Dynamic Fault Tree Analysis for NPP Emergency Diesel Generator System

Daochuan Ge, Shanqi Chen, Zhen Wang, Zhibin Chen

Key Laboratory of Neutronics and Radiation Safety, Institute of Nuclear Energy Safety Technology, Chinese Academy of Sciences, Hefei, Anhui, 230031, China
**zhen.wang@fds.org.cn*

INTRODUCTION

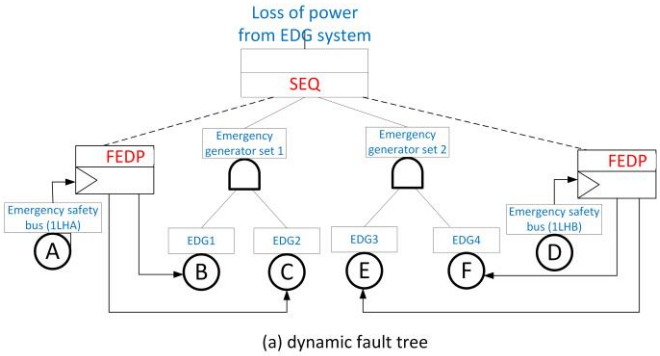
In recent years, the resilience thoughts based system safety management concept has been advocated by more people [1]. One foundation of its realization depends on dynamic safety assessment methods which can closely reflect the real failure behaviors of complex systems. Based on the R&D experience on advanced nuclear energy systems [2-4], now FDS team is developing this dynamic approach. To overcome the shortcomings of static modeling tools, dynamic safety assessment approaches were presented by many researchers, which can characterize dynamic failure behaviors of industrial systems, such like time-dependent, sequence-dependent, redundancy management, sequence enforcing, and functional dependent failure behaviors, and therefore can offer more accurate results. At present, the typical dynamic safety assessment approaches include: dynamic fault tree (DFT), dynamic flow graph and dynamic Bayesian Net. Among them, DFT presented by Professor J.B. Dugan [5] is extensively applied due to its simplicity and powerful dynamic modeling capacity. DFTs are now successfully applied in dynamic failure systems reliability evaluation, design and risk management.

Nuclear power plants as complex socio-technical systems; their safety attracts more people's attention [6]. It is found that station blackout (SBO) accident is the third most severe initiating event, and it poses great threat to the safety of the whole NPP. Hence, the emergency diesel generator system is the last security of the power supply and contributes much to the safety of the NPP. In a NPP, it is necessary that the safety systems can operate successfully with power for 24 hours after loss of offsite power (LOOP) accident so that the NPP can enter into a safe state. The time-dependent reliability of DGS in 24 hours after LOOP is very important. Hence, it is quite significant to make an effective reliability analysis of the DGS, and this issue has attracted many researchers' attention. Abdul-Nour et al., studied the probabilistic safety assessment (PSA) and reliability based maintenance policies for emergence diesel generator (EDG) in NPPs [7]. Lim et al., have performed a quantitative analysis of the risk impact considering starting time extension of the EDG [8]. Zubair et al., study the reliability date update methods for EDG [9]. Kancˇev et al., try to identify events that involve failures of EDG from specific operating experience and implement statistical analysis of events related to emergency diesel generators failures in NPP. However, these researchers just take static modeling techniques to analyze the reliability of DGS (i.e., fault tree, event tree, reliability block diagram and so forth models) and neglect the dynamic failure behaviors of DGS. Actually, DGS failure mechanisms are time-dependent and sequence- dependent.

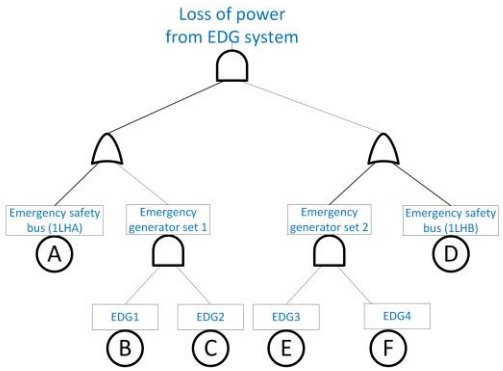
In order to show the truth between static and dynamic safety assessment methods, the case of diesel generator system (DGS) is studied in this article. A dynamic fault tree model based analyzing technique is adopted to evaluate the reliability of DGS at one Chinese NPP. The purposes of this paper are trying to accurately evaluate the reliability of NPP DGS after LOOP considering dynamic sequence-dependent failure behaviors. Comparisons between static fault trees (SFTs) and DFTs are also made, in order to find whether or not it is necessary to use DFTs to analyze NPP systems in the future.

SYSTEM DESCRIPTION AND MODELLING

The emergency diesel generator system consists of four diesel generators (B, C, E, F). The four regular diesel generators are configured as two trains, and each train is composed of two independent diesel generators. Under accident conditions, the first train is activated, and the second train still keeps at an unpowered standby state. If the first train fails, then the second train would immediately replace the first train. Only both trains fail, then the whole DGS loses. In addition, each train is dependent on its corresponding emergency safety bus (A or D). Due to the time constraint (i.e., early preparation work), the system is considered non-repairable in the first 3 hours, and after then, the system can be viewed as repairable for an access of workers' intervention. Therefore, the safety of the DGS in the first 3 hours should be guaranteed. In this article, the reliability of the system in the first 3 hours is evaluated. The static and dynamic fault tree models of the system's failure are built as shown in Fig. 1.



(a) dynamic fault tree



(b) static fault tree

Fig. 1. Dynamic and static fault tree of EDG system

RELIABILITY PARAMETERS AND METHODS

The reliability parameters (i.e., failure rates) of the DGS components are listed in Table 1.

TABLE 1 Reliability parameters of DGS components

Components	Failure Rate
A	4.73×10^{-7}/ h
B	1.99×10^{-2}/ h
C	1.99×10^{-2}/ h
D	4.73×10^{-7}/ h
E	1.99×10^{-2}/ h
F	1.99×10^{-2}/ h

The dynamic fault trees can be calculated through integrating the solution of each expanded cut sequence, and each cut sequence can be solved by multiple integration method. For more information about DFT, interested readers can refer to the references [10]. The results obtained from the dynamic and static fault trees are listed in Table 2.

TABLE 2 Reliability parameters of DGS components

Mission Time (h)	0.75	1.5	2.25	3
DFT	5.0×10^{-11}	9.7×10^{-10}	6.4×10^{-9}	2.5×10^{-8}
SFT	4.8×10^{-8}	7.5×10^{-7}	3.7×10^{-6}	1.1×10^{-5}

RESULTS

As observed in Table 2, the unreliability of the DGS is very low in the first 3 hours after LOOP. The unreliability results calculated by the SFT model are overestimated by about three orders of magnitude when compared with the DFT model. This overestimated unreliability sometimes needs to be reduced by additional redundancy designs or more regular inspection and maintenance. If it is done, it means that it may not only produce much expenditure but also do harm to the safety of the system. Hence, the sequence-dependent failure behaviors of the systems should be carefully considered and calculated by DFT methods.

As to nuclear power plants, some important systems (such as high-pressurized injection systems and digital control systems) often have temporal failure behaviors. Hence, it is necessary to apply dynamic approaches to evaluate their reliability in the future. In addition, as accurate temporal failure modeling tools, dynamic safety assessment approaches, such as DFT, can support the practical implementation of resilience engineering in complex systems.

ACKNOWLEDGMENTS

This work is supported by the National Magnetic Confinement Fusion Science Program of China [grant number 2015GB116000] and the National Natural Science Foundation [grant number 71671179] and we also thank other members of FDS team.

REFERENCES

1. A.W. Righi, et al., "A systematic literature review of resilience engineering: Research areas and a research agenda proposal," *Reliab. Eng. Syst. Safe.*, **141**, 142-152 (2015).
2. Y. Wu. "Development of High Intensity D-T Fusion Neutron Generator HINEG," *Int. J. Energ. Res.*, **42**, 68-72. (2018).
3. Y.Wu, et al., "A fusion-driven subcritical system concept based on viable technologies," *Nucl. Fusion*, **51**, 103036 (2011).
4. Y. Wu, FDS Team. "Design and R&D Progress of China lead-based Reactor for ADS Research Facility," *Engineering*, **2**,124-131 (2016).
5. J.B. Dugan et al., "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Trans. Rel.*, **41** (3), 363–373 (1992).
6. Y.C. Wu, at al., "Identification of safety gaps for fusion demonstration reactors," *Nat. Energy* **1**, 16154 (2016).
7. G. Abdul-Nour, et al., "Probabilistic safety assessment and reliability based maintenance policies: application to the emergency diesel generator of a nuclear power plant," *Comput. Ind. Eng.*, **42**, 433-438 (2002).
8. H. Lim, et al., "A quantitative analysis of a risk impact due to a starting time extension of the emergency diesel

generator in optimized power reactor-1000," *Reliab. Eng. Syst. Safe.,* **92**, 961-970 (2007).
9. M. Zubair, et al., "Reliability Data Update Method for emergency diesel generator of Daya Bay nuclear power plant," *Ann. Nucl. Energy.* **38**, 2575-2580 (2011).
10. D. Ge, et al., "Probabilistic model–based multi-integration formulas for quantifying a generalized minimal cut sequence," *P I Mech. Eng. O- J. Ris.* **229**(1), 73-82 (2015).