Annals of Nuclear Energy 120 (2018) 666–681

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Advanced combinatorial method for solving complex fault trees

José de Jesús Rivero Oliva [a,*], Jesús Salomón Llanes [b], Manuel Perdomo Ojeda [b], Antonio Torres Valle [b]

[a] Departamento de Engenharia Nuclear, Universidade Federal do Rio de Janeiro (UFRJ), Brazil
[b] Instituto Superior de Tecnologías y Ciencias Aplicadas, Universidad de La Habana (UH), Cuba

ARTICLE INFO

Article history:
Received 12 March 2018
Received in revised form 24 May 2018
Accepted 11 June 2018

Keywords:
Fault tree analysis
Combinatorial method
Minimal cut set

ABSTRACT

Combinatorial explosion is a common problem to both predominant methods for solving fault trees: Minimal Cut Set (MCS) approach and Binary Decision Diagram (BDD). High memory consumption impedes the complete solution of very complex fault trees. Only approximated non-conservative solutions are possible in these cases using truncation or other simplification techniques. The paper proposes a new method (CSolv+) for solving complex fault trees, without any possibility of combinatorial explosion. Each individual MCS is immediately discarded after its contribution to the basic events importance measures and the Top gate Upper Bound Probability (TUBP) has been accounted. An estimation of the Top gate Exact Probability (TEP) is also provided. Therefore, running in a computers cluster, CSolv+ will guarantee the complete solution of complex fault trees. It was successfully applied to 40 fault trees from the Aralia fault trees data base, performing the evaluation of the top gate probability, the 1.000 Significant MCSs (SMCS) and the Fussell-Vesely, RRW and RAW importance measures for all basic events. The high complexity fault tree nus9601 was solved with truncation probabilities from 10^{-21} to 10^{-27}, just to limit the execution time. The solution corresponding to 10^{-27}, evaluated 3.530.592.796 MCSs in 3 h and 15 min.

1. Introduction

Probabilistic Safety Assessment (PSA) has proved to be essential for demonstrating Nuclear Power Plants (NPP) safety. It also gives an important support to the decision making process related to safety. In a PSA, the evaluation of accident sequences derived from event trees is usually performed through the fault tree linking of systems fault trees (IAEA, 2010). This fault tree linking comprises not only the failed systems but also those which remain in success state. As a result, very large fault trees, with success gates at the top gate level, must be analyzed. The evaluation embraces the determination of the total risk (or failure probability), the most important accident scenarios (Significant Minimal Cut Sets) and the contribution of each basic event to the global value in terms of importance measures, as well as uncertainty and sensitivity analyses (IAEA, 2010).

Most of the NPP PSAs is evaluated applying the kinetic tree theory (Vesely, 1970), also known as the MCS approach or the "traditional" method. In the MCS approach the fault tree gates are systematically substituted by their entries, applying the Boolean algebra laws in several stages, until the top-event Boolean expression contains only basic events. The final form of the Boolean equation is an irreducible logical union of sets of basic events, denominated Minimal Cut Sets (MCSs). This process is characterized by a continuous and time consuming expansion of the amount of events combinations, demanding important memory resources. For large fault trees the combinatorial explosion impedes the complete evaluation[1], and only approximate solutions can be obtained using truncation methods (Ibáñez-Llano et al., 2010). Truncation is a non-conservative approach that reduces the amount of MCSs retained in the model, discarding those with negligible contribution to the total risk because of their low probability.

An alternative and very successful method of fault tree evaluation is based on the construction of a new structure, a Binary Decision Diagram (BDD) (Rauzy, 1993). The fault tree is converted into a BDD, which is a compact data structure representing the logical model of the top-event. The BDD can be evaluated completely

---

* Corresponding author at: Departamento de Engenharia Nuclear, Escola Politécnica, Universidade Federal do Rio de Janeiro (UFRJ), Av. Horácio Macedo, 2030, Bloco G, Sala 206, Cidade Universitária, CEP: 21.941-914 Rio de Janeiro, RJ, Brazil.

E-mail addresses: rivero@nuclear.ufrj.br (J.J. Rivero Oliva), jesuss50@nauta.cu (J. Salomón Llanes), mperdomo@instec.cu (M. Perdomo Ojeda), atorres@instec.cu (A. Torres Valle).

[1] Complete evaluation/solution: An evaluation (solution) of a fault tree based on the total amount of minimal cut sets, without truncation. CSolv+ performs this evaluation in the rare event approximation.

https://doi.org/10.1016/j.anucene.2018.06.019
0306-4549/

and more efficiently in comparison with the kinetic tree theory, determining the exact probability of the top-event without the need to obtain MCSs as intermediate results (Remenyte-Prescott, 2007).

“They have proved to be the most efficient tool to assess Boolean models such as fault trees. BDD make it possible to assess the top-event probability in an exact and very efficient way. BDD can be used to compute and to encode very large sets of MCS” (Rauzy, 2001).

“Many fault trees that could be analyzed only with the MCS approach by using the cut-off technique, could indeed be analyzed with the BDD approach without adopting any approximation” (Contini and Matuzas, 2011).

Unfortunately, memory consumption remains as a limitation (Deng et al., 2015) when a large fault tree leads to an extremely large BDD impossible to construct (Wang et al., 2016). Therefore, the BDD method does not avoid the combinatorial explosion. Only small and medium fault trees, up to several hundred of basic events can be evaluated completely (Ibáñez-Llano et al., 2010). More complex fault trees need the use of truncation and other simplification techniques. Additionally, the size of the BDD and, consequently, the efficiency of the method, strongly depend on the order in which the basic events are selected (Deng et al., 2015; Wang et al., 2016).

The problem of combinatorial explosion has been extensively treated in several references as an unresolved issue requiring further developments:

- “Nowadays, fault trees with several hundred gates and basic events have to be assessed. Despite their great efficiency, BDD sometimes fail to handle such models because they cannot avoid the exponential blow-up that results from manipulation of such large numbers of gates and events. Therefore, approximations have to be made” (Rauzy, 2001).
- “No scheme has been found that will produce a BDD (minimal or otherwise) for some large fault trees” (Reay, 2002).
- “Since the BDD algorithm is highly time and memory consuming, especially for large problems, it has been difficult to solve large reliability problems such as fault trees for accident sequences in a Probabilistic Safety Assessment (PSA)” (Jung et al., 2008).
- “During the analysis of very complex fault trees it may happen that the working memory is not sufficient to store the large BDD (LBDD) structure, since the number of nodes increases exponentially with the complexity of the fault tree” (Contini and Matuzas, 2010).
- “The main limitation in the analysis of complex fault trees is the insufficient working memory. This problem is common to all methods based on MCSs as well as those based on BDD” (Contini and Matuzas, 2011).
- “When solving a large FT in BDD algorithm, the high memory consumption is a limitation … BDD algorithm is an efficient method to perform FTA, however, the size of BDD structure exponentially increasing according to the number of variables, it has expensive memory consumption” (Deng et al., 2015).
- “It could happen that the construction of the BDD cannot be completed because of time or space constraints. This is due to the exponential increase of the number of nodes with the complexity of the fault tree” (Matuzas and Contini, 2015).
- “For large PSA models, usually it is not possible to derive the results in an acceptable time and memory cost. The truncation process is essential for these models” (Wei et al., 2016).
- “ZBDD is a good option to analyze large fault tree due to its highly compressibility of MCSs. However, there are still several practical cases in which fault trees are too complex and the corresponding ZBDDs are too large to be constructed” (Wang et al., 2016).

In the current state of the art only approximated non-conservative solutions are possible for very complex fault trees (with thousands gates and basic events) using truncation or other simplification techniques, and even with truncation, some important problems remain without an adequate solution:

- “There is the need to either estimate the truncation error - but there is no method able to accurately estimate it for large fault trees - or to demonstrate that the truncation threshold adopted reduces the truncation error to a negligible value” (Matuzas and Contini, 2015).
- “Since the application of truncation inevitably leads to under-estimate the top-event probability, there is the need to … estimate the truncation error or, alternatively, determine upper and lower bounds of the top-event unavailability … depending on the available working memory, the truncation method alone is not sufficient to analyze large fault trees when the SS[2] condition cannot be achieved. Hence, new methods are needed” (Contini and Matuzas, 2011).
- “Since the truncation process eliminates possible failures modes, the approximation is non-conservative … care must be taken to ensure that an appropriate truncation value is used” (Ibáñez-Llano et al., 2010).

It is then well established that both methods, the MCS and the BDD approach, cannot perform the complete evaluation of high complexity fault trees. The BDD method is highly memory consuming and the computers available working memory results insufficient to store the large BDDs derived from such fault trees. In these cases only approximated non-conservative solutions are possible using truncation.

In this context, the present paper provides a new approach for the complete evaluation of complex fault trees. The superiority of the proposed method lies in its extraordinary capacity to solve very complex fault trees completely. It is not limited by memory resources because in this approach there is no combinatorial expansion process and no additional structure as a BDD is required. There is no possibility of a combinatorial explosion leading to a memory blow-up. No matter how big a fault tree could be the advanced combinatorial method will never collapse.

2. Material and methods

A MCS is a set of basic events determining the fault condition of the top gate when all their members are faulty or unavailable. The adjective “minimal” means that they are all essential. If just one of the members is recovered, the top gate recuperates the success state. This condition is very easy to verify in the original fault tree. Hence, the MCSs of a fault tree can be generated, evaluated and discarded through a combinatorial algorithm testing all the possible combinations of basic events. However, it is evident that, for a large fault tree, this process could be endless if no restriction were applied to the number of combinations. That was precisely the problem here solved. The proposed fault tree advanced Combinatorial Solver (CSolv+) reduces substantially the number of combinations and, consequently, the fault tree can be solved in a reasonable time.

2.1. The basic combinatorial method

The fundamentals of the method will be explained through a simple case, the example fault tree shown in Fig. 1.

---

[2] Steady State value