Annals of Nuclear Energy 83 (2015) 316–321

Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

Development of reliability and probabilistic safety assessment program RiskA

Yican Wu *, FDS Team

Key Laboratory of Neutronics and Radiation Safety, Institute of Nuclear Energy Safety Technology, Chinese Academy of Sciences, Hefei, Anhui 230031, China

ARTICLE INFO

Article history:
Received 24 October 2014
Received in revised form 16 March 2015
Accepted 19 March 2015
Available online 10 April 2015

Keywords:
Probabilistic safety assessment
Zero-suppressed binary decision diagram
Fault tree
Event tree
RiskA

ABSTRACT

PSA (probabilistic safety assessment) software, the indispensable tool in nuclear safety assessment, has been widely used. An integrated reliability and PSA program named RiskA has been developed by FDS Team. RiskA supplies several standard PSA modules including fault tree analysis, event tree analysis, uncertainty analysis, failure mode and effect analysis and reliability database, etc. RiskA has several advanced features such as extensible framework, fast fault tree analysis, multiple models formats support and web-based co-modeling. Not only the overview of the architecture and basic functions of RiskA, but also the challenges and solutions in the development procedure of RiskA were introduced. The comparison between RiskA and other popular PSA codes has demonstrated that the calculation and analysis of RiskA is more accurate and efficient. Based on the development of this code package, many applications of safety and reliability analysis of some research reactors and nuclear power plants were performed.

1. Introduction

Nuclear safety is significant in nuclear industry. In history, there were three severe nuclear accidents which are Three Mile Island, Chernobyl and Fukushima accidents, attracting much attention from scientists, engineers and the public. An efficient safety analysis method could help to improve the safety of a Nuclear Power Plant (NPP). Probabilistic safety assessment (PSA) (Keller and Modarres, 2005) is one of the most useful methods for nuclear safety analysis. PSA software, the indispensable tool in PSA, has been widely used for the safety analysis of nuclear power plants and other complex systems of aerospace, ship industry, defense, etc. Up to now, there have been several quite popular PSA software, such as CAFTA and RiskSpectrum which are widely used in nuclear power plants, and Fault Tree+ and PTC Windchill FTA which are widely used in reliability field.

Several difficulties must be overcome for the further development of PSA software. Real-time calculation is needed in the on-line risk monitor, and co-modeling and automatic modeling are necessary when the PSA model is too large to be constructed by one person. In some cases, the functions of processing more complex dynamic models and multi-state models should also be supplied.

To provide an independent PSA software for China and to deal with some of the difficulties mentioned above, in collaboration with several universities and institutes, FDS Team studied various key algorithms and practical issues for the development of PSA software, and has developed an integrated reliability and probabilistic safety assessment program named RiskA (Wu et al., 2007). RiskA could be applied to probabilistic safety and reliability analysis of large complex systems such as nuclear reactors including human reliability analysis, web-based data management including reliability data and other related data, fault diagnosis, and risk monitoring, etc. The basic PSA methods such as failure mode and effects analysis, fault tree analysis, event tree analysis, uncertainty analysis, sensitivity analysis, importance analysis were all supported in this program.

The latest version of RiskA can assess the safety much more quickly and possess of more various functions for the purpose of fulfilling different users' requirements, and it was also developed with a view to conducing great convenience to the construction and transformation of complex fault tree and event tree models, the exhibition of the analysis results and the friendliness of human–computer interface. Furthermore, more appropriate program architecture was designed and applied after many years' efforts, which guarantees further function expansion and performance improving.

In this paper, not only the overview of the architecture and basic functions of RiskA, but also the challenges and solutions in the development procedure of RiskA were introduced. The

* Corresponding author.
E-mail address: yican.wu@fds.org.cn

http://dx.doi.org/10.1016/j.anucene.2015.03.020
0306-4549/

comparison between RiskA and other popular PSA codes has demonstrated that the calculation and analysis of RiskA is more accurate and efficient. Based on the development of this code package, many applications to safety and reliability analysis of some research reactors and nuclear power plants were performed.

The function structure of RiskA including software architecture design and analysis functions is introduced in Section 2. The advanced features applied in RiskA such as fast fault tree analysis algorithm and collaborative modeling are explained in Section 3. The successful applications of RiskA to reactors are provided in Section 4. Results and conclusions of this paper are drawn in Section 5 and Section 6.

2. Overall architecture and modules

RiskA supplies most of the general functions of reliability analysis and probabilistic safety assessment, and many other assistant functions are also supplied. Fig. 1 shows the modules structure of RiskA. There are four parts in this structure: (1) the first part is user input, which lets users input the PSA model and some necessary data by GUI or model transformation tool; (2) the second part is calculation engine, in which the general calculation functions like fault tree analysis, event tree analysis, uncertainty analysis, sensitivity analysis, importance analysis and failure mode and effects analysis are supplied; (3) the third part is user output, which outputs the analysis results, user customized reports and some other data; (4) the last part includes some necessary tools like reliability database, some other common tools and help documents which support the main functions of this software.

2.1. Fault tree analysis

Fault tree analysis module provides popular and advanced analysis for large scale fault tree since that it has adopted some enhanced MCS/ZBDD algorithms (Liu et al., 2007; Liu and Wu, 2003) and well-designed data structure to make full use of computation resources and improve computation speed and accuracy. This module is widely used for complex system safety and reliability analysis, including determining Minimal Cut Sets (MCSs), the probability of top event, the importance and sensitivity of components.

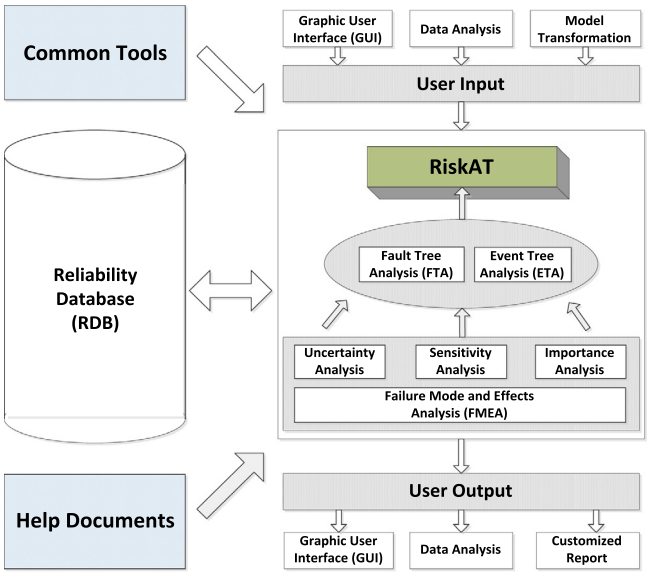

Fig. 1. Function structure of RiskA.

Basic event unavailability equations are developed using the parameter names from the Reliability Database module (see Section 2.5). Switching Events Set (SES) (Chen et al., 2014a) and Common Cause Failures (CCF) are two useful features for this module. SES feature allows users to add or modify a SES to any fault tree or sub-tree which can be very useful for users to model fault trees flexibly. CCF feature allows users to quickly add or modify common cause groups to the fault tree, and also compute the common cause basic event unavailability equations automatically.

All commonly used importance measures (e.g., Fussel–Vesely, RAW, RRW, etc.) are presented and could be computed for different levels of the model, such as basic events, components, systems and initiating events. Importance contributions from initiator fault trees are calculated directly as part of the basic event and component importance measures. Sensitivity analysis of basic events and components are also provided in this module.

In addition, a FTA-based risk monitor (Wang et al., 2009) can manage the risk of a complex system like nuclear power plant. As a plant specific real-time analysis tool, it can be used in instantaneous risk calculation, components' importance and sensitivity analysis, maintenance schedules evaluation and log management to make helpful suggestion about risk-informed decision making.

2.2. Event tree analysis

Event tree analysis module (Wang et al., 2008; Yuan et al., 2008) offers powerful event tree analysis. It's as important as FTA tool, and they constitute the main functions of PSA. This module enables the analysts to construct and link large event trees for each initial event considered. The event tree structure is developed graphically, the same as fault tree analysis module. The event tree initial events and function events used are consistent with those corresponding fault trees defined in the fault tree analysis module, so the frequency and unavailability of such events can be obtained from fault tree analysis module.

An event tree transfer page structure feature enables the development of unlimited numbers of sequences for analysis. During individual sequence's frequency quantification analysis, the linked event trees are walked, multiplying the initial event frequency and the success and failure branch split fractions to obtain the overall frequency of sequences.

A total of five kinds of success branch analysis are supported in RiskA: ignoring the function events of successful branch, only qualitative analyzing the function events of successful branch, independent assumed analyzing of all the function events system of successful branch, expanding all the function events system of successful branch using De Morgan technique and fast approximate analyzing using the Delete Term Procedure technique. Therefore, ETA module can fulfill the different demands of analysts from reliability, PSA and other scientific research or application fields.

The sequence representations in RiskA consider not only failure, null and success but also user-defined states of all preceding events making them uniquely suitable for modeling dependencies between human failures events. The ability to quantify hundreds of end states in a quantification process also makes RiskA well-suited for level 2 and level 3 analysis.

2.3. Uncertainty analysis

Uncertainty analysis (UA) module provides a series of advanced techniques that will ensure simulation process accurate and efficient. Uncertainty analysis is an individual module such that it can be used by other modules such as fault tree analysis module, event tree analysis module and reliability database module.

Uncertainty analysis involves investigating the uncertainty in the final output regardless of its data source while sensitivity