考虑启动时间和启动失效的核电厂冷冗余系统可靠性数值模拟方法

王韶轩[1,2] 林志贤[1,2] 戈道川[1] 吴 洁[1] 郁 杰[1]
1（中国科学院合肥物质科学研究院 核能安全技术研究所 合肥 230031）
2（中国科学技术大学 合肥 230026）

摘要 开展考虑设备启动时间和启动失效的核电厂冷冗余系统故障机理研究，提出一种基于蒙特卡罗数值模拟的可靠性分析方法，建立冷冗余系统失效概率的统计量表达式。以核电厂应急柴油发电机组为例，开展案例分析，获得应急柴油发电机组的失效概率分布曲线及各设备参数的敏感度曲线，并将结果与静态故障树（Static Fault Tree，SFT）、传统动态故障树（Dynamic Fault Tree，DFT）方法进行对比。案例结果分析表明：1）所提方法可以对冷冗余设备的启动时间与启动失效进行建模分析，反映冷冗余系统的真实失效场景与实际运行状态；2）所提方法精确评价系统失效概率、识别不同时间段的高敏感性设备参数、以及分析启动时间对系统失效概率的影响，对冗余系统的优化设计有一定的理论指导意义。

关键词 启动失效，动态故障树，核电厂，冷冗余，可靠性
中图分类号 TL99
DOI: 10.11889/j.0253-3219.2022.hjs.45.120604

Reliability numerical simulation for startup time and startup failure of cold redundancy system in nuclear power plant

WANG Shaoxuan[1,2] LIN Zhixian[1,2] GE Daochuan[1] WU Jie[1] YU Jie[1]
1(*Institute of Nuclear Energy Safety Technology*, *Hefei Institutes of Physical Science*, *Chinese Academy of Sciences*, *Hefei 230031*, *China*)
2(*University of Science and Technology of China*, *Hefei 230026*, *China*)

Abstract **[Background]** The startup time and startup-failure are widespread in most cold redundancy equipment of nuclear power plants (NPPs). The traditional static and dynamic fault tree cannot accurately model the startup time and startup-failure. **[Purpose]** This study aims to model the startup time and startup-failure behaviors in cold redundancy systems, and provide suggestions for the improvement of reliability assessment methods. **[Methods]** First, a DFT Monte Carlo simulation method was proposed for modeling and analyzing equipment's startup time and startup-failure behaviors in a cold redundancy system. Then, the emergency diesel generator set of the nuclear power plant was taken as an example, the distribution curve of system failure probability and the sensitivity of each component were obtained. Finally, the results were compared with the static fault tree method and traditional DFT method. **[Results]** 1) The proposed method can model and analyze the start-up time and start-up failure behaviors of cold redundant equipment, reflecting the real failure scenarios and actual operation status of cold redundant systems.

国家自然科学基金(No.71901203)资助
第一作者：王韶轩，男，1997年出生，2019年毕业于华中科技大学，现为博士研究生，主要从事核能系统可靠性和概率风险评价研究工作
通信作者：戈道川，E-mail：daochuan.ge@inest.cas.cn
收稿日期：2022-06-14，修回日期：2022-09-13
Support by National Natural Science Foundation of China (No.71901203)
First author: WANG Shaoxuan, male, born in 1997, graduated from Huazhong University of Science and Technology in 2019, doctoral student, focusing on the research of probabilistic safety assessment of nuclear power plants
Corresponding author: GE Daochuan, E-mail: daochuan.ge@inest.cas.cn
Received date: 2022-06-14, revised date: 2022-09-13

2) The proposed method can accurately evaluate the system failure probability, identify highly sensitive equipment parameters in different time periods, and analyze the influence of start-up time on the system failure probability. **[Conclusions]** The proposed method has certain theoretical significance for the optimal design of NPP's cold redundancy systems.

Key words Startup failure, Dynamic fault tree, Nuclear power plant, Cold redundancy, Reliability

安全是核电产业健康发展的前提，为保障安全，核电厂大量采用冗余设计。对于一些关键设备如泵、发电机等往往采用冗余配置以满足单一故障准则[1]。这些冗余设备平时处于冷备状态（即零功率状态），只有当主件失效后才会启动，在启动过程中需要一定的启动时间且存在启动失败可能。设备的启动时间是指设备从启动到正常工作或从初始状态完全转换到另一状态所需要的时间。设备启动时间的形成原因有很多：设备的正常运行需要满足一定的条件、设备的初始状态有所限制、人的操作行为需要时间等。在启动过程中设备可能会由于自身部件老化、工作环境变化、操作行为出现失误等原因而启动失败，在核电厂中某些特定的紧急情况下，部分关键设备的启动失败被视为失效，不考虑其二次启动。文献[2]分析了核电厂中应急柴油发电机启动失效和超时的原因；文献[3]探究了核电厂水压试验泵启动失效的问题。核电厂中存在大量对反应堆安全有重要影响的冷冗余设备，针对其启动时间与启动失效进行相应的可靠性建模分析对提高核电厂整体安全性有重要意义。

在静态故障树（Static Fault Tree，SFT）分析方法中，通常不考虑设备启动时间，一般将启动失效视为基本事件以做简化处理。传统SFT模型无法有效地对核电厂冷冗余系统中蕴含的动态失效行为进行建模，国际上普遍采用动态故障树（Dynamic Fault Tree，DFT）分析方法对含有时序失效行为的系统进行可靠性评估[4−5]。目前在DFT分析方法中，对于冷冗余设备启动时间与启动失效的处理依旧与SFT类似。针对上述问题，本文将采用蒙特卡罗数值模拟方法分析启动时间与启动失效对冷冗余系统可靠性的影响，并以核电厂应急柴油发电机组为例开展工程应用研究。

1　理论基础

1.1　动态故障树模型

DFT作为SFT的延伸，引入优先与（Priority And，PAND）门、功能相关（Functional-Dependence，FDEP）门、顺序强制（Sequence-Enforcing，SEQ）门、冷备（Cold Spare，CSP）门、温备（Warm Spare，WSP）门和热备（Hot Spare，HSP）门来描述系统中的时序失效行为[6]。图1展示了本文案例分析中涉及的三种动态门（CSP门、SEQ门和FDEP门），下面将对这三类动态门进行详细阐述。

CSP门如图1（a）所示，其包含一个主输入事件A_1，两个备用输入事件A_2和A_3。A_1开始处于工作状态，A_2在A_1发生失效后立即激活并转入工作状态，随后A_2失效，A_3被激活并转入工作状态，当A_3失效时门事件发生。用割序可表示为：$A_1 \rightarrow {}^{0}_{A_1}A_2 \rightarrow {}^{0}_{A_2}A_3$，其中${}^{0}_{Y}X$表示部件$X$作为$Y$的备件，且在备用状态下的失效率为0。

SEQ门如图1（b）所示，其包含3个输入事件A_1、A_2和A_3，强制其门下的输入事件以从左到右的顺序发生，其割序可逻辑等价地表示为：$A_1 \rightarrow {}^{0}_{A_1}A_2 \rightarrow {}^{0}_{A_2}A_3$。SEQ门与CSP门的失效模式非常相似，唯一的区别在于SEQ门的输入事件可以是基本事件也可以是门事件。

FDEP门如图1（c）所示，其包含一个触发事件A_T，两个相关基本事件A_1和A_2。当A_T发生失效时，A_1、A_2也随之发生失效，反之A_1、A_2是否失效，对A_T的状态没有影响。

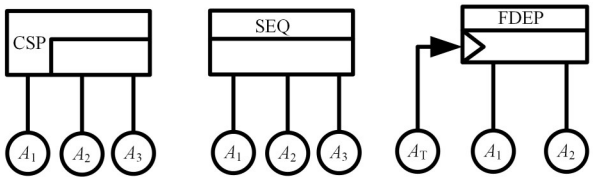

图1　动态逻辑门
(a) 冷备门，(b) 顺序强制门，(c) 功能相关门
Fig.1　Dynamic logic gates　(a) Cold spare gate, (b) Sequence-enforcing gate, (c) Functional-dependence gate

1.2　蒙特卡罗数值模拟

蒙特卡罗数值模拟方法的基本思想就是将解析模型转化为概率模型，通过重复构造符合一定规则的计算机随机数来求解问题[7−8]。最小割序是指导致DFT顶事件发生的一组最少先后发生的基本事件，其状态决定系统状态。最小割序集是指所有导致DFT顶事件发生的最小割序的集合。因此，利用最小割序集可以对DFT顶事件的发生概率进行数值模拟。本文采用“最小割序集+顺序失效域”的数值模拟方法分析DFT[9]。顺序失效域则是指由图形

化描述的顺序失效逻辑图所确定的带有一定顺序性的失效域[10]。以割序 $A_1 \to {}_{A_1}{}^{0}A_2 \to \cdots \to {}_{A_{n-1}}{}^{0}A_n$ 为例，其顺序失效逻辑图如图2所示。

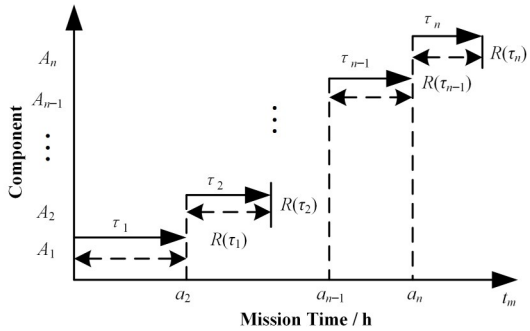

图2 $A_1 \to {}_{A_1}{}^{0}A_2 \to \cdots \to {}_{A_{n-1}}{}^{0}A_n$ 的顺序失效逻辑图

Fig.2 Sequence failure logic diagram for case: $A_1 \to {}_{A_1}{}^{0}A_2 \to \cdots \to {}_{A_{n-1}}{}^{0}A_n$

图2中，t_m 为任务时间；a_i 表示事件 A_i 的起始点；τ_i 表示失效时间（即设备寿命）；$R(\tau_i)$ 表示 τ_i 的有效失效时间段，即导致割序发生的有效时间段。对于任意一个 $R(\tau_i)$，当 i=1 时，$R(\tau_1)=\{\tau_1 | 0<\tau_1<t_m\}$；当 $2\leqslant i\leqslant n$ 时，$R(\tau_i)=\{\tau_i | 0<\tau_i<t_m-\tau_1-\cdots-\tau_{i-1}\}$。该割序的失效域 Ω 可表达为：

$$\Omega=\bigcap_{i=1}^{n}R(\tau_i) \tag{1}$$

DFT蒙特卡罗数值模拟方法的主要流程为：首先根据基本事件发生的概率分布抽取随机数来判断某一时刻对应设备的状态，再结合所得随机数与最小割序的顺序失效域判断该最小割序是否发生，如果发生（即系统失效），则跳入下一次模拟；如果不发生则进行下一个最小割序的判断，以此类推，直到完成所有最小割序的判断。当模拟次数足够多时，便可根据模拟结果得到DFT顶事件的发生概率，该方法的整体流程图如图3所示。其中：N 是总模拟次数，在相对误差为0.05并且置信水平为0.95的情况下，N=1 600/$\underline{P}_{\mathrm{f}}$ 即可确保模拟的结果足够可靠，$\underline{P}_{\mathrm{f}}$ 为事件的统计频率[11]。m 表示最小割序的个数，$\hat{\tau}_t=(\hat{\tau}_1^{(t)},\hat{\tau}_2^{(t)},...,\hat{\tau}_n^{(t)})$ 为失效时间 $\tau_t=(\tau_1,\tau_2,...,\tau_n)$ 的第 t 次随机抽样样本点。割序 $A_1 \to {}_{A_1}{}^{0}A_2 \to \cdots \to {}_{A_{n-1}}{}^{0}A_n$ 的发生概率可以表示为：

$$Pr\left\{A_1 \to {}_{A_1}{}^{0}A_2 \to \cdots \to {}_{A_{n-1}}{}^{0}A_n\right\}=\frac{1}{N}\sum_{t=1}^{N}I\left[h(\hat{\tau}_t)\right] \tag{2}$$

其中：$I[h(\hat{\tau}_t)]$ 为统计示性函数（Statistic Indicator Function，SIF），表达式如（3）所示：

$$I\left[h(\hat{\tau}_t)\right]=\begin{cases}1, & \hat{\tau}_t\in\Omega(\hat{\tau}_1^{(t)}\in R(\tau_1),\hat{\tau}_2^{(t)}\in R(\tau_2),...,\hat{\tau}_n^{(t)}\in R(\tau_n))\\ 0, & \text{other}\end{cases} \tag{3}$$

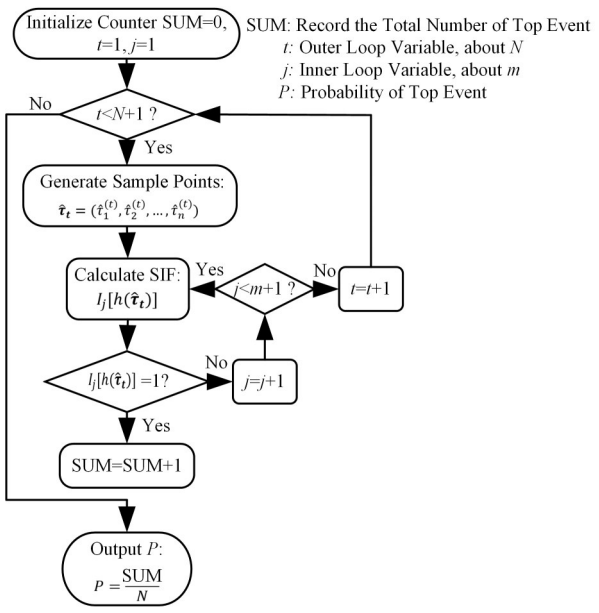

图3 基于最小割序集的动态故障树蒙特卡罗数值模拟流程图

Fig.3 Flow chart of Monte Carlo numerical simulation of DFTs based on minimum cut sequence sets

2 考虑设备启动时间与启动失效的冷冗余系统可靠性数值模拟方法

数值模拟作为一种虚拟现实技术可以直接仿真设备的启动时间以及启动状态过程，因此可用于冷冗余系统可靠性分析。

2.1 包含冷冗余设备的割序失效域

假设某最小割序为：

$$A_1 \to {}_{A_1}{}^{0}A_2 \to \cdots \to {}_{A_{i-1}}{}^{0}A_i \to \cdots \to {}_{A_{n-1}}{}^{0}A_n$$

其中：基本事件 A_i（i=2，…，n）表示冷冗余设备。下面以冷冗余设备 A_i 为例进行讨论，假设 A_i 启动时间为 Δt_i，启动失效概率为 P_i，其存在两种失效模式：1）启动未成功，即在启动过程中直接失效，用符号 $\underline{A}_{i.a}$ 表示；2）设备成功启动，在后续工作过程中发生随机失效，用符号 $\underline{A}_{i.w}$ 表示。本文中用随机数 R_i=rand 来模拟设备启动的结果，若 $R_i<P_i$，代表设备启动失效；若 $R_i\geqslant P_i$，则代表设备启动成功。鉴于这两种失效模式互斥，该割序的发生概率可表示为：

$$Pr\left\{A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}A_i \to \cdots \to {}^{0}_{A_{n-1}}A_n\right\} = Pr\left\{A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,a} \to \cdots \to {}^{0}_{A_{n-1}}A_n\right\} + Pr\left\{A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,w} \to \cdots \to {}^{0}_{A_{n-1}}A_n\right\} \tag{4}$$

针对割序：

$$A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,a} \to \cdots \to {}^{0}_{A_{n-1}}A_n$$

设备A_i在启动中直接失效，不存在后续随机失效情况，其对应的顺序失效逻辑图如图4所示。由图可得，当$k<i$时，各基本事件的有效失效时间段表达式与§1.2中一致，可写为$R(\tau_k)_a=\{\tau_k|0<\tau_k<t_m-\tau_1-\cdots-\tau_{k-1}\}$；当$k=i$时，由于不存在随机失效的情况，因此不考虑$\underline{A}_{i,a}$对应的有效失效时间段。当$i<k\leqslant n$时，由于启动时间$\Delta t_i$的存在，此类基本事件的有效失效时间段需考虑$\Delta t_i$的影响，可表示为：

$$R(\tau_k)_a=\left\{\tau_k|0<\tau_k<t_m-\tau_1-\cdots-\tau_{i-1}-\tau_{i+1}-\cdots-\tau_{k-1}-\triangle t_i\right\}$$

因此，割序$A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,a} \to \cdots \to {}^{0}_{A_{n-1}}A_n$的失效域$\Omega_a$可以表达为：

$$\Omega_a=\bigcap_{k=1}^{n}R(\tau_k)_a,\ k\neq i \tag{5}$$

对于割序：

$$A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,w} \to \cdots \to {}^{0}_{A_{n-1}}A_n$$

设备成功启动后发生随机失效，对应的顺序失效逻辑图如图5所示。由图5可得，当$k<i$时，各基本事件的有效失效时间段的表达式可表示为$R(\tau_k)_w=\{\tau_k|0<\tau_k<t_m-\tau_1-\cdots-\tau_{k-1}\}$；当$i\leqslant k\leqslant n$时，各基本事件的有效失效时间段可表示为：

$$R(\tau_k)_w=\{\tau_k|0<\tau_k<t_m-\tau_1-\cdots-\tau_{i-1}-\tau_i-\tau_{i+1}-\cdots-\tau_{k-1}-\triangle t_i\}$$

因此，

割序$A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,w} \to \cdots \to {}^{0}_{A_{n-1}}A_n$的失效域$\Omega_w$可以表达为：

$$\Omega_w=\bigcap_{k=1}^{n}R(\tau_k)_w \tag{6}$$

2.2　基于最小割序集的数值模拟方法

本方法与“最小割序集+顺序失效域”的DFT数值模拟方法类似。首先判断一个割序是否发生，如果发生则跳出本次模拟；如果不发生，则模拟下一个割序，以此类推。模拟流程如图6所示，其中：G_j表示在最小割序j中需要考虑启动时间与启动失效的冷冗余设备个数，其余符号的含义与图3一致。

图6中如何“计算当前最小割序j的失效域”为本文讨论的重点，该过程主要包括三部分：1）对最小割序进行分类；2）对设备启动过程进行模拟；3）最小割序失效域的计算。首先根据当前最小割序中是否含有需要考虑启动时间与启动失效的冷冗余设备进行分类讨论。对于不含此类冷冗余设备的最小割序，按§1.2中所提到的方法计算其失效域；对于包含的最小割序，则§2.1中的方法对所含设备的启动状态用随机数进行模拟，并记录模拟结果。最后依据模拟结果求解最小割序所对应的失效域Ω_j，如式（7）所示。通过Ω_j与$\hat{\tau}_t$判断本次模拟中当前最小割序是否发生，如式（8）所示。如果发生则跳出本次模拟；如果不发生，则模拟下一个割序，以此类推。

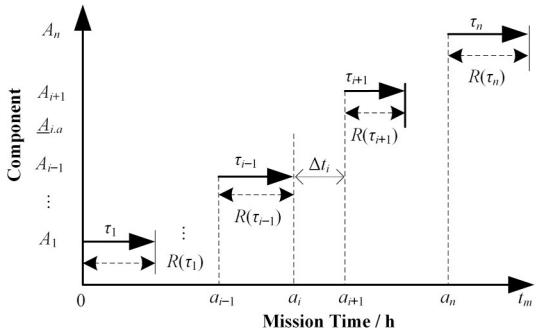

图4　$A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,a} \to \cdots \to {}^{0}_{A_{n-1}}A_n$的顺序失效逻辑图

Fig.4　Sequence failure logic diagram for case: $A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,a} \to \cdots \to {}^{0}_{A_{n-1}}A_n$

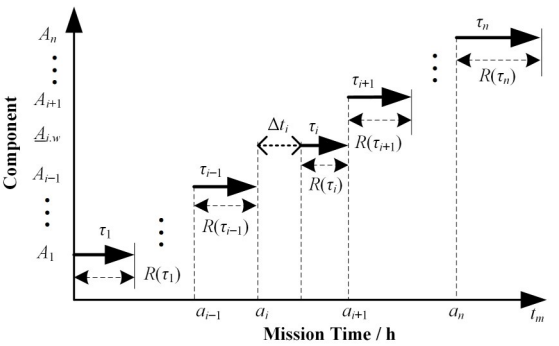

图5　$A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,w} \to \cdots \to {}^{0}_{A_{n-1}}A_n$的顺序失效逻辑图

Fig.5　Sequence failure logic diagram for case: $A_1 \to {}^{0}_{A_1}A_2 \to \cdots \to {}^{0}_{A_{i-1}}\underline{A}_{i,w} \to \cdots \to {}^{0}_{A_{n-1}}A_n$

$$\Omega_j=\begin{cases}\Omega_a, R_i<P_i\\ \Omega_w, R_i\geqslant P_i\end{cases} \tag{7}$$

$$I_j[h(\hat{\tau}_t)]=\begin{cases}1, \hat{\tau}_t\in\Omega_j\\ 0, \text{ other}\end{cases} \tag{8}$$

最终，系统的失效概率（P_{system}）可计算为所有最小割序发生的次数（SUM）除于总仿真次数N。冷冗余系统失效概率的统计量表达式为：

$$P_{\text{system}} = \frac{\sum_{j=1}^{m} I_j[h(\hat{\tau}_t)]}{N} = \frac{\text{SUM}}{N} \tag{9}$$

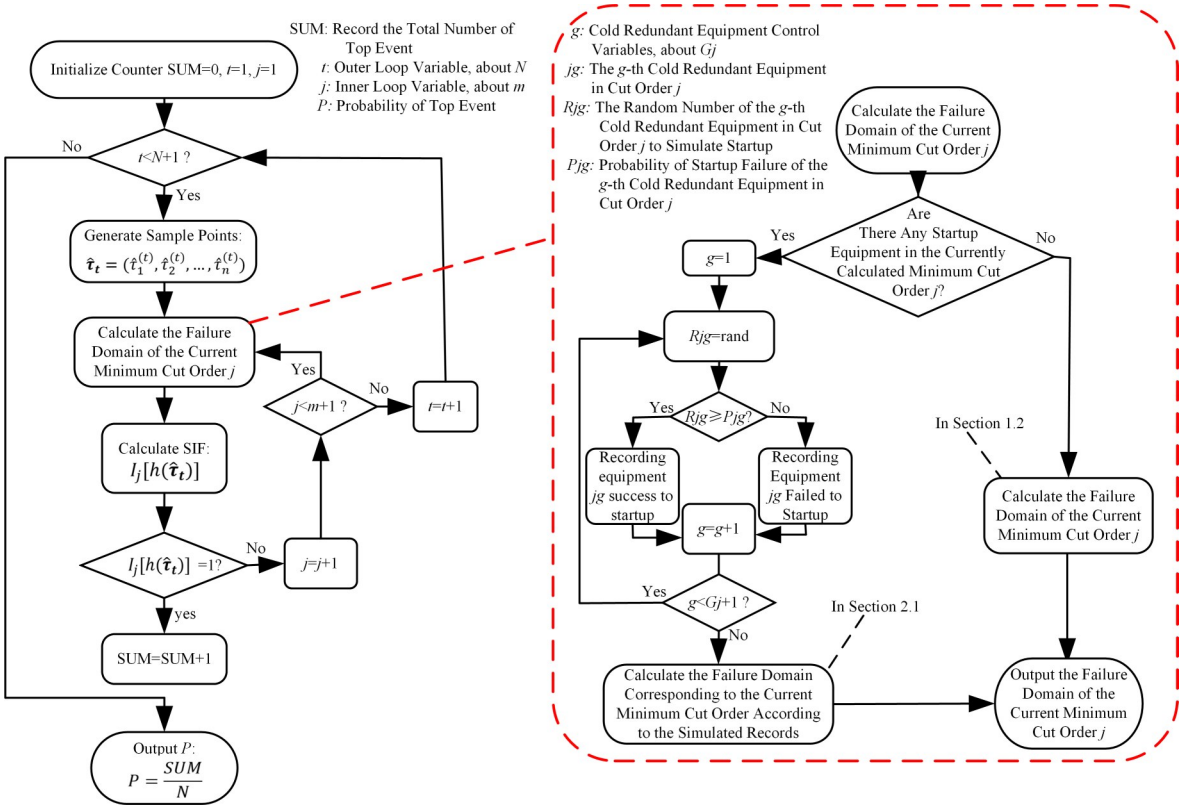

图6 基于蒙特卡罗数值模拟的DFT中设备启动时间与启动失效建模方法

Fig.6 Modeling method of equipment startup time and startup failure in DFT based on Monte Carlo numerical simulation

3 案例分析

3.1 事故描述

应急柴油发电机组（Emergency Diesel Generators，EDGs）是核电厂重要的专设安全设施之一。作为核电厂内的应急电源，在丧失厂用主电源和外电源后，EDGs要及时启动为应急厂用设备供电，以保证反应堆安全停堆并防止主要设备损坏。图7展示的是某核电厂单机组的电力供应系统结构简图[12]。其中EDGs共包含5台柴油发电机（4台常规柴油发电机+1台备用柴油发电机）。4台常规柴油发电机被分为两个应急发电机组：应急发电机组A（包含柴油发电机A1与柴油发电机A2）和应急发电机组B（包含柴油发电机B1与柴油发电机B2）。

丧失场外电事件发生后，首先启动A，此时B处于冷备状态。A可能会由于自身发生随机失效或者应急安全母线LHA故障而失效。当A失效后，B才会启动。同样地，B可能会由于自身发生随机失效或者应急安全母线LHB故障而失效[13]。当A、B都失效后备用柴油发电机才会启动，当备用柴油发电机也失效后，SBO事故发生。在这种情况下EDGs的故障顺序是：首先A发生失效，接着B启动并失效，最后备用柴油发电机启动并失效，SBO事故发生。本文将使用DFT对系统顺序失效行为进行建模，并将在§3.2中进行详细说明。

3.2 应急柴油发电机系统的动态失效模型及设备失效参数

应急发电机组B与备用柴油发电机平时处于冷备用状态，由于发电机组放置区域、人员的操作和设备的状态等一系列不确定性因素，到备用柴油发电机真正投入使用需要一定的启动时间Δt。在核电厂运行的历史上曾出现过应急柴油发电机启动失败的案例[14-15]。启动油量的控制[2]、快速启动导致的柴油发电机老化[16]、系统接线和现场布置错误[17]等都是影响柴油发电机能否正常启动的因素。本文假这些处于冷备状态的柴油发电机具有一定的启动失效概率P。EDGs中相关设备的失效参数参考文献[12]与[13]，具体如表1所示。以EDGs供电失效为顶事

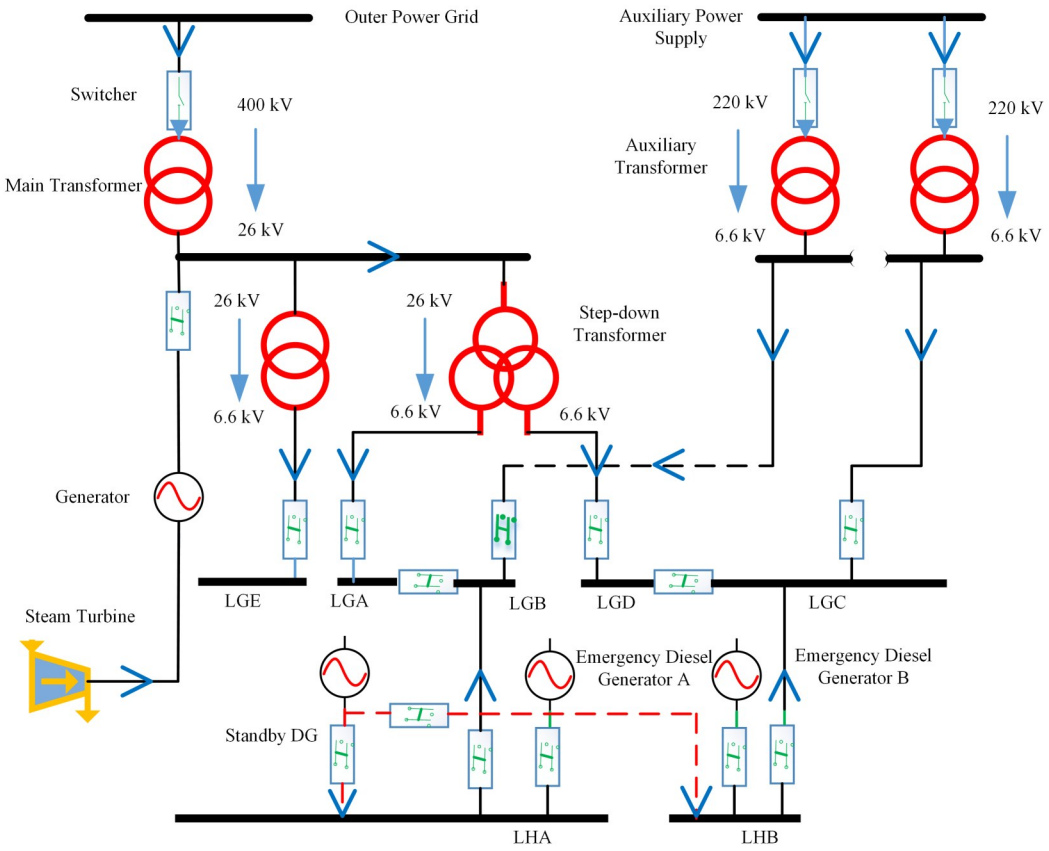

图7 某核电厂简化电力供应系统图
Fig.7 System diagram of simplified power supply for nuclear power plant

件，根据§3.1中描述的失效行为对系统进行DFT建模分析，DFT模型如图8所示。SEQ门表征EDGs备件中存在的强制顺序失效行为，FDEP门表征LHA/LHB与A/B之间的依赖关系。

3.3 计算分析

3.3.1 失效概率对比分析

采用所提方法、传统DFT方法和SFT方法分别计算EDGs在任务时间t=24 h内的失效概率，并着重比较了所提方法与传统DFT方法的计算差异，即两种方法所得结果的相对误差$\varepsilon=(P_{\mathrm{D}}-P_{\mathrm{P}})/P_{\mathrm{D}}\times100\%$，其中：$P_{\mathrm{D}}$为传统DFT方法的计算结果；$P_{\mathrm{P}}$为所提方法的计算结果；$\varepsilon$计算结果如图9(a)所示。计算平台为MATLAB软件，样本数的设置同§1.2一致，事件的统计频率$\underline{P}_{\mathrm{f}}$用传统DFT方法对应的结果做代替。从图9(a)可以看出，由于考虑了柴油发电机的冷备特性与启动时间，本文所提方法得到的系统失效概率较SFT与传统DFT方法更低。由于考虑了启动时间，本文所提方法的计算结果较传统DFT方法有明显的改善，尤其是在任务初期。启动时间所产生的影响有限，且随着任务时间的增加ε不断减小，在24 h时，ε=10.20%。此外，本文进一步探究了

表1 EDGs设备的失效信息
Table 1 Failure information of EDGs

设备名称 Equipment name	失效率 Failure rate / h	启动失效概率 Probability of startup failure	启动时间 Startup time / h
A1	0.019 9	—	—
A2	0.019 9	—	—
B1	0.019 9	0.023 6	0.2
B2	0.019 9	0.023 6	0.2
SDG	0.019 9	0.023 6	0.5
LHA	4.73×10^{-7}	—	—
LHB	4.73×10^{-7}	—	—

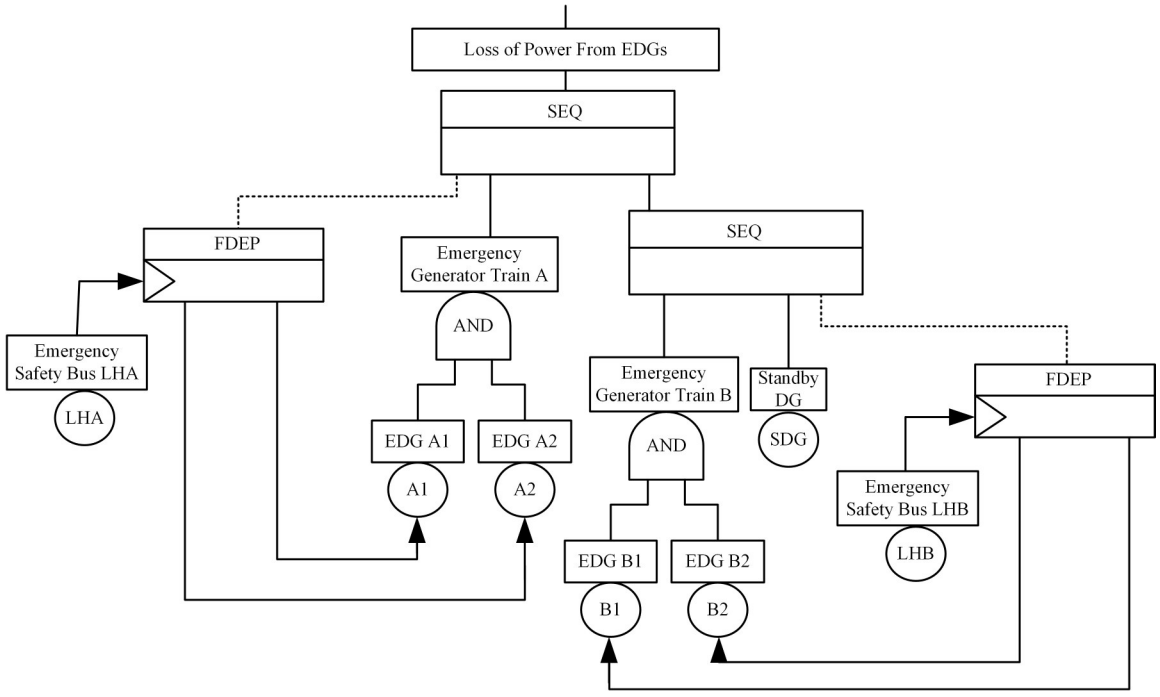

图8 EDGs的DFT模型[13]
Fig.8 DFT model of EDGs[13]

影响此概率差的因素以及这些影响因素单独所占的份额，结果如图9(b)所示。ε_{B1}、ε_{B2}和ε_{SDG}分别表示只考虑对应柴油发电机启动时间时，所提方法与传统DFT方法计算结果的相对误差；ε_0则表示不考虑启动时间时的相对误差。从图9(b)可以看出，在不考虑启动时间时，本文所提方法与传统DFT方法结果一致，即所提方法中对启动失效概率的处理符合传统方法中“将设备的启动失效视为基本事件”的假设，因此两种方法的结果差异来自于启动时间。而在B1、B2和SDG这三个设备的启动时间中，SDG的启动时间对结果的影响最大。

3.3.2 参数敏感性分析

为了评估各参数对系统失效概率不确定性贡献的重要程度，本文对EDGs中相关参数进行了敏感性分析，计算公式如下所示：

$$S_X = \frac{R_U}{R_L} \tag{10}$$

式中：R_U为参数X的值是原来的10倍时系统失效概率；R_L为参数X的值是原来的0.1倍时系统失效概率。S_X为参数X的敏感度，当S_X>1，表示该参数对系统失效具有正面影响，而S_X越偏离1表示参数对系统失效概率的影响越大。图10展示了在任务时间24 h内设备参数的敏感度变化曲线，表2为各参数

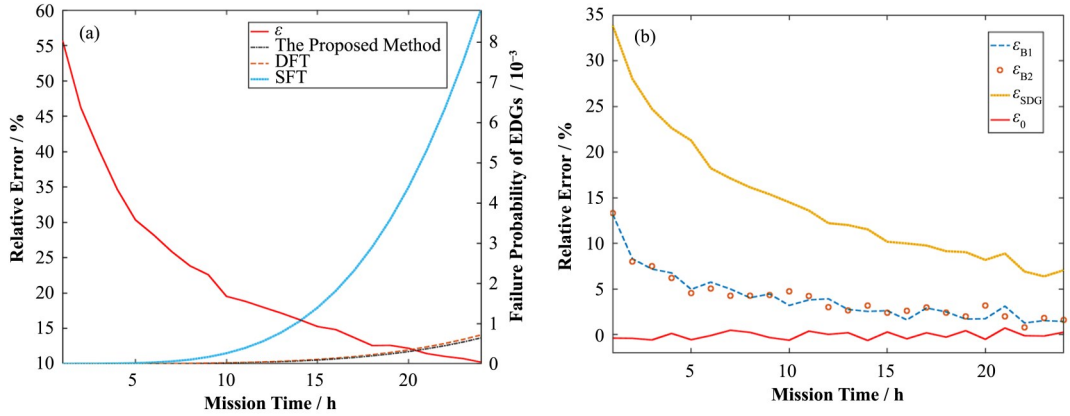

图9 EDGs失效概率对比分析 (a) 失效概率对比，(b) 设备启动时间对EDGs失效概率的影响
Fig.9 Comparison of EDGs failure probability (a) Failure probability comparison, (b) Effect of equipment startup time on EDGs failure probability

在t为2 h和24 h时对EDGs系统失效概率的敏感度及其排名，其中P_{B1}、P_{B2}和P_{SDG}分别表示对应柴油发电机的启动失效概率；λ_{LHA}和λ_{LHB}分别表示应急安全母线LHA和LHB的失效率；λ_{A1}、λ_{A2}、λ_{B1}、λ_{B2}和λ_{SDG}分别表示对应柴油发电机的失效率。

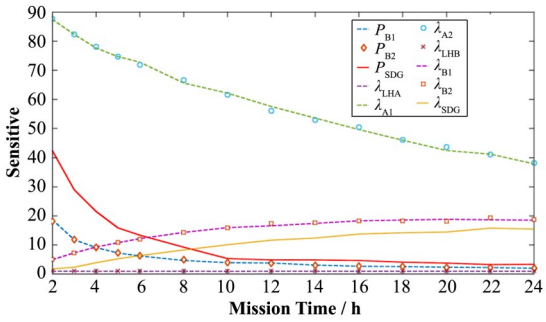

图10 设备参数的敏感度变化曲线
Fig.10 The sensitivity change curve of equipment parameters

由图10和表2可知，在初始阶段“λ_{A2}”和“λ_{A1}”是最敏感的参数，敏感度为88.02和87.32。启动失效参数“P_{SDG}”、“P_{B1}”和“P_{B2}”分别排在第3、4、5位，敏感度为42.38、19.08和18.13，对系统的失效有显著影响。随着任务时间的增加，在24 h时最敏感的参数为“λ_{A2}”和“λ_{A1}”，敏感度为38.45和37.89。排在第3位和第4位的则分别是“λ_{B2}”和“λ_{B1}”。而启动失效参数“P_{SDG}”、“P_{B2}”和“P_{B1}”分别排在第6、7、8位，敏感度为3.38、2.17和2.09。综上所述，由于启动相关参数是固定值，因此在初始阶段对结果影响较大，随着任务时间的增加，影响逐渐减小。因此，提高柴油发电机的启动可靠性尤其是在初始阶段，对提高EDG的整体安全性具有重要意义。

3.3.3 不确定性分析

考虑到设备启动时间的随机性，本文对EDGs失效概率进行不确定性分析。假设设备启动时间服从正态分布，具体如表3所示。系统任务时间设置为24 h，通过抽样程序获得1 000组启动时间的样本，然后将每一组样本输入到所提方法的计算模型中产生一个随机输出样本（EDGs失效概率）。最后将1 000个EDGs失效概率绘制成频率直方图，如图11所示。

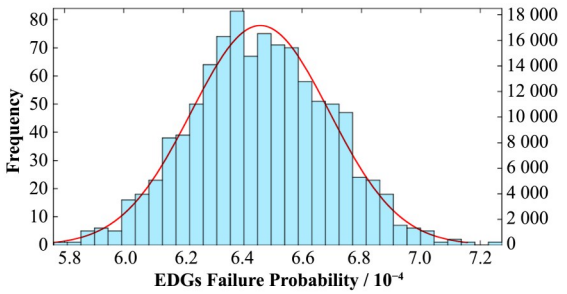

图11 EDGs失效概率的频率直方图
Fig.11 Frequency histogram of EDGs failure probability

从图11可以看出，EDGs失效概率服从正态分布。表4展示了EDGs失效概率均值、标准差以及对应的置信区间。由表4可知，在24 h内EDGs发生失效的概率的置信水平为95%的置信区间为（6.445~6.474）×10^{-4}。

表2 EDGs设备参数的敏感性指标
Table 2 Sensitivity index of EDGs equipment parameters

参数名称 Parameters name		P_{B1}	P_{B2}	P_{SDG}	λ_{LHA}	λ_{A1}	λ_{A2}	λ_{LHB}	λ_{B1}	λ_{B2}	λ_{SDG}
2 h	S_X	19.08	18.13	42.38	1.03	87.32	88.02	1.02	4.98	5.19	1.80
	Rank	4	5	3	9	2	1	10	7	6	8
24 h	S_X	2.09	2.17	3.38	1.00	37.89	38.45	0.99	18.54	18.72	15.44
	Rank	8	7	6	9	2	1	10	4	3	5

表3 启动时间的分布参数
Table 3 Distribution parameters of startup-time

设备名称 Equipment name	启动时间均值 Average startup time Δt / h	标准差 Standard deviation
B1	0.2	0.066 7
B2	0.2	0.066 7
SDG	0.5	0.166 7

表4 参数估计结果
Table 4 Results of parameters evaluations

发生概率 Probability of occurrence	均值 Mean	均值置信区间(95%) Mean confidence interval (95%)	标准差 Standard deviation	标准差置信区间(95%) Standard deviation confidence interval (95%)
EDGs	6.459×10^{-4}	$(6.445\sim6.474)\times10^{-4}$	2.325×10^{-5}	$(2.227\sim2.432)\times10^{-5}$

3.3.4 启动特性对结果的影响

根据国内外核电站运行经验，适当延长柴油发电机启动时间，有利于降低其启动失败概率，延长运行寿命[16]。因此，本文假设柴油发电机的启动时间与启动失效概率成反比，即启动时间与启动失效概率的乘积为一个定值K，本文称之为启动常数，具体如下所示：

$$K = P_{\Delta t} \cdot \Delta t \tag{11}$$

式中：Δt为启动时间；$P_{\Delta t}$为Δt时间内的启动失效概率。K可以通过设备当前的启动时间和启动失效概率乘积获得，如表5所示。为评估启动特性对EDGs失效概率的影响，启动时间分别选取为表1中启动时间的20%、60%、140%和180%。计算EDGs在任务时间t=24 h内的失效概率，并与原结果进行比较，如图12(a)所示。由于在不同启动时间下系统失效概率间的数值差异过大，为了更直观地比较系统失效概率变化趋势，本文采用对数ln(θ)来展示，具体如图12(b)所示，其中$\theta=P_X/P_p$；P_X为基于新的启动参数的计算结果。可以看出，在任务初期，启动时间变化对结果有较大影响，且随着启动时间的延长，系统失效概率随之降低。

表5 设备的启动常数
Table 5 Startup constants of equipment

设备名称 Equipment name	启动常数 Startup constants
B1	0.004 72
B2	0.004 72
SDG	0.011 8

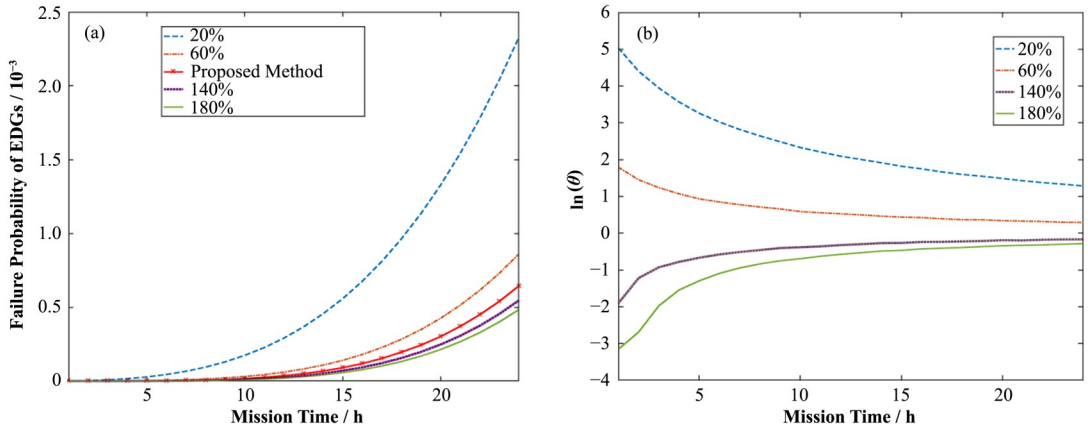

图12 启动特性对EDGs失效概率的影响 (a) 不同启动时间下的概率值，(b) 不同启动时间下的ln(θ)值
Fig.12 Effect of startup characteristics on EDGs failure probability (a) Probability under different start time, (b) ln(θ) under different start time

4 结语

本文重点研究了备用设备启动时间与启动失效对冷冗余系统失效概率的影响，提出了一种冗余系统可靠性数值模拟方法，利用所提方法对核电厂EDGs失效概率进行了分析。案例结果分析表明：1）本文所提方法能够对以往方法无法考虑冷备件启动时间耦合启动失效的问题进行建模分析，从而能更加准确地反映冷冗余系统的实际运行状态与真实的失效场景；2）启动时间对结果影响在任务早期较大，后随任务时间的增长而减小；3）设备参数的敏感性分析为后期提高系统可靠性提供了理论依据；4）在24 h内EDGs发生失效的概率的置信水平为95%的置信区间为(6.445~6.474)×10^{-4}；5）适当延长柴油发电机启动时间有利于降低EDGs系统的失效概率。本文中案例的计算结果展示了该方法在精确建模与释放保守风险方面的潜力，未来将针对核电厂复杂系统开展更为详细的建模研究。

致谢 感谢中国科学院合肥物质科学研究院核能安全技术研究所公共技术中心提供测试平台。

作者贡献声明 王韶轩：起草文章、统计分析、设计分析案例；林志贤：技术支持、分析数据；戈道川：审阅文章内容、技术指导；吴洁：审阅文章内容；郁杰：形式检查、方向指导。

参考文献

1 董毅漫, 张弛, 宋大虎, 等. 我国核电安全目标发展取向的思考[J]. 核安全, 2012, **11**(4): 10－15. DOI: 10.16432/j.cnki.1672-5360.2012.04.007.
DONG Yiman, ZHANG Chi, SONG Dahu, *et al*. Thinking of nuclear power safety goal development orientation in China[J]. Nuclear Safety, 2012, **11**(4): 10－15. DOI: 10.16432/j.cnki.1672-5360.2012.04.007.

2 闵济东, 赖斌生, 余泽辉, 等. 核电厂某型应急柴油机启动超时的原因分析[J]. 科技视界, 2020(33): 98 – 100. DOI: 10.19694/j.cnki.issn2095-2457.2020.33.040.
MIN Jidong, LAI Binsheng, YU Zehui, *et al*. Cause analysis of starting overtime of an emergency diesel engine in nuclear power plant[J]. Science & Technology Vision, 2020(33): 98 – 100. DOI: 10.19694/j. cnki. issn2095-2457.2020.33.040.

3 张瑞明, 林建, 雷亚清. 关于A核电站水压试验泵启动失败的探究[J]. 电子测试, 2013(23): 142 – 143. DOI: 10.3969/j.issn.1000-8519.2013.23.063.
ZHANG Ruiming, LIN Jian, LEI Yaqing. The analysis of the hydrotest pump start failure of A nuclear power station [J]. Electronic Test, 2013(23): 142 – 143. DOI: 10.3969/j. issn.1000-8519.2013.23.063.

4 Fahmy R A, Gomaa R I. Dynamic fault tree analysis of auxiliary feedwater system in a pressurized water reactor [J]. Kerntechnik, 2021, **86**(2): 164 – 172. DOI: 10.1515/kern-2020-0067.

5 Ghadhab M, Junges S, Katoen J P, *et al*. Safety analysis for vehicle guidance systems with dynamic fault trees[J]. Reliability Engineering & System Safety, 2019, **186**: 37 – 50. DOI: 10.1016/j.ress.2019.02.005.

6 Dugan J B, Bavuso S J, Boyd M A. Dynamic fault-tree models for fault-tolerant computer systems[J]. IEEE Transactions on Reliability, 1992, **41**(3): 363 – 377. DOI: 10.1109/24.159800.

7 高僮. 基于动态故障树和蒙特卡罗仿真的列控系统风险分析研究[D]. 北京: 北京交通大学, 2014.
GAO Tong. Research on dynamic fault tree and Monte Carlo based risk analysis of train control system[D]. Beijing: Beijing Jiaotong University, 2014.

8 苗祚雨. 基于确定随机Petri网和蒙特卡罗仿真的动态故障树定量可靠性分析方法研究[D]. 北京: 北京交通大学, 2014.
MIAO Zuoyu. Research on dynamic fault tree quantitative reliability analysis method based on deterministic and stochastic Petri net and Monte Carlo simulation[D]. Beijing: Beijing Jiaotong University, 2014.

9 Ge D C, Li D, Lin M, *et al*. SFRs-based numerical simulation for the reliability of highly-coupled DFTs[J]. Eksploatacja i Niezawodnosc - Maintenance and Reliability, 2015, **17**(2): 199 – 206. DOI: 10.17531/ein.2015.2.5.

10 戈道川. 核电厂系统动态故障树快速可靠性分析及风险成本多目标优化方法研究[D]. 上海: 上海交通大学, 2016.
GE Daochuan. Research about quick dft-based reliability analysis and risk vs cost multiple objectives optimization of nuclear power plant systems[D]. Shanghai: Shanghai Jiao Tong University, 2016.

11 张建国, 苏多, 刘英卫. 机械产品可靠性分析及优化[M]. 北京: 电子工业出版社, 2008.
ZHANG Jianguo, SU Duo, LIU Yingwei. Reliability analysis and optimization of mechanical products[M]. Beijing: Electronic Industry Press, 2008.

12 李哲. 基于GO法的核电厂LOOP事件及SBO事件可靠性分析[D]. 北京: 清华大学, 2011.
LI Zhe. Reliability analysis of LOOP and SBO events in nuclear power plant based on the GO methodology[D]. Beijing: Tsinghua University, 2011.

13 Guo D Q, Yang M J, Wu H M, *et al*. Dynamic reliability evaluation of diesel generator system of one Chinese 1 000 MWe NPP considering temporal failure effects[J]. Frontiers in Energy Research, 2021, **9**: 793577. DOI: 10.3389/fenrg.2021.793577.

14 张明佳. 核电站应急柴油发电机组可靠性数据的建立与应用[D]. 上海: 上海交通大学, 2009.
ZHANG Mingjia. Development of reliability data npp emergency diesel generator set in nuclear power plant and its application[D]. Shanghai: Shanghai Jiao Tong University, 2009.

15 Rossi C E. Information notice No.90-25: loss of vital AC power with subsequent reactor coolant system heat-up[R]. Nuclear Regulatory Commission, NRC, Office of Nuclear Reactor Regulation, Washington D C, 20555, 1990: 285.

16 周勇, 朱鹏树, 陈星, 等. 核电站应急柴油发电机组慢启动优化研究[J]. 核科学与工程, 2018, **38**(4): 689 – 695.
ZHOU Yong, ZHU Pengshu, CHEN Xing, *et al*. Research on slow start optimization of emergency diesel generator sets in nuclear power plants[J]. Nuclear Science and Engineering, 2018, **38**(4): 689 – 695.

17 万寒阳. 核电厂应急柴油发电机特点及调试管理[J]. 科技视界, 2020(13): 141 – 143. DOI: 10.19694/j. cnki. issn2095-2457.2020.13.52.
WAN Hanyang. Characteristics and commissioning management of emergency diesel generators in nuclear power plants[J]. Science and Technology Vision, 2020 (13): 141 – 143. DOI: 10.19694/j. cnki. issn2095-2457. 2020.13.52.