Nuclear Engineering and Technology 53 (2021) 103–110

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

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

Original Article

A rapid modeling method and accuracy criteria for common-cause failures in Risk Monitor PSA model

Bing Zhang [a], Shanqi Chen [b, *], Zhixian Lin [b, c], Shaoxuan Wang [b, c], Zhen Wang [b], Daochuan Ge [b], Dingqing Guo [d, a], Jian Lin [a], Fang Wang [b], Jin Wang [b, **]

[a] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen, 518172, China
[b] Key Laboratory of Neutronics and Radiation Safety, Institute of Nuclear Energy Safety Technology, Chinese Academy of Sciences, Hefei, 230031, Anhui, China
[c] University of Science and Technology of China, Hefei, Anhui, 230027, China
[d] School of Mechanical Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China

ARTICLE INFO

Article history:
Received 23 January 2020
Received in revised form
11 June 2020
Accepted 13 June 2020
Available online 15 June 2020

Keywords:
Nuclear power plant
Probabilistic safety assessment
Risk monitor
Common-cause failure
Criteria for modeling accuracy

ABSTRACT

In the development of a Risk Monitor probabilistic safety assessment (PSA) model from the basic PSA model of a nuclear power plant, the modeling of common-cause failure (CCF) is very important. At present, some approximate modeling methods are widely used, but there lacks criterion of modeling accuracy and error analysis. In this paper, aiming at ensuring the accuracy of risk assessment and minimizing the Risk Monitor PSA models size, we present three basic issues of CCF model resulted from the changes of a nuclear power plant configuration, put forward corresponding modeling methods, and derive accuracy criteria of CCF modeling based on minimum cut sets and risk indicators according to the requirements of risk monitoring. Finally, a nuclear power plant Risk Monitor PSA model is taken as an example to demonstrate the effectiveness of the proposed modeling method and accuracy criteria, and the application scope of the idea of this paper is also discussed.

1. Introduction

The Risk Monitor is one of the advanced applications of probabilistic safety assessment (PSA). It is a real-time risk analysis tool based on specific nuclear power plants (NPPs) information. A Risk Monitor can reflect the current status of each system and component of an NPP, and thereby determine the point-in-time risk (instantaneous risk) of the NPP, the risk importance index of systems and components, etc., to support the operational decision [1].With the development of PSA and computer technology, Risk Monitors and their applications in NPPs are increasing. Such as rapid risk computing core and Risk Monitors based on the fault tree [2,3], Risk Monitor and uncertainty analysis based on the GO-FLOW method [4], etc. In addition, the scope of NPPs risk monitoring is gradually expanding [5,6], and the accuracy of the frequency of initiating events [7], the importance index [8,9], and the common-cause failure (CCF) models [10] are also continuously improved. The Risk Monitor PSA model is based on the basic PSA model for analyzing the average risk of NPPs. The average or hypothetical conditions in the basic PSA model have to be reviewed based on the needs of instantaneous risk analysis, and the simplified parts of the model have to be eliminated to reduce the adverse impact on the risk analysis of an NPP under real-time configurations. Furthermore, enhanced modeling is performed to reflect various risks caused by different operational states and the environment around an NPP, so as to ensure that instantaneous risks can be calculated accurately for all configurations of the NPP.

Due to the interconnection of systems and components in an NPP, the failures of components also inevitably cause impacts on each other. At present, PSA applications usually use CCF models to model and analyze the interconnections which are not well known and thus cannot be modeled explicitly in a fault tree. According to the NUREG/CR-6268 of US NRC (Nuclear Regulatory Commission) [11], CCF means: a subset of dependent failures in which two or more component fault states exist at the same time, or within a short interval, because of a shared cause. CCF is one of the main contributing factors to the risks of NPPs. Moreover, the changes in

* Corresponding author. Key Laboratory of Neutronics and Radiation Safety, Institute of Nuclear Energy Safety Technology, Chinese Academy of Sciences, P.O. Box 1135, No. 350, Shushanhu Road, Hefei, Anhui, 230031, China.
** Corresponding author.
E-mail addresses: shanqi.chen@fds.org.cn (S. Chen), jin.wang@fds.org.cn (J. Wang).

https://doi.org/10.1016/j.net.2020.06.021

the configurations of systems and components during NPP operation will affect the CCF probabilities of redundant components, thus affecting the analysis results of the Risk Monitor. If some components of an NPP are out-of-service, the components that were originally not important in the system may even become very important. Therefore, timely and accurately modeling and assessment of CCF is an indispensable content of instantaneous risk monitoring for NPPs [1].

However, at present, the research on CCF modeling for risk monitoring is relatively rare. In 1998, H. Schoonakker et al., proposed the treatment of CCF in the Risk Monitor, and theoretically explained the unreasonable cut sets problem caused by the probability of out-of-service component being set to "1″ in Risk Monitor PSA model [12]. A survey on the existing technology of Risk Monitors was made by an expert group sponsored by IAEA (International Atomic Energy Agency) and OECD/NEA (the Organization for Economic Co-operation and Development/Nuclear Energy Agency), and the survey report introduced two situations, i. e. the component is out-of-service by plan and the component fails, in which the CCF model needs to be modified, and the report also explained the causes and modification methods based on the simplest Beta factor model [1]. In 2007, Xuhong He proposed a method for modification of CCF model in the out-of-service condition [13], which was the same as setting "1″ in the literature in 1998, so it will cause errors. Xuhong He also estimated the failure probabilities for a redundant system with a component failure based on the Beta factor and Multiple Greek Letter (MGL) models. In 2015, Hari Prasad theoretically analyzed the failure probability changes of the remaining in-service components while a component is out-of-service based on the basic parameter model [14], but the basic parameter model cannot be applied to the CCF in the Risk Monitor PSA model. In 2017, Min Zhang discussed the CCF probabilities evaluation after a component failure, and divided the component failures into independent failures and failures possibly caused by all reasons. Min Zhang also given a parameter estimation method of the common-cause failure group (CCFG) in Risk Monitor based on the Alpha model. Due to the limitation of the reliability data, he recommended the independent failure hypothesis approach which was optimistic and would result in a larger error [15].

In summary, it can be found that various CCF modeling methods proposed for the Risk Monitor PSA model have their own advantages, and at the same time, approximate modeling methods are commonly used. However, there is a lack of accuracy criterion and error analysis for approximate modeling, and impacts from other factors such as running/standby and system alignments are seldom considered. Based on the practice of instantaneous risk monitoring of NPPs, we analyze the impacts to CCF from the changes in an NPP configuration. Based on this, a comprehensive modeling method for CCFs in Risk Monitors, including accurate and approximate modeling, is proposed and shown by examples. Furthermore, the criteria for modeling accuracy of CCF is given to guide the CCF modeling. The motivation of this contribution is trying to reduce the Risk Monitor PSA model scale and calculation time while maintaining the accuracy of instantaneous risk assessment according to the regulation requirements.

2. Common cause failure in risk monitor and proposed solution

2.1. Common cause failures in risk monitor

The environment and configurations of NPPs may undergo various changes in the operation, such as the switching of running/standby equipment, components being out-of-service due to failure or periodic testing. These may lead to the changes of CCF probabilities of components. Therefore, risk monitoring requires a more detailed CCF model extension for all possible configurations of NPPs in order to be able to reflect the CCF probabilities of components in a variety of situations. After analyzing the changes in the operation of NPPs and their impact on CCF, we summarize the following three cases.

1) One of the redundant components of a system can operate normally, but if it is out-of-service due to periodic testing and preventive maintenance, the number of redundant components in the system will decrease, and the CCF probabilities of other redundant components in the system will change. In rare cases, an increase in redundant components will also cause a change in the CCF probabilities.
2) When a component is out-of-service due to a failure, it is usually necessary to test the remaining components. After the test is completed, the CCF modeling and analysis can be performed according to specific components status. However, the instantaneous risk of an NPP still generally needs to be evaluated before testing. At this time, the cause of component failure and the status of the remaining components have not yet been determined. Therefore, certain assumptions can be used to help estimate.
3) When there is a switch between running/standby trains, or the interconnection mode of the system redundant alignments is changed, it will cause changes in the operating/standby failure modes of components. In addition to changes in the alignments of the system components, this also cause the change of CCF probabilities for specific failure modes.

In summary, the CCF modeling and modification in the Risk Monitor PSA model, and the model changes in operating/standby system alignments, the NPP configurations, and undeveloped events all require the addition of new fault trees, basic events and house events to the basic PSA model. As a result, the Risk Monitor PSA model becomes larger than the basic ones. In order to give the risks of an NPP within 1–2 minutes [1], such as the minimum cut set, the core damage frequency (CDF), and the importance of components, it is necessary to control the scale of the Risk Monitor PSA model while ensuring enough accuracy.

2.2. Proposed CCF modeling method in risk monitor

Through analysis, we found that the construction and modification of the CCF model of the Risk Monitor involves three basic issues: the first is how to characterize the determined status of a component? The second is how to correctly model the CCF probabilities of components caused by the change in the number of redundant components. The third is what assumptions are used to estimate the system's CCF probability when some components failure and the status of the remaining components is not determined. All CCF related cases in the Risk Monitor can be solved by a combination of answers to these three issues.

For example, for the first case in chapter 2.1, it needs both characterization of the component state and remodeling of the CCF probabilities. By contrast, reference 13 introduced a method to deal with this case only by setting the basic event unavailability to TRUE (similar to "1" in reference 12, which means the basic event will definitely happen). It only characterized the out-of-service status of the component and did not deal with the change of the CCF probabilities, which would cause errors.

According to the scale of a general NPP Risk Monitor PSA model, there are hundreds of CCFGs, but many CCFGs have small impacts on the CDF. If they are all accurately modeled, it will cause not only a huge scale of Risk Monitor PSA model which results in slow

calculations, but also unnecessary waste of work efforts. In order to solve this problem, a rapid modeling method is proposed in this contribution based on the idea that a component can correspond to multiple basic events. For the three cases in Chapter 2.1, we propose accurate and approximate modeling methods accordingly. The accurate modeling methods here mean methods that can deal with all the above three basic issues, while approximate modeling methods mean ones that can only deal with the first and third ones.

1) There are two methods to characterize the status of out-of-service components. One is to set the basic event of out-of-service components to TRUE logic in the fault tree model and treat it as a house event, meaning that its impact on the risk of NPPs is equivalent to the components that have failed. The other one is to add an OR logic gate and a house event, and place the house event and the fault tree part corresponding to the out-of-service component side by side under the OR gate. When the component is out-of-service, the house event value is set to TRUE, and its effect is equivalent to the previous method. When the component is in-service, the value of the house event should be FALSE logic, and its impact on NPP risks is equivalent to normal operating components.

Note: Red color represents the value of fault tree nodes are TRUE. Fig. 1-A directly sets the basic event to TRUE, and Fig. 1-B shows the representation by a house event.

2) For changes in the number of redundant components, i. e., the modeling of the impact of out-of-service components on failure probability of remaining components, we also propose two methods. One is to change the basic events and CCF events into independent dynamic events, resulting in multiple different unavailability values in the Risk Monitor model database for an event. A landmark event for each dynamic event is also added to reflect the correlation between different configurations of the NPP and unavailability values. The unavailability of each dynamic event will be calculated according to the CCF model of the actual in-service components, as mentioned by Hari Prasad [14]. Note that it is necessary to delete the CCFG in the fault tree model in order to change the CCF event to an independent dynamic event, and all CCF events related to out-of-service components need to be set to FALSE.

To show how it works, a redundant system with four parts A, B, C and D is taken as an example below. All event combinations that will cause component A to fail can be expressed as:

$$A_T = E_A + E_{AB} + E_{AC} + E_{AD} + E_{ABC} + E_{ABD} + E_{ACD} + E_{ABCD} \quad (1)$$

Among them, A_T represents the total unavailability. E_A is the basic event in the fault tree model and represents the independent failure of component A. E_{AB} is a CCF event related to A, which represents the CCF of components A and B, and is limited to these 2 components. E_{AC}, E_{AD}, E_{ABC}, E_{ABD}, E_{ACD} and E_{ABCD} have similar definitions.

Assuming that component D is out-of-service due to periodic testing or preventive maintenance, the total unavailability of A will not change, but the involved events and the unavailability of these events will change. A_T will be expressed as following:

$$A_T = E_A + E_{AB} + E_{AC} + E_{ABC} \quad (2)$$

Therefore, in addition to setting E_D to TRUE to characterize the out-of-service of component D in the fault tree model, setting E_{AD}、E_{BD}、E_{CD}、E_{ABD}、E_{ACD}、E_{BCD}、E_{ABCD} to FALSE is also required, which means that these CCF events will not occur. The unavailability of E_A, E_{AB}, E_{AC}, and E_{ABC} in formula 2 needs to be calculated using a CCF model consisting of three components in-service, namely A, B, and C, instead of using the original CCF model.

Note: Red color represents the value of fault tree nodes are TRUE, while green color represents FALSE. Fig. 2-A is the fault tree model part where the component D is located, and Fig. 2-B is the fault tree model where the component A is located.

Another proposed method is based on multiple basic events corresponding to one component. Generally, *n*-1 basic events need to created based on the number of configuration states of this redundant system (assumed *n*), and requires *n* CCFG to model CCFs in these system configurations. These CCFGs will only contain basic events standing for components that are still in-service in a certain configuration. Multiple basic events and CCFGs are needed here because that PSA usually adopts the uniformity CCF assumption [16], i. e. failure probabilities of basic events in a CCF model are the same, and a basic event cannot be in two or more CCFGs at the same time in current PSA software. This method needs to create *n* OR logic gates, 2*n* AND logic gates and *n* house events in the PSA model. For each configuration, the house event and new CCFG of in-service components should be put under an AND logic gate. Finally, the new CCFGs and original one should be put under an OR logic gate. Thus, the switch of the states for system configuration can be characterized, which is similar to the method of characterizing the

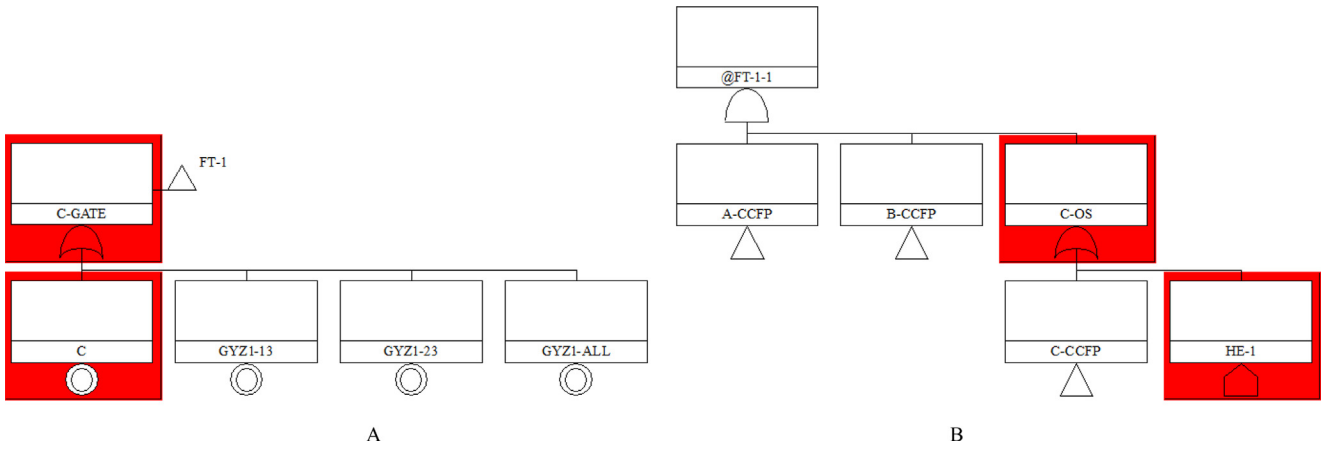

Fig. 1. Characterization of the out-of-service status of components.

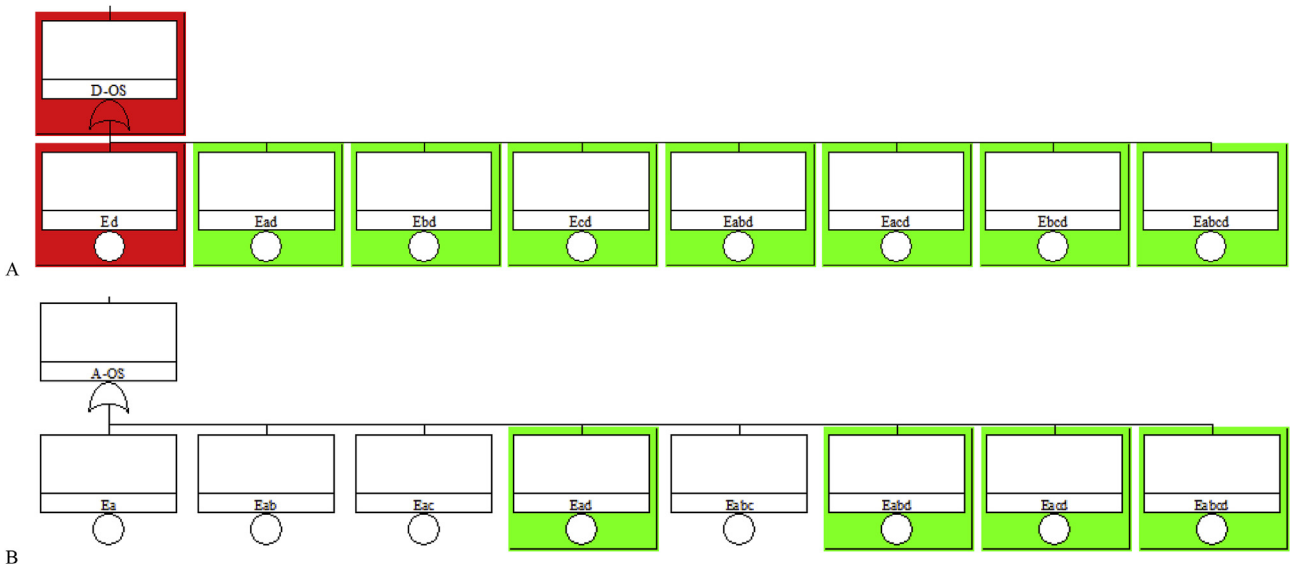

Fig. 2. CCF model of components after out-of-service based on dynamic events.

out-of-service status of a component.

The previous redundant system of four components A, B, C, and D is still used as an example. Before component D is out-of-service, the total unavailability event combination A_T of component A is also shown in formula 1.

Assume that the system has two configuration states, that is, all four components or three components will be in-service. In the model, three basic events AD1, AD2 and AD3 need to be newly created, and another CCFG (including the newly created three basic events) is established. After component D is out-of-service, the total unavailability event combination A_T of component A is shown by the following formula:

$$A_T = E_{AD1} + E_{AD12} + E_{AD13} + E_{AD123} \quad (3)$$

In the above formula, E_{AD1} is the basic event in the fault tree model and represents the independent failure of component A. E_{AD12} is a CCF event related to A, only representing the CCF of basic events A and B. E_{AD13} and E_{AD123} represent similar meanings. The unavailability of these CCF events is calculated using a CCF model consisting of three components AD1, AD2, and AD3.

Note: Fig. 3-A is the model state of component A while component D is in-service, and Fig. 3-B is the model state while component D is out-of-service. Red color represents the value of fault tree nodes are TRUE, while green color represents FALSE.

3) When a component fails and the status of the remaining components is not determined, the IAEA-OECD report [1] gives three assumptions for the system failure probability to estimate the CCF. They are:
   a) the CCF probability of the system is unchanged when the component failures independently;
   b) if the component failure belongs to the most severe CCF, the entire redundant system fails;

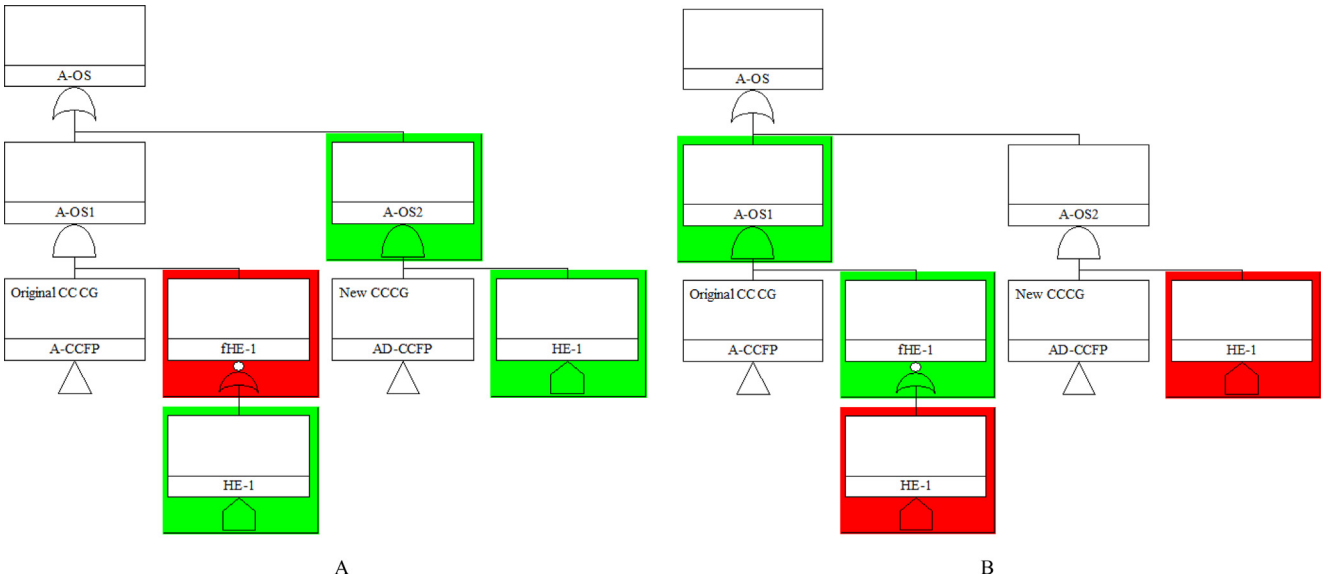

Fig. 3. CCF model considering normal operation or out-of-service of components based on multiple CCFG.

c) setting the unavailability of the redundant system as the CCF factor Beta of the Beta model to reflect the possibility of CCF of the system.

For the first assumption that the component fails independently, the CCF probability of the system does not change. At this time, the basic event of the failed component needs to be set to TRUE according to the IAEA-OECD report [1]. For the second assumption, the unavailability of the entire redundant system needs to be set to TRUE. However, these two assumptions are either too optimistic or conservative with big errors.

Similar to the last assumption of the IAEA-OECD report [1], theoretically accurate model formulas have been given in the literature of 2007 and 2017 [13,15]. However, for the construction of an NPP Risk Monitoring PSA model, their calculation formulas are too complicated, the artificial workload is relatively large, and data support may be lacking [15].

For the third assumption, this contribution proposes an approximate modeling method that is closer to the actual state of the NPP and easy for application in the modeling of Risk Monitor. Here, the unavailability of the redundant system needs to be set to an intermediate value between (0, 1), and this value is proposed to be selected separately according to the number of components in each redundant system and the failure criteria of the system. Taking the MGL model as an example, the CCF parameters are assumed to be β, γ, and δ. If the original redundant system contains 4 components, the failure criterion is three-out-of-four, that is, failure of 3 or more components will cause the system to fail. Then after component D fails, the system will fail when two or more components fail, so it becomes a two-out-of-three failure criterion. Therefore, according to the parameter definition of the MGL model, γ is the conditional probability that the common cause of a component failure that is shared by one or more components will be shared by two or more components in addition to the first [17]. Therefore, the unavailability of a redundant system composed of remaining components can be set to γ to represent the possibility of its CCF. By analogy, Table 1 gives some common examples of redundant systems in the NPP and the system unavailability under different failure criteria.

2.3. Proposed criteria for the accuracy of CCF model

In the above three basic issues in section 2.2, the methods for characterization of component status is simple and accurate. For the status of remaining components that is not determined in the third issue, a more accurate modeling method has been proposed, and the impact of CCF probability assumptions on the NPP risk calculations is temporary. Therefore, we focus on the accuracy criteria of modeling for the second issue, i.e. the impact to the unavailability of remaining in-service components resulted from the out-of-service component. It is not only the problem that has the greatest impact on the Risk Monitor PSA model and but also the case with the most workload in the modeling process.

According to the IAEA-OECD report [1], the main idea of the verification for an NPP Risk Monitor PSA model is to compare and verify its cut sets with the original basic PSA model in various typical configurations of the NPP, and this usually requires that the first 200–1000 cut sets are consistent with the results of the original PSA model in the calculation of CDF/LERF (Large early release frequency). Therefore, in order to ensure the consistency of these cut sets, the first CCF model approximation criterion proposed in this paper can be derived: In the calculating of CDF in a typical configuration of NPP, if events in a CCFG appear in the first 200–1000 cut sets, this CCFG must be modeled by accurate method, and cannot be modeled by an approximate method that will change the cut sets.

In fact, for general PSA models, there are only dozens of CCFGs involved in the first 1000 cut sets. Therefore, if the remaining CCF models are all approximate, the increase in the Risk Monitor PSA model can be reduced to about one tenth of that of totally accurate model method. However, the remaining CCF models cannot be all approximate. Because multiple CCF components with approximate model will cause error accumulation, which will result in that the accuracy of calculations for CDF, AOT (Allowed Outage Time), etc., cannot meet regulatory requirements, and affect the application of the Risk Monitor. Therefore, another criterion is needed to determine how many CCF models can be approximately modeled while ensuring their accumulated errors do not impact the calculation accuracy.

The impacts of approximate CCF modeling can be divided into two kinds: The first one is that the out-of-service component is not affected by CCF, or its CCF has been modeled accurately. Thus, the approximate CCF models in the PSA model will produce the same deviation for the calculation of $CDF_{point\text{-}in\text{-}time}$ and $CDF_{baseline}$, so the effects of their differences will be offset each other, and the calculation of CDF will not be affected in the end. Only the second one needs to be considered, that is, the out-of-service component is in the approximate CCF models, therefore the error of the CDF calculation is determined by the error of the approximate CCF models including out-of-service components at the same time.

According to the requirements of RG1.177 issued by the U. S. NRC for the increased risk due to out-of-service of components during the operation of an NPP [18], the incremental conditional core damage probability (ICCDP) of less than 10^{-6} is acceptable for a reactor with a baseline CDF of about 10^{-4}. The calculation formula of ICCDP is shown as bellow:

$$ICCDP = (CDF_{point\text{-}in\text{-}time} - CDF_{baseline}) \times T_{config} < 10^{-6} \quad (4)$$

For example, a redundant system has n CCF components in a same CCFG in the basic PSA model. When a component is out-of-service due to periodic tests, we assume that $CDF_{point\text{-}in\text{-}time\text{-}a}$ is used to represent the CDF calculated using the accurate CCF modeling method, and $CDF_{point\text{-}in\text{-}time\text{-}s}$ is used to represent the CDF calculated by the approximate modeling, then:

$$ICCDP_{accurate} = (CDF_{point\text{-}in\text{-}time\text{-}a} - CDF_{baseline}) \times T_{config} < 10^{-6} \quad (5)$$

Table 1
Unavailability of redundant systems after components out-of-service.

Number of components in the original CCFG	Unavailability of a redundant system after a component is out-of-service		
	2 events fail resulting in the failure of the original system	3 events fail resulting in the failure of the original system	4 or more events fail resulting in the failure of the original system
2	β	–	–
3	β	Bγ	–
4	β	Bγ	βγδ
n, $n > 4$	β	Bγ	βγδ

$$ICCDP_{similar} = (CDF_{point\text{-}in\text{-}time\text{-}s} - CDF_{baseline}) \times T_{config} < 10^{-6} \quad (6)$$

Therefore, the error caused by the approximate CCF modeling method will directly affect the calculation of ICCDP, and this error will continue until the next upgrade of the Risk Monitor PSA model, which is usually more than 1 year. The calculation of real time risk indicators, such as CDF and AOT for Risk Monitor, is usually based on the assumption that the state of NPPs lasts for one year. This will cause the impact of the approximate CCF model method on the risk calculation will be equivalent to the out-of-service effect of components that lasts for one year. On the basis of the above two equations, we can get the following equation.

$$\Delta ICCDP = (CDF_{point\text{-}in\text{-}time\text{-}s} - CDF_{point\text{-}in\text{-}time\text{-}a}) \times T_{config} \quad (7)$$

In which, T_{config} is 1 year/1 year. We found that ΔICCDP has the same structure as ICCDP, and ΔICCDP must be less than the regulatory limit of 10^{-6}. Otherwise, the ICCDP brought by the approximate CCF model error will exceed the regulatory limit, even there is no out-of-service for any component. In addition, it should be taken into account that the baseline CDF of pressurized water reactors (PWR) currently operating is generally 10^{-4}, while the CDF of a newly built nuclear power plant is generally 10^{-5}. In order to make the method in this paper applicable to NPPs with different baseline CDF, 10^{-6} is converted to 1% of the baseline CDF for current PWR. Therefore, we can obtain the second approximation rule for CCF models: In the Risk Monitor PSA model, the CDF change caused by cumulative errors from approximate CCF modeling must be less than 1% of the baseline CDF. As shown in the following formula:

$$| CDF_{point\text{-}in\text{-}time\text{-}s} - CDF_{point\text{-}in\text{-}time\text{-}a} | < CDF_{baseline} \times 1\% \quad (8)$$

It should be noted that the above formulas only give the minimum requirements to ensure the effectiveness of the Risk Monitor application. This specific limit can also be increased according to the requirements for ICCDP calculation accuracy, such as 0.1% of the baseline CDF. In addition, it should be noted that only the out-of-service components will result in error accumulation. The number of out-of-service components in an NPP during operation is usually relatively small, so generally it is not necessary to calculate many CCF models for error accumulation, which further provides space for the application of proposed method.

Finally, if the Risk Monitor PSA model is built on the basis of a level-2 basic PSA model, LERF is usually used in addition to the CDF to measure the risk of NPPs. In this regard, according to the RG1.177, the restriction requirements of ICLERP are given as follows:

$$ICLERP = (LERF_{point\text{-}in\text{-}time} - LERF_{baseline}) \times T_{config} < 10^{-7} \quad (9)$$

The limiting criteria and formula of ICLERP on CCF model can also be deduced according to the above idea. Namely, the maximum change in the LERF due to cumulative error must be less than 1% of the baseline LERF, which is shown as the following formula:

$$| LERF_{point\text{-}in\text{-}time\text{-}s} - LERF_{point\text{-}in\text{-}time\text{-}a} | < LERF_{baseline} \times 1\% \quad (10)$$

2.4. Application example in risk monitor by MGL model

The MGL model is token as an example to illustrate the application of the proposed CCF modeling methods and accuracy criteria in Risk Monitor. Assume a system containing three components A, B, and C, which fails only all three components fail, and a CCFG with a size of three for these components is established. If the total unavailability of a component is p, and the CCF model parameters of the MGL are β, γ, and δ. After the component C is out-of-service, the unavailability of component A modeled by the accurate method is $P_a(A)$, which is calculated as follows.

$$P_a(A) = P_a(E_A) + P_a(E_{AB}) = p(1\text{-}\beta) + p\beta \quad (11)$$

$P_a(E_A)$ represents the unavailability p(1-β) of the basic event E_A, which reflects the independent failure of component A. $P_a(E_{AB})$ represents the unavailability pβ of the basic event E_{AB} and reflects the CCF of parts A and B. The unavailability of component A modeled by the approximate method is $P_s(A)$, and the formula is as follows:

$$P_s(A) = P_s(E_A) + P_s(E_{AB}) + P_s(E_{AC}) + P_s(E_{ABC}) = p(1\text{-}\beta) + p(1\text{-}\gamma)\beta + p\beta\gamma \quad (12)$$

The total unavailability of the component itself does not change, that is $P_a(A) = P_s(A) = p$. The unavailability of the redundant system consisting of the remaining 2 components calculated by the accurate modeling method is:

$$P_a(Sys) = P_a(E_{AB}) + P_a(E_A)*P_a(E_B) = p\beta + p^2(1\text{-}\beta)^2 \quad (13)$$

The unavailability of the redundant system calculated by the approximate modeling method is:

$$P_s(Sys) = P_s(E_{AB}) + P_s(E_{ABC}) + P_s(E_A)*Ps(E_B) + P_s(E_{AC})*P_s(E_B) + P_s(E_{BC})*P_s(E_A) + P_s(E_{AC})*P_s(E_{BC}) \quad (14)$$

$$P_s(Sys) = (1/2)p(1\text{-}\gamma)\beta + p\beta\gamma + p^2(1\text{-}\beta)^2 + p^2(1\text{-}\beta)(1\text{-}\gamma)\beta + (1/4)p^2(1\text{-}\gamma)^2\beta^2 \quad (15)$$

According to the general NPP model and the reference data of NUREG/CR-5497 [19], p is generally less than 0.01, β is generally 0.01, and γ is generally 0.1.Therefore, after a component in a redundant system is out-of-service, the error between accurate modeling and approximate modeling is:

$$| P_a(Sys) - P_s(Sys) | \approx (1/2)p\beta \quad (16)$$

Similarly, we can derive the errors of a CCF system of two-out-of-three, four-out-of-four, three-out-of-four, etc. After a component is out-of-service, the errors between accurate and approximate model are shown in Table 2.

Therefore, the errors of CCF model can be calculated and the impacts on the CDF from the errors can be estimated by multiply the CCF errors by the frequency of the initiating events, and the basic events unavailability of the cut sets where these CCF events are located. A simpler and more conservative estimation can be made by only considering the impact of the initiating event.

3. Results and discussion

3.1. Case study and results

In order to verify the proposed method, we take a Chinese NPP PSA model as an example, and modify the CCF model using this method to complete the construction of the Risk Monitor PSA model. Then, its CDF and minimum cut sets are calculated and compared for several typical configurations of an NPP to illustrate the correctness and effectiveness of the method. The PSA model includes 48 event trees, 1599 fault trees, and 205 CCFGs. The CCFGs containing 3 or more basic events are all constructed by the MGL

Table 2
Errors between accurate and approximate model.

Number of basic events in the original CCFG	After a component is out-of-service, the errors between accurate and approximate model		
	2 events fail resulting in the failure of the original system	3 events fail resulting in the failure of the original system	4 events fail resulting in the failure of the original system
3	(1/2)pβ	(1/2)pβ	–
4	(1/2)pβ	(1/2)pβ-(5/6) pβγ	(2/3)pβγ
5	(1/2)pβ	(1/2)pβ-(5/6)pβγ	(2/3)pβγ

Table 3
Numbers of CCFGs in previous cut sets resulting in core damage.

NPP configuration	Number of CCFG in the first 200 cut sets	Number of CCFG in the first 500 cut sets	Number of CCFG in the first 1000 cut sets	CDF
Normal operation	6	14	23	1.460×10^{-7}
Normal cold shutdown	17	21	23	1.343×10^{-8}
Refueling cold shutdown	15	24	30	2.332×10^{-8}

CCF model. The modification and calculation are carried out according to the following steps.

1) First, the CDFs are calculated with the probability truncation of 10^{-13}, and the order truncation is unlimited. Then, 24 CCFGs that occur in the first 500 cut sets are selected to be accurately modeled, according to the proposed accuracy criteria. The CDF results and the numbers of CCFGs involved in the first 200, 500 and 1000 cut sets are shown in Table 3.
2) According to the possible configuration of the NPP during operation, components of 17 CCFGs that may be out-of-service at the same time were screened out. Among them, 6 CCFGs occur in the first 500 cut sets, and are modeled accurately. The errors of other 11 CCFGs are calculated and compared according to the accuracy criterion proposed in section 2.3, and no CCF is found to result in the accumulation error exceeding the limit. Thus, the remaining 11 CCFGs were all modeled according to the approximate method proposed.
3) Finally, under several typical configurations of NPPs, the CDFs are calculated for the PSA model before and after the CCF modification, and the first 500 minimum cut sets are compared. The results are shown in Table 4.

In Table 4, the CCF components in ESWS (Essential Service Water System) sub train occur earliest in the 630th cutting set, and they are modeled by the approximate method. According to Table 4, under these typical NPP configurations, the error of the CDF result is less than 0.3%, and the minimum cut sets are also consistent. This shows that the proposed method can complete the CCF modification in the basic PSA model of the NPP while ensuring the calculation accuracy. Moreover, in the building of CCF model of the Risk Monitor, the basic events and logic gates newly added to the fault tree in the Risk Monitor PSA model are only about 12% of the traditional method.

3.2. Discussion

Although only the MGL model is token as an example in this contribution, it can be found from the method derivation that the method is not limited to the specific form of the CCF model, it can be applied to various CCF models commonly used in PSA, such as the Alpha model. In addition, importance considerations can also be added into the accuracy criteria. For example, a component with a Risk Achievement Worth importance equal/higher than 0.1, or with a Fussell-Vesely importance equal/higher than 100 (generally used as the limit value for safety classification), can be selected for accurately modeling besides the first 500 cut sets. For the analysis case in section 3.1, there are 9 CCFGs with components importance measures exceeding the limit, which should be modeled accurately. These 9 CCFGs also occur in the first 500 cut sets, which demonstrate the consistency of these criteria.

The derivation of this contribution is based on the assumption that the parameters of the CCF model are unchanged. In fact, after the number of components of the CCFG changes, the parameters of the CCF model will change, and the parameters after the change should be adopted. Therefore, there will be some errors. However, as shown in the reference data of NUREG/CR-5497 [18], the variation of the parameters is very small for different numbers of CCF components in a CCFG, usually less than 10%, so it will not affect the formulas and the accuracy criteria proposed.

In the derivation of formula 3, three basic events and a CCFG were newly created, but it is not shown that which component is out-of-service. Because the uniformity assumption is commonly used for CCF in the current PSA model [16]. Thus, no matter which component is out-of-service, the unavailability of the remaining components is the same. In fact, the status characterization of the out-of-service component can be expressed by the original basic event of the component, that is, $E_{A,}$ $E_{B,}$ $E_{C,}$ and E_{D}. Therefore, in order to reduce the size of the model, the number of new basic events and CCFGs can be and also should be minimized.

When there is a switch between the running/standby trains in a redundant system, or the interconnection of a redundant system is changed, it will result in the change of system component operation/failure mode, it is necessary to characterize the status of system trains, and combine the change of CCF probabilities for components in a specific failure mode. It is worth noting that this will cause simultaneous changes in the start-up failure and running failure in CCFGs, and they are both need to be modeled accordingly.

Table 4
Comparison of CDF and cut sets before and after model modification.

NPP configuration	Consistency of the first 500 cut sets (yes/no)	CDF of Risk Monitor model	CDF of the basic PSA model
B2 of ESWS sub train is out-of-service in normal operation	yes	1.500×10^{-7}	1.499×10^{-7}
B2 of ESWS sub train is out-of-service in normal cold shutdown	Yes	1.345×10^{-8}	1.342×10^{-8}
B2 of ESWS sub train is out-of-service in refueling cold shutdown	Yes	2.361×10^{-8}	2.361×10^{-8}

In addition, there may be CCFGs of different types of components in a system train. Thus, it is often necessary to model these CCFGs at the fault tree part corresponding to each component separately, and it cannot be simply modeled at the logic gate where the system trains are located. This is different from the out-of-service status of a single component.

Finally, there are also a few other considerations should be explained here:1) In the operation of NPPs, components of a second-order redundant system are generally not allowed to be out-of-service under non-fault conditions. 2) It is possible that two or more components of a redundant system are out-of-service, such as the size of CCFG is reduce from 4 components to 2 components. In that situation, the size of a CCFG can be reduced twice by following the approximate modeling method proposed, but it is better to apply the precise modeling method. 3) The general PSA model considers the maximum number of redundant components in the system, so this contribution does not discuss the increase in the number of components in the CCFG, which is recommended to use accurate modeling. These circumstances will not affect the effectiveness of the proposed method and accuracy formulas.

4. Conclusion

In the development of Risk Monitor PSA model based on the basic PSA model of an NPP, the common-cause failures modeling of redundant systems and components is a very important content. In this contribution, we analyze the impacts of the NPP configuration on the CCF, and summarize three basic issues, namely, the characterization of the component states, the CCFG modeling with the change of the redundant components number, and the assumption of the CCF probabilities when the components states are not determined. Then, corresponding multiple accurate and approximate modeling methods are proposed respectively, and criteria for the accuracy of CCF modeling based on cut sets and risk indicators (such as core damage frequency) are derived according to the good practices described in the IAEA-OECD sponsored survey report and a regulatory guide of NRC for the NPP risk monitoring. The proposed methods are aiming to reduce the model scale of the Risk Monitor, and increase the speed of risk calculation while meeting the accuracy of risk assessment. The effectiveness of the methods is demonstrated by an analysis case of a typical NPP Risk Monitor PSA model, and the suitable scope of the method idea is also explained through discussion.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We thank other FDS Team members, and authors and contributors of references cited in this work. This work is supported by the National Natural Science Foundation of China (71671179, 51805511, 71901203, 51906249) and National Key R&D Program of China (2018YFB1900301, 2019YFE0191600).

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.net.2020.06.021.

References

[1] C.H. Shepherd, F.J. Yllera, B. Kaufer, D.W. Henneke, D. Gaynor, J. Sedlak, et al., Risk monitors - the state of the art in their development and use at nuclear power plants - produced on behalf of IAEA and OECD/NEA WGRisk, in: Nuclear Energy Agency of the OECD (NEA), 2004, p. 250.
[2] F. Wang, J.Q. Wang, J. Wang, Y.Z. Li, L.Q. Hu, Y.C. Wu, Risk monitor RiskAngel for risk-informed applications in nuclear power plants, Ann. Nucl. Energy 91 (2016) 142–147.
[3] J. Wang, F. Wang, S.Q. Chen, J.Q. Wang, L.Q. Hu, Y. Yin, et al., Fault-tree-based instantaneous risk computing core in nuclear power plant risk monitor, Ann. Nucl. Energy 95 (2016) 35–41.
[4] X. Dai, M. Yang, B. Zou, H. Lu, Hierarchical modeling of GO-FLOW models for online risk monitoring of nuclear power plants, in: 2017 25th International Conference on Nuclear Engineering, ICONE, American Society of Mechanical Engineers (ASME), Shanghai, China, 2017. July 2, 2017 - July 6, 2017.
[5] Z.G. Ma, H. Yoshikawa, T. Nakagawa, M. Yang, Knowledge-based software design for Defense-in-Depth risk monitor system and application for AP1000, J. Nucl. Sci. Technol. 54 (5) (2017) 552–568.
[6] H. Yoshikawa, T. Nakagawa, Development of plant DiD Risk Monitor system for NPPs by utilizing UML modelling technology, Ifac Papersonline 49 (19) (2016) 397–402.
[7] Y.J.B. Lee, T.J. Lin, S.F.M. Liang, Accuracy enhancement in estimation of the initiating event frequencies in risk monitor application on Kuosheng NPP, Ann. Nucl. Energy 76 (2015) 40–47.
[8] J.K. Vaurio, Importance measures in risk-informed decision making: ranking, optimisation and configuration control, Reliab. Eng. Syst. Saf. 96 (11) (2011) 1426–1436.
[9] J.Q. Wang, F. Wang, J. Wang, S.Q. Chen, L.Q. Hu, Y.Z. Li, et al., A new importance assessment method for risk-informed SSC categorization, Int. J. Energy Res. 42 (4) (2018) 1779–1786.
[10] A. O'Connor, A. Mosleh, A general cause based methodology for analysis of common cause and dependent failures in system risk and reliability assessments, Reliab. Eng. Syst. Saf. 145 (2016) 341–350.
[11] T.E. Wierman, D.M. Rasmuson, A. Mosleh, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding. NUREG/CR-6268, U.S. Nuclear Regulatory Commission, 2007.
[12] H. Schoonakker, M. van der Borst, in: A. Mosleh, R.A. Bari (Eds.), Treatment of Common Cause Failures in Risk Monitoring, Springer-Verlag London Ltd, Godalming, 1998, pp. 437–442.
[13] X. He, J. Tong, J. Chen, Maintenance risk management in Daya Bay nuclear power plant: PSA model, tools and applications, Prog. Nucl. Energy 49 (1) (2007) 103–112.
[14] M. Hari Prasad, G. Vinod, V.V.S. Sanyasi Rao, Risk management of NPPs using risk monitors, International Journal of System Assurance Engineering and Management 6 (2) (2015) 191–197.
[15] M. Zhang, Z. Zhang, A. Mosleh, S. Chen, Common cause failure model updating for risk monitoring in nuclear power plants based on alpha factor model, Proc. Inst. Mech. Eng. O J. Risk Reliab. 231 (3) (2017) 209–220.
[16] S. Chen, J. Wang, F. Wang, J. Wang, L. Hu, Asymmetrical common-cause failures analysis method applied in fusion reactors, J. Fusion Energy 35 (2) (2016) 221–228.
[17] A. Mosleh, D.M. Rasmuson, F.M. Marshall, Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment. NUREG/CR-5485, U.S. Nuclear Regulatory Commission, 1998.
[18] Office of Nuclear Regulatory Research, An Approach for Plant-specific, Risk-Informed Decisionmaking: Technical Specifications, Regulatory Guide 1.177, U.S. Nuclear Regulatory Commission, 2011.
[19] F.M. Marshall, D.M. Rasmuson, A. Mosleh, Common-cause Failure Parameter Estimations. NUREG/CR-5497, U.S. Nuclear Regulatory Commission, 1998.