by evaluating the dependability attributes. When a safety-critical system is discussed, dependability attributes refer to the crucial features and properties that guarantee the system's performance, availability and dependability in order to carry out its safety-related tasks. It is essential to have these characteristics to ensure that the system will function accurately and safely. Dependability attributes encompass several key elements such as reliability, availability, safety, security, integrity and maintainability[22]. A comprehensive analysis and risk assessment process is mandatory to address the aforementioned attributes and meet safety standards and regulations, such as those outlined in various safety standards (e.g. ISO 26262 for automotive systems, DO-178C for avionics, IEC 61508 for industrial systems etc.).

Both a simulated environment and mathematical modelling can be used to carry out the risk analysis. To simulate the various models for various safety- critical systems, there are numerous tools accessible over the past decades. Getting real-time reliability datasets to assess dependability attributes for different SCSs is quite difficult, so many benchmark datasets can be used for research purposes. This study also presents a list of some reliability datasets and an explanation of the tools.

Research Methodology

The goal of this study is to provide a comprehensive analysis of the FTA along with tools and datasets. We used selected keywords to search web databases for pertinent papers. As this review focuses on the fault tree risk assessment of SCSs, so the keywords selected are fault tree analysis, risk analysis, dependability attribute, risk assessment, reliability dataset, fault tree analysis simulation tool, or safety-critical system. The online databases are Google Scholar, IEE Explore, ACM Digital Library, Science Direct, Wiley Online Library, Springer Nature Link and Scopus.

Articles were excluded that are not related to the keywords and are not written in English. Articles presenting implementations of State-of-the-Art methods or FTA techniques are included.

Fault Tree Analysis (FTA)

It represents a literature survey of widely used FTA risk assessment methods by explaining the evaluation of the dependability attributes along with the tools and datasets. Fault Tree Analysis (FTA) is a deductive top-down graphical approach to analyze and understand the causes of failure within the system. FTA aids in comprehending the reasoning behind the occurrence of the contributing events that result in the top event failure. As a result, this study helps in system design and assists in identifying and fixing the vulnerabilities that led to the top event[36].

A fault tree is constructed by combining the event and gates. The events are represented as system-level events and component-level events. At the same time, the gates are of various types depending on the type of fault tree as explained in the study[33]. Similar to a static fault tree (SFT), the dynamic fault tree (DFT) has basic events, intermediate events, top events and static gates (AND, OR etc.)[17]. Additionally, it contains dynamic gates like Priority AND

(PAND), Function Dependency (FDEP) and "SPARE" that make it easier to describe recurrent ideas in reliability engineering. Quantitative, qualitative and sensitivity analysis are performed to prove the correctness of the FTA model of any safety-critical system. All the aforementioned analysis is carried out by evaluating the dependability attributes.

Quantitative Analysis: Quantitative evaluation is used for modeling the failure probabilities of the event or component. While evaluating the quantitative analysis of an FTA, the dependability attributes evaluation comes into the picture. Below is the list of the key terms associated with the dependability attributes. These are:

Modelling Failure Probability (P(t)): To know the likelihood of the top event, the failure probability needs to know which can be evaluated from the basic event probability. The basic event probability will be calculated from the failure rate of the events or components, which can be obtained from various sources of the reliability database. Based on the type of distribution followed by each component such as exponential, normal, lognormal, Weibull etc., the failure probability can be calculated using the respective equations. The range varies from 0 to 1.

Unreliability (F(t)): In the case of FTA, events are connected with the logic gates, so further evaluation can be carried out using the set theory of boolean logic.

Reliability (R(t)): This attribute signifies the ability to perform a specified task or deliver a certain outcome in a certain time period and without failure, which is evaluated using equation 1.

$$R(t) = 1 - F(t) \quad where \quad t > 0 \tag{1}$$

Expected number of failure (ENF): It is defined as the expected number of failure probability of the top event within the specified time limit as mentioned in equation 2.

$$ENF(t) = F(t) \quad where \quad t > 0 \tag{2}$$

Availability (A(t)): It is defined as the likelihood that the system functions correctly and it is calculated using equation 3

$$A(t) = \frac{MeanTimeToFailure(MTTF)}{MeanTimeBetweenFailure(MTBF)} \quad where \quad t > 0 \tag{3}$$

Mean Time to Failure (MTTF): MTTF assesses the system's reliability by evaluating the excepted or average time the device performs successfully.

The MTTF of the complete system[18] is given in equation 4:

$$MTTF = \int_0^\infty R(t)dt \tag{4}$$

For components following exponential distribution, the MTTF of the individual component is presented in the equation 5.

$$MTTF = 1/\lambda \text{ where } \lambda = \text{Failure rate of a component} \tag{5}$$

This metric is useful for non-repairable scenarios.

Mean Time to Repair (MTTR): MTTR is defined as the average time required to repair a system following a failure. It is useful for repairable components and is evaluated using equation 6:

$$MTTR = \frac{Maintenance\ Time}{Number\ of\ Repairs} \tag{6}$$

Mean Time between Failure (MTBF): MTBF evaluates the expected time between two consecutive failures. Basically, it justifies the lifespan of the system using the equation 7.

$$MTBF = MTTR + MTTF \tag{7}$$

Qualitative Analysis: Elucidating the redundant fault tree and identifying vulnerabilities are two purposes of the qualitative study of FTA. Qualitative analysis can be evaluated using minimal cut-sets (MCSs), minimal path-sets (MPSs)[6] and common cause failure (CCF)[33]. MCS is defined as a set of the minimum number of the basic events or components in a set that are responsible for the top event to fail. The techniques to analyze the MCSs of the FTA are:

Classical Method: This method includes Boolean Manipulation[16] and Binary Decision Diagram[1]. The boolean expression is represented in disjunctive normal form (DNF) where each conjunction is considered MCS. In the case of BDD, it is represented as a directed acyclic graph.

MOCUS Algorithm[14]: It is a computer program to obtain the MCS from the FTA using a top-down approach.

MICSUP Algorithm[29]: This algorithm is a computerized program using a bottom-up approach. MPS is defined as the combination of the components, that if they do not fail, the system remains functional. It is the complement of the MCS tree[6]. The CCF refers to the correlated failure of multiple events within a system due to a common cause. This can be added to the fault tree by using OR logical gate.

Sensitivity Analysis: To know the criticality of the events and the uncertainties associated with the events, sensitivity analysis is performed. Following are the methods to analyze the uncertainty associated with the parameter[9].

Fussel-Vesely (F-V) Importance Measures: This is a quantitative risk assessment to assess the importance or

criticality of the individual components in a safety-critical system. This can be evaluated using equation 8:

$$F - V_i = \frac{P(\textit{Failure Probability of } MCS_i)}{P(TE)} \quad (8)$$

where i = 1, 2, 3, ..., n number of events in FTA.

A higher F-V value indicates a greater contribution to the system risk.

Risk Reduction Worth (RRW): It is used to obtain the change of the top event probability by re-quantifying each basic event probability in the respective FTA as 0. It is obtained as mentioned in equation 9:

$$RRW_i = P(\textit{Old TE value}) - P(\textit{New TE value}) \quad (9)$$

Risk Achievement Worth (RAW): It analyzes the change of the top event probability by re-quantifying each basic event probability in the respective FTA as 1. It is obtained as mentioned in equation 10:

$$RAW_i = P(\textit{New TE value}) - P(\textit{Old TE value}) \quad (10)$$

Birnbaum Importance Measure (BM): It indicates the sensitivity of each event probability by adding RRW and RAW values for the same events presented using equation 11.

$$BM_i = RRW_i + RAW_i \quad (11)$$

To do all the above analysis, either mathematical modelling or simulation can be used. To evaluate the above-mentioned attributes, a reliability dataset is required. Some well-known datasets, along with the tools, have been listed in table 1 and 2.

Reliability Dataset: Getting real-time reliability data of the components or the system is quite difficult while evaluating the dependability attributes of the SCSs. To overcome this challenge, a reliability dataset can be used. Many reliability datasets are available to carry out the risk assessment process. But in this study, we focused on a few widely-used recent datasets presented in table 1. These datasets consist of the failure rate of the various components used for safety-critical systems.

FTA Tools: Implementing mathematical modeling of a complex system is quite time-consuming and error-prone even though it provides exact value. So, simulation comes into the picture to avoid the aforementioned drawbacks. In the current era, a lot of simulation tools are available related to risk and safety assessment. As this survey focuses only on the FTA, so it focused only on the survey of the FTA analysis tool. Out of all, only a few frequently used FTA evaluation tools are listed. The lists of the simulation tools are tabulated in table 2.

Conclusion

This study provides a survey of the various types of analysis to assess the FTA. Through this review, the significance of FTA lies in its ability to analyze and understand the risk associated with it, which contributes to the overall safety and reliability of the SCS. As FTA is limited to static evaluation, many drawbacks emerge, especially while evaluating dynamic complex systems. Currently, most of the SCSs are dynamic in nature, so static FTA cannot be that much reliable. To overcome this, the FTA model can be combined with other risk analysis techniques such as Markov analysis, Bayesian belief network, Petri-Nets etc.

Besides the survey of various analysis of the FTA, this study also focuses on the numerous reliability datasets along with the simulation tools.

Table 1
Reliability Dataset[39]

Reliability Dataset	Related Components	Application	Version
NPRD-2023[25]	Mechanical, Electromechanical and Electrical	Military/ Commercial	2023
EPRD-2014[11]	Electronic	Military/ Commercial	2014
FMD-2016[12]	Mechanical, Electromechanical, Electrical and Electronic	Military/ Commercial	2016
OREDA-2015[26]	Mechanical, Electromechanical, Electrical, Electronic onshore and offshore components	Oil/ Gas	2015
217Plus:2015[40]	Electrical and Electronic	Military/ Commercial	2015
MIL-HDBK-217F[24]	Electrical and Electronic	Military/ Commercial	2010

Table 2
List of FTA Tools[5]

FTA Tools	Type	Analysis	License	User-friendly
OpenFTA[2 8]	Static	Qualitative and	Quantitative - Open-source	GUI
OpenAltarica[2 7]	Static	Qualitative and Quantitative	Free	Programming Language
ALD Fault Analyzer[2]	Static	Qualitative and Quantitative	Free	GUI
Isograph Fault tree+[18]	Static	Quantitative	Licensed	GUI
ITEMtoolkit[1 9]	Static	Qualitative and Quantitative	Licensed	GUI
DFTCalc[4]	Static, Dynamic	and Quantitative	Open-source	GUI
Sharpe Tool[35]	Static	Qualitative and Quantitative	Licensed	GUI
Relyence Fault tree Software[32]	Static	Qualitative and Quantitative	Licensed	GUI

References

1. Akers, Binary decision diagrams, *IEEE Transactions on Computers*, **100(6)**, 509-516 **(1978)**

2. ALD Fault Tree Analyzer, https://www.fault-tree-analysis-software.com/ **(2024)**

3. Andrews J.D. and Dunnett S.J., Event-tree analysis using binary decision diagrams, *IEEE Transactions on Reliability*, **49(2)**, 230-238 **(2000)**

4. Arnold F., Belinfante A., Van der Berg F., Guck D. and Stoelinga M., DFTC alc: a tool for efficient fault tree analysis, Computer Safety, Reliability and Security: 32nd International Conference, SAFECOMP 2013, Springer, **32**, 293-301 **(2013)**

5. Baklouti A., Nguyen N., Choley J.Y., Mhenni F. and Mlika A., Free and open source fault tree analysis tools survey, 2017 Annual IEEE International Systems Conference (SysCon) IEEE, 1-8 **(2017)**

6. Barlow R.E. and Proschan F., Statistical theory of reliability and life testing: probability models, New York, Holt, Rinehart and Winston **(1975)**

7. Bouti A. and Kadi D.A., A state-of-the-art review of FMEA/FMECA, *International Journal of Reliability, Quality and Safety Engineering*, **1(04)**, 515-543 **(1994)**

8. Bozzano M. and Villafiorita A., Design and safety assessment of critical systems, CRC Press **(2010)**

9. Čepin M., Assessment of power system reliability: methods and applications, Springer Science & Business Media **(2011)**

10. DeLong T.A., Smith D.T. and Johnson B.W., Dependability metrics to assess safety-critical systems, *IEEE Transactions on Reliability*, **54(3)**, 498-505 **(2005)**

11. Electronic Parts Reliability Data EPRD-2014, https://www.quanterion.com/product/publications/electronic-parts-reliability-data-eprd-2014/ **(2014)**

12. Failure Mode / Mechanism Distributions FMD-2016, https://www.quanterion.com/product/tools/failure-mode-mechanism-distributions-fmd-2016 **(2016)**

13. Feiler P.H., Gluch D.P. and Hudak J., The architecture analysis & design language (AADL): An introduction, Carnegie Mellon University, 145 **(2006)**

14. Fussell J.B., Henry E.B. and Marshall N.H., MOCUS: A computer program to obtain minimal sets from fault trees, Aerojet Nuclear Co., Idaho Falls, ID (United States) **(1974)**

15. Goyal A., Carter W.C., deSouza-e-Silva E. and Lavenberg S.S., The system availability estimator, Twenty-Fifth International Symposium on Fault-Tolerant Computing, Highlights from Twenty-Five Years, 182 **(1995)**

16. Haasl D.F., Fault tree handbook, Office of Nuclear Regulatory Research, Nuclear Regulatory Commission, Washington, DC (USA), Technical Report **(1981)**

17. Ili´c S. and Gli˘sovi´c J., Dynamic fault tree analysis of lawnmower, Center for Quality **(2015)**

18. Isograph, https://www.isograph.com/software/reliability-workbench/fault-tree-analysis-software/ **(2024)**

19. ITEM Toolkit, https://www.itemsoft.com/fault_tree.html **(2024)**

20. Kletz T.A., Hazop & Hazan: identifying and assessing process industry hazards, CRC Press **(2018)**

21. Knight J.C., Safety critical systems: challenges and directions, Proceedings of the 24th international conference on software engineering, 547- 550 **(2002)**

22. Maurya A. and Kumar D., Reliability of safety-critical systems: A state-of-the-art review, *Quality and Reliability Engineering International*, **36(7)**, 2547-2568 **(2020)**

23. Modarres M., Kaminskiy M.P. and Krivtsov V., Reliability engineering and risk analysis: a practical guide, CRC Press **(2016)**

24. MIL-HDBK-217F, https://www.quanterion.com/wp-content/uploads/2014/09/MIL-HDBK-217F.pdf **(2014)**

25. Nonelectronic Parts Reliability Data (NPRD), Quanterion Solutions Incorporated, https://www.quanterion.com/nprd-2023/ **(2023)**

26. Offshore & onshore reliability data, https://www.oreda.com/ **(2024)**

27. OpenAltaRica, https://www.openaltarica.fr/ **(2024)**

28. OpenFTA, https://www.openfta.com/ **(2024)**

29. Pande P.K., Spector M.E. and Chatterjee P., Computerized fault tree analysis: TREEL and MICSUP, ORC 75-3, Operations Research Center, University of California, Berkeley **(1975)**

30. Pukite J. and Pukite P., Modeling for reliability analysis: Markov modeling for reliability, maintainability, safety and supportability analyses of complex systems, John Wiley & Sons **(1998)**

31. Rausand M. and Hoyland A., System reliability theory: models, statistical methods and applications, John Wiley & Sons **(2003)**

32. Relyence Fault tree software, https://relyence.com/products/fault-tree/ **(2024)**

33. Ruijters E. and Stoelinga M., Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools, *Computer Science Review*, **15**, 29-62 **(2015)**

34. Rumbaugh J., The unified modeling language reference manual, Pearson Education India **(2005)**

35. SHARPE (Symbolic Hierarchical Automated Reliability and Performance Evaluator) Tool, https://sharpe.pratt.duke.edu/ **(2024)**

36. Stamatelatos M., Vesely W., Dugan J., Fragola J., Minarick J. and Railsback J., Fault tree handbook with aerospace applications **(2002)**

37. Sunanda B.E. and Seetharamaiah P., Modeling of safety-critical systems using Petri nets, *ACM SIGSOFT Software Engineering Notes*, **40(1)**, 1-7 **(2015)**

38. Trivedi K.S. and Bobbio A., Reliability and availability engineering: modeling, analysis and applications, Cambridge University Press **(2017)**

39. Vintr Z. and Vintr M., Tools for components reliability prediction, *Advances in Automation and Robotics*, **2**, 317-319 **(2017)**

40. 217 Plus™: 2015 Calculator, https://www.quanterion.com/products-services/tools/217plus/ **(2015)**.

(Received 21st November 2024, accepted 25th December 2024)