核动力工程
Nuclear Power Engineering
EI工程索引(美国)(2021)收录
CA化学文摘(美国)(2020)收录
JST日本科学技术振兴机构数据库(日本)(2020)收录
北大中文核心期刊（2020版）收录

核电厂仪控系统误动作事故分析

蔡　伟，鲍国刚，乐志东，路长冬

Analysis of Mal-Operation Accidents of Nuclear Power Plant I&C System

Cai Wei, Bao Guogang, Yue Zhidong, and Lu Changdong

在线阅读 View online: https://doi.org/10.13832/j.jnpe.2021.05.0167

文章编号：0258-0926(2021)05-0167-06; doi:10.13832/j.jnpe.2021.05.0167

核电厂仪控系统误动作事故分析

蔡 伟，鲍国刚，乐志东，路长冬

中广核研究院有限公司上海闵行分公司，上海，200241

摘要：为全面评价核电厂仪控系统误动作事故，提出基于简化分析的方法，该方法基于功能组概念对仪控误动作假设始发事件（PIE）进行了系统化地识别和归并，得到不能被已有事故分析包络的潜在新增事故工况，并根据保守的分析假设和准则，针对识别出的潜在新增事故进行了定性评价和定量分析。研究结果表明，核电厂保护系统能够对仪控系统误动作事故提供多样化保护，事故后果满足验收准则，并建议增设“2个热管段实际压力与饱和压力之差低 2 信号触发安注启动以及所有主泵停运”功能。

关键词：仪控系统误动作；假设始发事件（PIE）；事故分析；多样化保护

中图分类号：TL364^{+}.4 **文献标志码：**A

Analysis of Mal-Operation Accidents of Nuclear Power Plant I&C System

Cai Wei, Bao Guogang, Yue Zhidong, Lu Changdong

Shanghai Minhang Branch, China Nuclear Power Technology Research Institute Co., Ltd., Shanghai, 200241, China

Abstract: A method based on the simplified analysis was proposed in order to comprehensively evaluate the accidents of spurious actuation of Instrumentation and Control (I&C) systems of the Nuclear Power Plant (NPP). Based on the concept of “functional group”, the Postulated Initiating Events (PIEs) of spurious I&C actuation were systematically identified and grouped to obtain the potential additional accidents that cannot be bounded by the existing accident analysis. Then these potential additional accidents were qualitatively assessed and quantitatively analyzed according to the conservative analysis assumptions and rules. The results show that the protection systems of the NPP can provide diverse protection against the spurious I&C accidents and the consequences meet the acceptance criteria. Besides, the function of “startup of safety injection and trip of the main pumps triggered by the low 2 signal of the difference between the local pressure and saturation pressure in two hot legs” was suggested to be added.

Key words: Mal-operation of I&C system, Postulated initiating event (PIE), Accident analysis, Diverse protection

0 引 言

仪控系统对于核电厂运行控制和事故保护至关重要，须重视其潜在失效风险。各国监管法规均要求核电厂设计中必须考虑所有可预见的仪控系统和部件失效以及共因故障（CCF）风险，实现纵深防御[1-2]。实践中，设计者往往偏重系统拒动这一失效模式，通过设置多样化保护系统，在主保护系统失效时提供后备安全功能[3-5]。实际上现代仪控系统误动作（简称仪控误动作）事件概率和风险同样可观[6-7]，然而，针对仪控误动作问题，当前研究存在的不足：①缺少对仪控误动作事件的全面识别，分析范围不够全面；②分析局限于单个误动事故，对于 CCF 的影响评价不够。国际上，对于仪控误动作评价，英国已经明确提

收稿日期：2020-07-28；**修回日期：**2020-09-02

作者简介：蔡 伟（1983—），男，高级工程师，硕士，现主要从事核电厂安全分析研究，E-mail: laocaihehe@sina.com

出监管要求[8]，经合组织核能署（NEA）也发布了共识文件[9]，但目前业界还缺少一个清楚、充分的监管导则，从而使分析评价存在困难和不确定性[10]。

为此，本研究尝试提出基于简化分析的方法，基于功能组对仪控误动作假设始发事件（PIE）进行较为全面系统地识别；根据保守的分析准则并考虑系统 CCF，对识别出的潜在新增事故进行分析评价，论证核电厂保护系统对事故的缓解作用，从而补充完善安全分析结果，并为仪控误动作事故分析方法论和导则研究提供参考。

1 仪控误动作事故分析流程

仪控误动作分析主要包括 3 个步骤：PIE 识别、PIE 归并以及事故分析与评价，总体流程如图 1 所示。

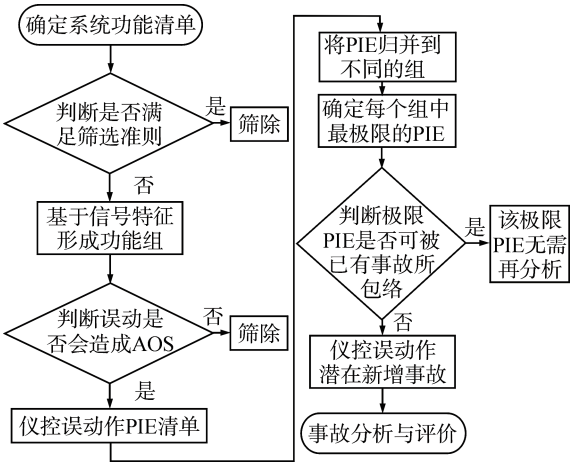

图 1 仪控误动作事故分析流程

Fig. 1 Analysis Procedure for I&C Mal-Operation Accidents

AOS—异常运行状态

2 PIE 识别与归并

2.1 PIE 识别

由于仪控系统工艺设计中通常已考虑单个部件随机失效，因此本研究聚焦多个部件 CCF。鉴于仪控系统的复杂性，不可能罗列所有部件的全部失效组合，需要加以简化。本研究基于功能组概念对主要仪控误动作进行识别，其中功能组定义为具有相似信号特征的一组系统功能，必须满足相似的系统平台、核电厂状态、功能类型和误触发信号等条件。如反应堆保护系统（RPS）误触发蒸汽发生器（SG）窄量程高水位信号，导致紧急停堆和主给水满负荷管线自动隔离，则该信号与 2 个自动功能称为 1 个功能组。

在产生功能组时，如果符合表 1 中的筛选准则，则该功能不予考虑。此外，采取以下假设[9]：①考虑核电厂正常运行的各种状态，包括：1-功率运行、2-热备用、3-热停堆、4-SG 冷却中间停堆、5-余热排出系统（RHR）冷却停堆和 6-冷停堆（1~6 为核电厂状态编号）；②仅考虑单个功能组误动作，不考虑多个独立功能同时触发或与其他事故叠加；③考虑“允许信号”对相应功能的闭锁作用。

表 1 系统功能筛选准则

Tab. 1 Screening Criteria for System Functions

序号	准则	说明
1	就地操作功能	不需要仪控系统控制
2	非能动功能	不需要仪控系统控制
3	指示功能	不直接驱动设备
4	允许信号功能	不直接驱动设备
5	不改变设备状态	不会造成AOS

得到功能组后，通过判断误动作是否会造成核电厂 AOS 识别出 PIE。

根据以上方法和原则，对华龙一号核电机组进行仪控误动作分析，分析范围包括：①电厂控制和保护系统，包括 RPS、安全自动化系统（SAS）、多样化驱动系统（KDS）、电厂标准自动化系统（PSAS）和严重事故仪控系统（KDA）；②含有仪控部件的主要工艺系统，包括主系统、辅助系统和专设安全系统等共 29 个系统。经过对数百个功能组的识别以及合并简化，共得到 109 个功能组误动作 PIE。

2.2 PIE 归并

归并目的是对导致相似瞬态后果的 PIE 进行合并和简化，识别潜在新增事故。归并过程步骤如下：①根据瞬态特征和后果对 PIE 进行分组，分组结果见表 2；②在每个组中通过包络分析确定导致最严重后果的极限 PIE；③判断极限 PIE 是否可被核电厂已有事故分析 [包括设计基准工况（DBC）和未造成堆芯损伤的 A 类设计扩展工况（DEC-A）] 所包络，如是，则无需再分析，否则产生潜在新增事故。

表 2　PIE 瞬态分组

Tab. 2　Groups of PIEs by Transients

分组	瞬态说明	PIE数量
A	二次侧排热增加	13
B	二次侧排热减少	30
C	反应堆冷却剂流量减少	5
D	反应性与功率分布异常	8
E	反应堆冷却剂装量增加	20
F	反应堆冷却剂装量减少	23
G	反应堆冷却剂系统压力升高/下降	6
H	乏燃料水池相关事故	4

在归并过程中，采取如下保守假设：①考虑系统级 CCF，即对于发生误动作的系统，假设该系统的其他保护功能均失效[8, 11]，特别地，由于 RPS 和 SAS 位于同一仪控平台，假设 RPS 和 SAS 会同时发生 CCF；②考虑系统优先级作用，即高优先级系统的误动作状态不能被低优先级系统所改变，除非操纵员执行就地手动操作，当前电厂优先级设置为 RPS>KDS>SAS>KDA>PSAS（按从高到低）；③根据仪控系统的信号特征，考虑可能一个或多个功能序列误动作。

PIE 归并结果见表 3 和表 4，共产生 17 个极限 PIE 和 10 个潜在新增事故。

表 3　PIE 归并结果

Tab. 3　Grouping Results of PIEs

触发系统	PIE总数	极限PIE数量	潜在新增事故数量
RPS	26	10	8
KDS	12	0	0
SAS	26	4	2
KDA	0	0	0
PSAS	42	1	0
非集中式系统	3	2	0

由表 3 可知，极限 PIE 可包络大部分同组的 PIE。此外对于 KDS 和 PSAS 误触发的 PIE，绝大部分可被 RPS 或 SAS 误触发的极限 PIE 所包络，这可以从系统功能上加以解释：①KDS 承担 RPS 失效时的多样化保护功能，相当于 RPS 功能的一个子集；②PSAS 用于核电厂运行自动控制，非集中式系统用于局部操控，在已有事故分析中本身就保守地不考虑其缓解作用。对于具有类似瞬态特征和后果的 PIE，当由 RPS 或 SAS 误触发时，考虑系统 CCF，此时丧失的保护功能最大化，且不能由 KDS 或 PSAS 来改变误动作状态，事故工况最为恶劣，因此潜在新增事故均由 RPS 或 SAS 误触发导致。

表 4　潜在新增事故

Tab. 4　Potential Additional Accidents

序号	触发系统	事故	核电厂状态
1	RPS	应急给水误启动	1~4
2	RPS	蒸汽大气排放阀误开启	1~6
3	RPS	RHR管线误隔离	5~6
4	RPS	主蒸汽隔离阀误关闭	1~4
5	RPS	下泄管线误隔离	1~6
6	RPS	中压安注误启动	5~6
7	RPS	稳压器安全阀误开启	5~6
8	SAS	下泄管线误全开	1~6
9	SAS	稳压器电加热器误启动	1~6
10	RPS	乏燃料水池冷却系统管线误隔离	1~6

3　仪控误动作事故分析

3.1　定性评价

对潜在新增事故，考虑叠加 RPS 和 SAS 发生 CCF，依靠 KDS 来缓解。RPS 和 SAS 是事故保护的主防线，KDS 提供独立于 RPS 和 SAS 的多样化的自动和手动保护功能。

潜在新增事故在已有事故（DBC 和 DEC-A）分析中均有类似瞬态事件相对应，主要区别是潜在新增事故只依靠 KDS 缓解事故，DBC 和 DEC-A 可以依靠 RPS 和 SAS 缓解（并且 KDS 仍然可用）。

本研究采用类比的方式进行评价：从瞬态角度，2 者具有相似的始发事件和瞬态进程；从系统功能角度，KDS 具有缓解事故所需的绝大部分自动和手动功能，如紧急停堆、启动安注和启动应急给水等，相比 RPS 的差别是 KDS 的保护整定值和响应时间不同，保护动作稍晚启动；从分析准则角度，RPS 和 SAS 同时失效的概率很低，一般认为已超出 DBC 范畴，其验收准则相比 DBC 可适当放宽，分析假设可更为现实[3, 12-13]，如，可参照已有 DEC-A 的验收准则；从事故后果角度，已有事故分析结果具有一定的安全裕量，能够支撑定性评价。

对每个事故进行类比分析，对比瞬态序列、

所需保护功能、信号整定值和延迟时间等，并且考虑系统优先级作用和操纵员手动干预的时间限制（假设事故后 30 min 在主控室执行手动操作，事故后 1 h 执行就地操作）。定性评价的结论是认为 KDS 能够缓解潜在新增事故后果并满足验收准则。此外，考虑到部分事故（应急给水误启动、蒸汽大气排放阀误开启和稳压器安全阀误开启）与已有事故工况存在一些特殊差异，为消除不确定的风险，需对此进行定量分析以进一步支持评价结果。

3.2 定量分析

3.2.1 应急给水误启动 该工况对应 DBC“给水系统故障引起给水流量增加”，其中包括了应急给水误启动的情况，并证明堆芯偏离泡核沸腾比（DNBR）远高于设计限值。相比而言，该工况的风险在于：由于 RPS 优先级高于 KDS，使得 KDS 的应急给水自动隔离保护功能不起作用，必须由操纵员于 1 h 后就地隔离应急给水，该工况存在导致 SG 满溢和放射性释放风险，而 DBC 则不会满溢。

为计算分析，采取如下保守假设：①初始为热停堆，此时 SG 二次侧初始水装量和放射性活度最大，汽空间体积最小，满溢时间最早；②所有列应急给水误以最大流量和最低温度向 SG 注入；③SG 一次侧向二次侧的泄漏率为最大值；④二次侧放射性核素全部经阀门向环境释放，忽略混合和闪蒸夹带等缓解作用。

经手动计算评估，事故后约 23 min SG 满溢，事故后 0~2 h 内非居住区边界上有效剂量为 1.1 mSv，规划限制区边界上有效剂量为 0.2 mSv，均远低于国家标准[14]规定的极限事故 100 mSv 的限值。

3.2.2 蒸汽大气排放阀误开启 该工况对应 DBC“SG 的一条释放管线或一个安全阀误开”，结果不会触发停堆信号，反应堆稳定在一个较高的功率水平。相比而言，该工况的风险在于可能触发多列排放阀误开启，相比 DBC 的破口面积更大，存在超功率和燃料损坏风险。

为计算分析，采取如下保守假设：①初始为满功率，初始条件和中子学参数按照对 DNBR 不利的方向选取；②考虑不利的保护整定值和延迟时间；③分别考虑 1、2 和 3 列排放阀误开。

采用 THEMIS 程序计算系统瞬态，1 列排放阀误开时，和 DBC 类似，不会触发紧急停堆；2 列和 3 列排放阀误开时，均由 KDS 的“功率量程高中子注量率”信号触发停堆保护。采用 FLICA III-F 程序计算堆芯 DNBR（图 2），其值均高于限值 1.19。

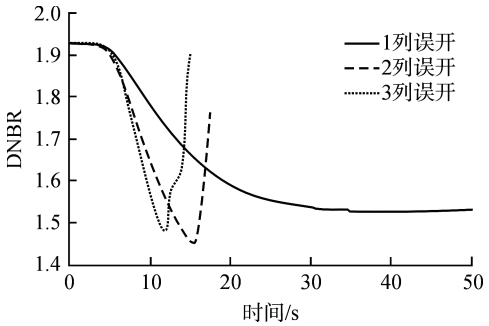

图 2 堆芯 DNBR

Fig. 2 Core DNBR

3.2.3 稳压器安全阀误开启 该工况由 RPS 的一回路低温超压保护信号误触发。对应 DBC“RHR 冷却停堆模式下小破口失水事故”，分析当量直径为 5 cm 的冷管段小破口事故，结果未出现堆芯裸露，能够长期导出堆芯余热。相比而言，该工况的风险在于：①稳压器安全阀破口当量直径略大于 5 cm；②相比 RPS，KDS 仅有“热管段环路水位低”一个自动安注信号可用，并且缺少自动停运 RHR 泵以防止气蚀的信号，保护功能可能存在不足。

为计算分析，采取的保守假设：①初始为 2 列 RHR 冷却停堆模式，3 台主泵运行，堆芯衰变热为最大值，RHR 冷却能力为最小值，以此使堆芯热量最大化；②考虑最大的一回路温度正不确定性、压力正不确定性和水装量负不确定性；③考虑不利的保护整定值和延迟时间。

采用 CATHARE 程序计算，该工况由于破口位于稳压器顶部，热管段水位并未下降，堆芯未裸露，但由于冷管段压力不断降低（图 3），使得主泵所在位置出现空泡（图 4），存在主泵气蚀风险。尽管 KDS 设有“2 个环路主泵压差低和安注信号同时存在触发所有主泵停运”的保护信号，但由于并未触发安注信号，且主泵两侧压差起初未明显下降，因此 KDS 未能及时触发主泵停运。为避免主泵气蚀，考虑在 KDS 上增设“2 个热管段实际压力与饱和压力之差（ΔP_{sat}）低 2

信号触发安注启动以及所有主泵停运”功能。此外分析 2 种情况：①“2 个 ΔP_{sat} 低 2”信号同步停运 RHR 泵；②不停运 RHR 泵。计算得到瞬态事件序列见表 5，主要结果见图 5~图 8。

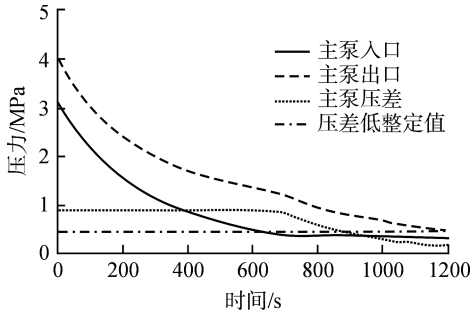

图 3　冷管段压力

Fig. 3　Pressure of Cold Leg

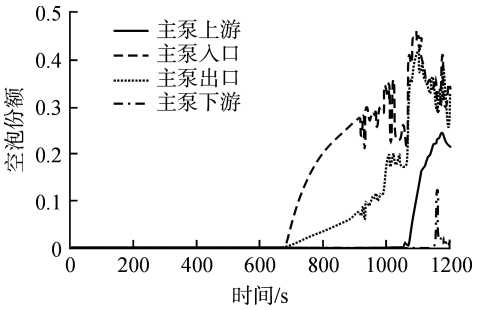

图 4　冷管段空泡份额

Fig. 4　Void Fraction of Cold Leg

表 5　瞬态事件序列

Tab. 5　Transient Event Sequence

瞬态事件	时间/s	
	情况1	情况2
瞬态开始	0	0
产生ΔP_{sat}低2信号	672	672
RHR泵停运	677	—
主泵停运	678	678
安注启动	701	701
安注流量与破口流量平衡	2236	2615

“—”表示不发生此事件

由图 5 和图 7 可知，2 种情况均避免了主泵气蚀。在 RHR 泵持续运行情况下，热管段未出现空泡（图 7），一回路在 RHR、安注和破口流量的共同作用下不断冷却（图 8）；在 RHR 泵停运情况下，由于冷却不足使得热管段出现空泡，但不久后消失（图 5），此后一回路温度缓慢上升（图 6），待操纵员干预后可依靠二次侧进行冷却，并重新连接 RHR 直至达到安全停堆。2 种情况均未出现堆芯裸露，在安注启动后一回路

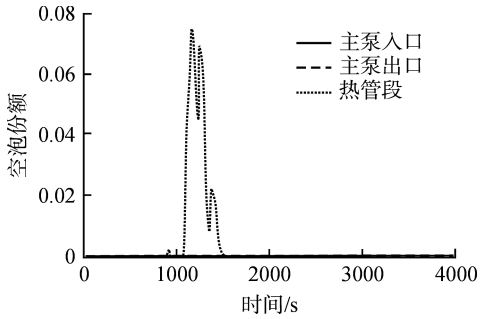

图 5　空泡份额（情况 1）

Fig. 5　Void Fraction (Case 1)

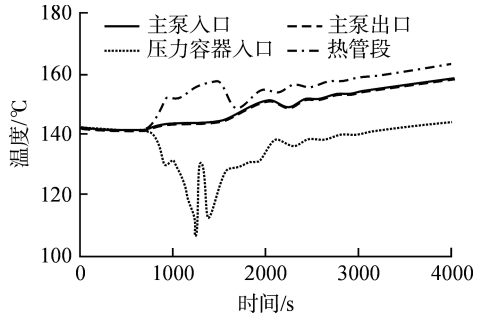

图 6　一回路冷却剂温度（情况 1）

Fig. 6　Primary Coolant Temperature (Case 1)

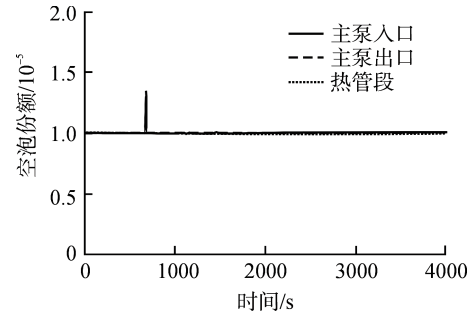

图 7　空泡份额（情况 2）

Fig. 7　Void Fraction (Case 2)

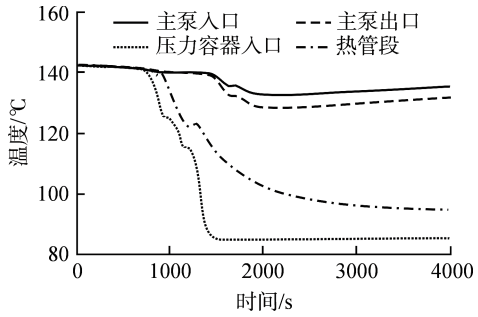

图 8　一回路冷却剂温度（情况 2）

Fig. 8　Primary Coolant Temperature (Case 2)

水装量很快恢复。

由进一步分析可知，由于 RHR 吸入口位于热管段波动管接口上游，注入口位于主泵下游，安注注入口也位于主泵下游，实际上从 SG 到主泵这一段并没有冷流体注入，导热很差，甚至存在二次侧向一次侧倒传热现象。从图 8 也可看出，即使不停运 RHR，主泵处温度仍然较高。因此，有必要及时停运主泵，减少主泵产热量以避免发生气蚀。

在 RPS 设计中包括“2 个热管段 ΔP_{sat} 低 1 信号触发安注启动”和“2 个热管段 ΔP_{sat} 低 2 信号触发 RHR 泵停运”保护功能，本研究建议增设的 KDS 功能能够在 RPS 失效时对主泵起到多样化保护作用，且整定值比 RPS 稍低，不会影响 RPS 的主防线功能。此外考虑到 KDS 功能的完整性，从保护设备角度建议同步停运 RHR 泵。

4 结束语

本研究基于简化分析方法，完成了仪控误动作 PIE 识别及潜在新增事故分析，论证了核电厂多样化保护系统能够保护和缓解事故后果，此外对 KDS 触发安注启动和主泵停运的功能设计提出了改进建议。研究成果可为核电厂安全分析提供支持，为仪控误动作分析方法论和导则研究提供参考。后续需进一步评估仪控误动作失效概率和事件频率，综合考虑其对核电厂设计的影响。

参考文献：

[1] 国家核安全局. 核动力厂设计安全规定：HAF 102—2016[S]. 北京：国家核安全局，2016: 26.

[2] ARIANS R, SOMMER D. Concepts for the architecture of digital I&C systems in NPPs and approaches for their assessment[R]. Brussels: EUROSAFE Forum, 2012.

[3] 肖鹏，刘宏春，周继翔，等. 核电厂多样化保护系统设计[J]. 核动力工程，2014, 35(2): 90-93.

[4] 穆海洋，宋雨，管运全. 田湾核电站反应堆保护系统多样化的研究[J]. 核安全，2018, 17(3): 17-21.

[5] 肖鹏，周继翔，刘宏春，等. 纵深防御和多样性策略在安全级数字化控制系统研发中的应用[J]. 上海交通大学学报，2018, 52(S1): 14-19.

[6] KORSAH K, MUHLHEIM M D, HOLCOMB D E. Industry survey of digital I&C failures: ORNL/TM-2006/626[R]. USA: Oak Ridge National Laboratory, 2007.

[7] 许标，刘明星，韩文兴，等. 核电厂安全级DCS系统可靠性参数测试方案的分析和计算[J]. 仪器仪表用户，2018, 25(11): 86-88.

[8] Office for Nuclear Regulation(ONR). Safety assessment principles for nuclear facilities[S]. U. K: ONR, 2020: 94-96.

[9] Digital Instrumentation and Control Working Group. Common position on spurious actuation: CP-DICWG-13[R]. Paris: Multinational Design Evaluation Programme, 2017.

[10] GARCIA I L. Spurious actuations in digital instrumentation and control systems-evaluation framework: IAEA-CN-251[C]. Vienna: International Conference on Topical Issues in Nuclear Installation Safety, 2017.

[11] IAEA. Protecting against common cause failures in digital I&C systems of nuclear power plants: NP-T-1.5[R]. Vienna: IAEA, 2009.

[12] 田皓文，关仲华，肖鹏. 核电厂多样化保护系统设计中验收准则的分析确定[J]. 核动力工程，2017, 38(S2): 146-148.

[13] NRC. Standard review plan, branch technical position 7-19, guidance for evaluation of diversity and defense-in-depth in digital computer-based instrumentation and control system[S]. USA: NRC, 2010: 6-7.

[14] 环境保护部和国家质量监督检验检疫总局 发布. 核动力厂环境辐射防护规定：GB6249—2011[S]. 北京：中国环境科学出版社，2011: 6.

（责任编辑：杨灵芳）