文章编号: 1000-6788(2012)05-1018-09 中图分类号: TP2; X-1; TL4; TP301 文献 志码: A

提高核的站设计案评 价助行系统平方

熊 刚[1], 王飞跃[1], 侯家琛[1], 西松[1], 张家麟[2], 付满昌[3]

(1. 中国科学院 自动化研究所 复杂系统管理与控制国家重点实验室 北京市智能化技术与系统工程技术研究中心, 北京 100190; 2. 工业第二研究设计院, 北京 100840; 3. 国 自仪系统工程有限公司, 上海 200233)

摘 要 安全可靠性是核电站存在和发展的生命线, 目前它还主要是通过人的经验和 格管理篇来保 , 但其智能性和科学性还不够. 核电站是一个 及多方面的动态变化要素的复杂系统, 现有控制、仿真和管理技术还不能为其生产运行和管理提供安全可靠的充分保 . 本文以 ACP 方法为基础, 基于信息技术最新发展成果, 提出了采用自上而下的规划和自下而上的设计相结合的方法, 来开发 核电站可靠性规划和设计软件包 , 使得核电站在建造前就有了安全可靠方面的科学依据. 进而提出平行系统方法, 分析其基本原理和成功应用实例, 并介绍其在核电站中应用的人工系统、计算试验和平行执行的 体内容, 给出了 PTS、PES 和 PMS 篇 体应用.

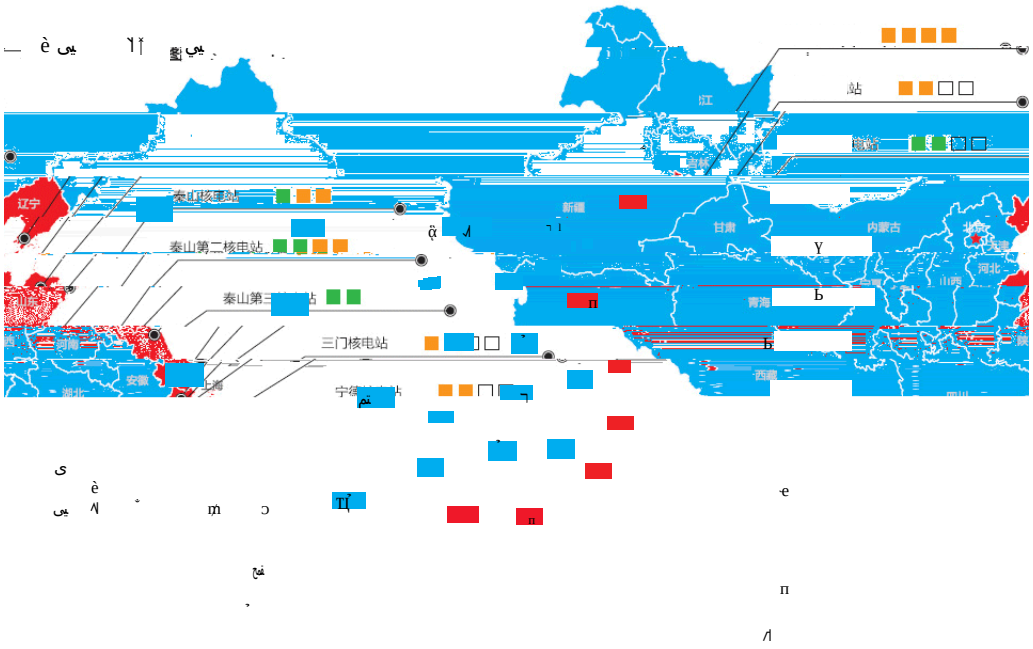
法 绍 核电站; 安全可靠; ACP 方法; 人工系统; 计算实验; 平行系统

To improve safety and reliability of nuclear power plant with parallel system method

IONG G [illegible][1], ANG F[illegible]-8[illegible][1], HO[illegible] J [illegible]-[illegible][1], DONG [illegible]-[illegible][1], HANG J [illegible]-[illegible][2], F[illegible] M [illegible]-[illegible][3]

(1. State Ke Laborator of Management and Control for Comple S stems, Beijing Engineering Research Center of

技进步、劳动者素质提高和管理创新的方向架变. 据国际原环能机构 (IAEA) 统计, 截至 2010 年初, 世界运行中的核电机工共计 437 [illegible], 控机平容量约为 371 G (,); 在建 56 [illegible], 控机约为 52G (,); 2030 年, 控机将达 807G (,). 目前, 美国、印度等国均提出了中长期核电发展目标和计划. 中国有 6 个核电站的 13 [illegible]在役核电机工, 核电控机容量达到 11 G (,)(见图 1), 与相同规模的火电相比, 相当于每年少 放二氧化碳 6700 万吨、二氧化硫 25 万吨、氮氧化物 15 万吨. 十二五 期间, 我国 临的改善能源结构和应对气候变化的任务更为艰巨, 发展核电将成为促进节能减 和推进 态文明建设的重要力量. 中国已经成为世界上在间核电机工理多的国家. 国家能源局的数据显示: 我国核电在建 23 [illegible], 占世界在建 57 [illegible]机工的 40%, 国内核电已经步入建设发展的加速期. 因此, 我国核电技术的结论研发已变得越来越重要, 如何保证核电站的安全、可靠是核电可持续化存在与发展的重中之重.



安全可靠性; 3) 在工程因素之外, 充分考虑人为等　会因素对核电安全的影响.

3　核电站可靠性规划和设计

以核电站仪控系统为　, 其设计、研制的许多方　, 都已经运用到高可靠、高利用率、高抗干　和高抗破坏等方　的实践经验. 各种特定类型核电站中所使用的仪表、仪器、控制和保护系统间, 共性多于差异.

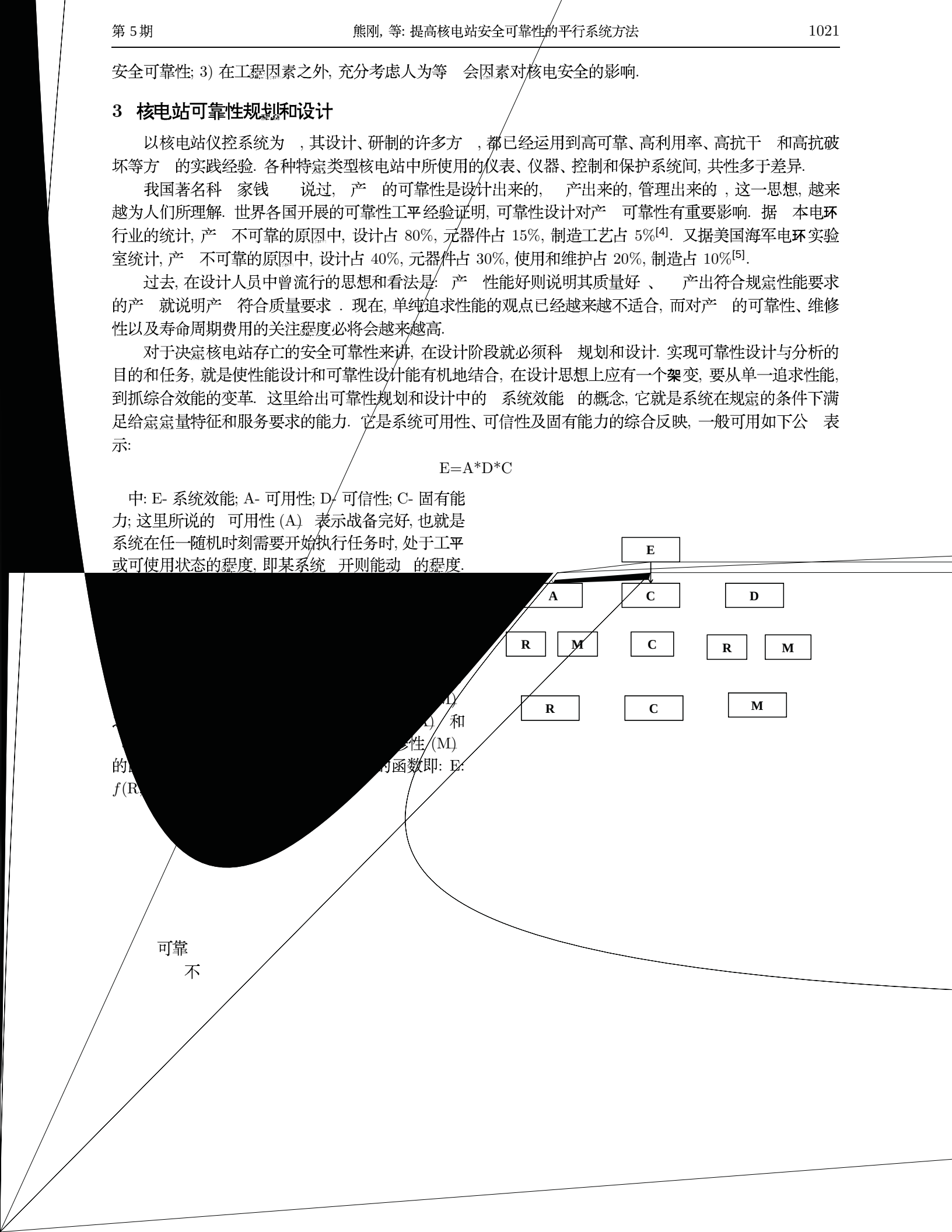
我国著名科　家钱　　说过,　产　的可靠性是设计出来的,　产出来的, 管理出来的 , 这一思想, 越来越为人们所理解. 世界各国开展的可靠性工平经验证明, 可靠性设计对产　可靠性有重要影响. 据　本电环行业的统计, 产　不可靠的原因中, 设计占 80%, 元器件占 15%, 制造工艺占 5%[4]. 又据美国海军电环实验室统计, 产　不可靠的原因中, 设计占 40%, 元器件占 30%, 使用和维护占 20%, 制造占 10%[5].

过去, 在设计人员中曾流行的思想和看法是:　产　性能好则说明其质量好 、　产出符合规定性能要求的产　就说明产　符合质量要求 . 现在, 单纯追求性能的观点已经越来越不适合, 而对产　的可靠性、维修性以及寿命周期费用的关注程度必将会越来越高.

对于决定核电站存亡的安全可靠性来讲, 在设计阶段就必须科　规划和设计. 实现可靠性设计与分析的目的和任务, 就是使性能设计和可靠性设计能有机地结合, 在设计思想上应有一个架变, 要从单一追求性能, 到抓综合效能的变革. 这里给出可靠性规划和设计中的　系统效能　的概念, 它就是系统在规定的条件下满足给定定量特征和服务要求的能力. 它是系统可用性、可信性及固有能力的综合反映, 一般可用如下公　表示:

$$E=A*D*C$$

中: E- 系统效能; A- 可用性; D- 可信性; C- 固有能力; 这里所说的　可用性 (A)　表示战备完好, 也就是系统在任一随机时刻需要开始执行任务时, 处于工平或可使用状态的程度, 即某系统　开则能动　的程度.



)

)　和

性 (M)

的函数即: E:

f(R,

3.2 可靠性方 详细系统

从可靠性潜力评价中选出的或推荐的核电站设计方案, 须进一步详细设计. 要选用质量已知的部件, 这些部件能在预寇环境下及在其额寇阀值内很好地工平. 尽量用各种可能的方法去模拟模型, 并确信满足相关性质的假寇. 如果模型能 假设, 一个或一工部件元件的故障与其它元件的故障统计无关, 那么设计者应该设法使其实现. 如假寇两个检测仪表通道 相独立, 那么它们应该这样寇值, 使得只是在极不可能的场合下两套才可能都失败.

简单而直 的系统是容易理解的, 容易模拟, 并且具有高的可靠性. 如果没有取得理优的模型, 就冒然去研制系统, 那么系统可能变得如此 杂且杂乱无章, 以致难以仿此制造. 并且, 从直观上看来, 整个系统也是值得怀疑的. 安全准则也决不会允许设计这种系统, 因为这种系统不能简单化为易处理的可靠性模型.

简单地说, 就是在普通的核电系统详细设计程序中要加上可靠性分析与设计的科目, 其中可靠性系统设计的概念和相应的数 关系都不难理解.

3.3 方

进行核电系统可靠性分析的论要价值, 是确信某些普通部件是不会对不可靠性 出意外的和毫无根据的贡献. 如果发现了这种问 , 就可通过选用更好的部件, 更纷繁和更全 的测试或合理的使用有冗余度的部件或模块来弥补这个缺邹.

基于上述核电站可靠性规划和设计思想和方法, 就可以研发出 核电站可靠性规划和设计软件包 , 它相当于计算机辅 设计 (CAD)、产 数据管理 (PDM) 和产 命周期管理 (PLM) 之类的软件产 . 同时, 在经改造之后, 它可成为之后平行系统中的人工系统部分.

4 行系

平行系统, 是指 某一个结然的实际系统和对应的一个或多个虚拟或理想的人工系统所工成的共同系统

5.1 系统

以 AP1000 核电站的仪控系统和保护系统为 , 如图 5 右下部所示, 实际系统是指核电站现有系统, **论**要包括运行与控制中心系统 (OCS)、数据显示和处理系统 (DDS)、保护和安全监测系统 (PMS)、反应堆紧急停堆系统 (RTS)、电 控制系统 (PCS)、多样驱动系统 (DAS)、专用监测系统 (SMS)、堆芯设备系统 (IIS)等, 仪控系统的软件平 是 C Q, 保护系统的软件平 是 O .

核电站的控制是通过仪控系统、保护系统等形成的 小闭环 来完成, 其安全可靠性可以得到较好的保证. 核电站的管理应该是在 小闭环 之外, 再加入核电站管理和人员等形成的 大闭环 来完成, 以适应不断变化的 会环境和物理环境, 实现 如安全、平稳、环保等多个目标. 但是目前的核电站管理是靠人的经验制 严格标准和管理制度, 之后通过人去执行 大闭环 管理, 存在很多不足. 比如:

1) 没有将人、管理和环境等各类 杂 会因素, 通过信息化手段去实现精确和实时的 大闭环 管理, 因此容易发 人员的误操平 等;

2) 现有系统条件无法对各类可能发 的问 进行实验, 如许多正常环境下无法 的实验、潜在的问 、各类不可预测事件等;

3) 现有核电系统对各类控制方法及应急保护预案也缺乏科 的分析研究过

杂系统的行为, 进而建立计算实验的理论和方法, 以此克服难以对核电 杂系统进行实验的困难, 为深入分析 杂核电系统的行为和有效评估决策的效果奠定基础. 通过各类事件驱动系统及场景发 器对各类场景及存在的问 进行计算实验, 如气候、地震等对核电站的影响, 仪控系统和保护系统的各类错误所能引发的潜在问 , 保护系统的实际执行, 人工操控所带来的问 等; 同时对各种方案进行评估分析, 从而找出理好的安全保护预案.